UNIVERSIDAD PERUANA UNIÓN

FACULTAD DE INGENIERÍA Y ARQUITECTURA

Escuela Profesional de Ingeniería de Sistemas

Una Institución Adventista

Implementación de los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte

Por:

Samuel Gavidia Mamani

Luis Daniel Torres Torres

Asesor:

Ing. Lizeth Geanina Huanca López

Lima, abril de 2018

Área temática: Ingeniería de Sistemas y Comunicaciones.

Línea de Investigación – UPEU: Tecnología de Información e Innovación Tecnológica.

Ficha catalográfica:

Gavidia Mamani , Samuel
Implementación de los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte / Samuel Gavidia Mamani; Asesor: Ing. Lizeth Geanina Huanca López. –Lima, 2018.
250 páginas: figuras, tablas

Tesis (Licenciatura)--Universidad Peruana Unión. Facultad de Ingeniería y Arquitectura. Escuela Profesional de Ingeniería de Sistemas, 2018.
Incluye referencias, resumen y anexos.

1. ISO/IEC 27002:2013. 2. Nivel de Seguridad de la Información. 3. COBIT 5. 4. Análisis de Riesgo. 5. Plan de Tratamiento de Riesgo I. Torres Torres, Luis Daniel, autor.

DECLARACIÓN JURADA DE AUTORIA DEL INFORME DE TESIS

Ing. Lizeth Geanina Huanca López, de la Facultad de Ingeniería y Arquitectura, Escuela Profesional Ingeniería de Sistemas, de la Universidad Peruana Unión.

DECLARO:

Que el presente informe de investigación titulado: ***"Implementación de los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte"*** constituye la memoria que presentan los **Bachilleres (Samuel Gavidia Mamani y Luis Daniel Torres Torres)** para aspirar al título de Profesional de Ingeniero de Sistemas, ha sido realizada en la Universidad Peruana Unión bajo mi dirección.

Las opiniones y declaraciones en este informe son de entera responsabilidad del autor, sin comprometer a la institución.

Y estando de acuerdo, firmo la presente constancia en *Lima,* a los 17, Abril del año 2018.

Ing. Lizeth Geanina Huanca López

"Implementación de los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte"

TESIS

Presentada para optar el Título Profesional de Ingeniero de Sistemas

JURADO CALIFICADOR

Dra. Erika Inés Acuña Salinas
Presidenta

Mg. Immer Elías Cuellar Rodríguez
Secretario

Mg. Daniel Lévano Rodríguez
Vocal

Ing. Lizeth Geanina Huanca López
Asesora

Lima, 17 de abril de 2018

Dedicatoria

A nuestros padres que nos apoyaron en todo momento, por inculcarnos valores y principios, a ellos va nuestra gratitud por apoyarnos siempre.

Agradecimiento

Agradecemos a Dios por hacer que culminemos una etapa más como profesionales en nuestras vidas, a la escuela de Ingeniería de Sistemas de la UPEU, a la Dra. Erika Acuña, al Mg. Elías Cuellar, al Mg. Daniel Lévano y al Mg. Omar Loayza por darnos tiempo y sus enseñanzas para seguir creciendo en nuestros propósitos; además, agradecer al Ing. Carlos Saavedra jefe del área de TI de la UPN por su dedicación, tiempo y su aporte brindado, y también a nuestra querida asesora la Ing. Lizeth Geanina Huanca López, por compartir sus conocimientos en el desarrollo del proyecto de tesis, a todos ellos les damos las gracias por su colaboración.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ABREVIATURAS Y ACRÓNIMOS

TI: Tecnología de información

ISO: International Organization for Standardization (Organización Internacional de Normalización)

IEC: International Electrotechnical Commission (Comisión electrotécnica Internacional)

COBIT: Control Objetives for Information and related Technology (Objetivos de control para la información y tecnologías relacionadas)

PAM: Process Assessment Model (Modelo de Evaluación de Procesos)

DSS: Deliver, Service and Support (Entrega, Servicio y Soporte)

UPN: Unión Peruana del Norte

SGSI: Sistema de Gestión de Seguridad de la Información

SI: Seguridad de la Información

IASD: Iglesia Adventista del Séptimo Día

PTR: Plan de tratamiento de riesgo

ISACA: Information Systems Audit and Control Association (Asociación de Auditoria y Control de Sistemas de Información)

RESUMEN

Esta tesis tiene por objetivo mejorar el nivel de seguridad física y lógica de la información del área de TI de la Unión Peruana del Norte.

En conjunto con la norma ISO/IEC 27002:2013, se utilizó el Framework Objetivos de Control para la información y tecnologías relacionadas (COBIT).

Se implementó una metodología de elaboración propia, para el desarrollo del proyecto, la cual se complementó en 5 fases. Cada fase contó con la aprobación de especialistas en el tema para corroborar la veracidad de la implementación, además, cada fase contiene actividades para desarrollar y cumplir con la mejora en seguridad.

En la fase 1 se desarrolló el compromiso con la organización para la implementación del proyecto. En la fase 2 y 5 se realizó la evaluación preliminar y la evaluación final. En la fase 3 se desarrolló el análisis de acuerdo a lo que menciona la norma ISO/IEC: 27005 para la identificación y medición de riesgos, que abarca sobre la identificación de activos, amenazas y vulnerabilidades. En la fase 4 se realizó la implementación de los controles seleccionados de la ISO/IEC 27002:2013.

La implementación de los controles de la ISO/IEC 27002:2013 permite mejorar el nivel de seguridad de la información del área de Tecnologías de Información (TI) de la Unión Peruana del Norte (UPN), permitiendo que el área de TI cumpla con el objetivo trazado para el desarrollo y beneficio de la organización, haciendo que la información se encuentre protegida y segura en su uso, almacenamiento, procesamiento y distribución.

Palabras Clave: Controles de seguridad, ISO/IEC 27002:2013, Nivel de Seguridad de la Información, COBIT 5, Análisis de Riesgo, Plan de Tratamiento de Riesgo

ABSTRACT

This thesis aims to improve the level of physical and logical security information in the IT area of the North Peruvian Union.

In conjunction with the ISO/IEC 27002:2013 Standard, the Control objectives Framework for information and related technologies (COBIT) was used.

A self-elaboration methodology was implemented for the development of the project, which was complemented in 5 phases. Each phase had the approval of specialists in the field to corroborate the veracity of the implementation, in addition, each phase contains activities to develop and comply with the improvement in security.

In Phase 1, the commitment to the Organization for the implementation of the project was developed. In Phase 2 and 5, the preliminary evaluation and final evaluation were carried out. In Phase 3, the analysis was developed according to the ISO/IEC: 27005 standard for the identification and measurement of risks, covering the identification of assets, threats and vulnerabilities. In Phase 4, the implementation of the selected controls of ISO/IEC 27002:2013 was carried out.

The implementation of the ISO/IEC 27002:2013 controls makes it possible to improve the level of information security in the Information Technology area (TI) of the Peruvian North Union (UPN), allowing the IT area to meet the objective laid out for the Development and benefit of the Organization, making the information protected and secure in its use, storage, processing and distribution.

Keywords: Safety Controls, ISO/IEC 27002:2013, information security level, COBIT 5, risk analysis, risk management Plan

INTRODUCCIÓN

Hoy en día la seguridad de la información es uno de los puntos más importantes que toda organización necesita tener, encargada de proteger y salvaguardar la información ante cualquier amenaza.

Tener la seguridad de la información mínima crea descontrol general en la organización, lo que origina desventajas en el mercado y posibles quiebras en el futuro; por eso la seguridad de la información forma parte de los objetivos de las organizaciones, y a pesar de tener conciencia sobre los daños, muchas organizaciones no se enfrentan a este punto importante con la dedicación y la responsabilidad con la que debiera tratarse. La Unión Peruana del Norte (UPN), mediante las actividades que realiza, se dedica al estudio bíblico llevando a gran parte del país un mensaje de la Iglesia Adventista del Séptimo Día. Para cualquier evento de la UPN el soporte tecnológico lo da el área de Tecnología de Información (TI), realizando sus funciones de soporte, infraestructura y desarrollo.

El Área de Tecnologías de Información (TI) es la encargada de velar por la seguridad de la información en la organización. Esto permite controlar el mantenimiento de los dispositivos tecnológicos, desarrollo de software y seguridad en la red, para que la información llegue segura a su destino; además, se encarga de brindar soporte a las distintas áreas de la UPN, además de brindar accesos a los usuarios de la organización.

La investigación realizada para la organización brindó documentos, registros, procesos y políticas de seguridad de la información, establecidas por los controles de la norma ISO/IEC 27002:2013, que permiten mejorar el nivel de la seguridad de la organización.

CAPÍTULO I: GENERALIDADES DE LA INVESTIGACIÓN

1.1. Identificación del problema

Romo Villafuerte & Valarezo Constante (2012) mencionan que para la protección de los activos de la información nos basamos en los pilares fundamentales de la seguridad de la información que son disponibilidad, integridad y confidencialidad.

Al no cumplir con esos 3 puntos importantes, se genera una desorganización general internamente, llegando a tener desventajas y pérdidas que perjudiquen el crecimiento de la organización en el mercado, por eso la seguridad de la información está dentro de los objetivos de las organizaciones, y a pesar de esa concienciación generalizada, muchas de ellas no se enfrentan a este problema con suma importancia, dedicación y responsabilidad con la que debiera tratarse.

Según Aguirre & Aristizabal (2013), ante el rápido desarrollo, incremento y sofisticación de la tecnología, también va en aumento los ataques cibernéticos en las organizaciones, donde se manifiestan las necesidades de la organización, por ello se tendrá que tomar medidas que ayuden a proteger la información de los ataques.

Teniendo la tecnología necesaria a disposición se puede llegar a gestionar y manejar un mejor control de la información en las organizaciones. Con el transcurrir del tiempo la tecnología avanza y la organización tiene que sincronizar sus procesos con los objetivos para así cumplir con los requisitos de la organización. La seguridad de la información se suele comparar con una sucesión, llegando a saber que es segura y confiable si el eslabón más débil también cumple con ello. Se necesita tratar la seguridad de información para encontrar ese eslabón y protegerlo, estableciendo puntos importantes para la protección de ella, tales como: establecimiento de políticas de seguridad de la información, y un establecimiento eficiente y eficaz en la seguridad física y lógica de la información.

El área de TI de la UPN programa sus funciones de acuerdo al Plan Operativo Anual (POA), donde se percibía que carecían de una infraestructura apropiada para el desarrollo de sus actividades. Adicionalmente, se observaba que existía un mal manejo de las políticas de seguridad de la información, puesto que estas no se encontraban documentadas, ni estaban bien definidas, además de no ser revisadas constantemente, igualmente se distinguió que existía una ineficiente gestión de riesgos de la información, por lo que se llegó a percibir que dentro del área de TI de la UPN existió un bajo nivel de gestión de la seguridad física y lógica de la información. Entre los factores principales que intervinieron se halló que hubo medidas limitadas de seguridad de la información a nivel lógico y físico lo que conllevaba a darse posibles errores los cuales podrían ser: pérdida de información, fallas en los sistemas y aplicaciones, fallas internas en los activos de información, entre otros. Esta situación motivaba la vulnerabilidad de la información, lo que se agravaba por el desconocimiento de la norma ISO/IEC 27002 para la Gestión de la Seguridad de la Información por parte del personal del Área de TI. (C. Saavedra, entrevista personal, 29 de marzo del 2016). Como consecuencia, era probable que se dieran ataques y riesgos en los activos de la información, lo cual conllevaba a que existiese un bajo control en el acceso lógico y físico de la información.

La ineficiente gestión de riesgos se dio por la inadecuada identificación de activos de información, identificación de vulnerabilidades e identificación de amenazas de los activos, donde en este último se tuvo poco conocimiento de los tipos de amenazas, por lo cual la organización no brindaba los beneficios que se esperaba y con ello pudieron ocurrir grandes pérdidas, que pudiesen generar altos costos para restablecer los activos de información y a la vez poder generar un alto impacto de los riesgos sobre la organización.

Ante la deficiente difusión de temas sobre seguridad de la información, hubo la posibilidad de generarse grandes problemas en la infraestructura por las deficientes prácticas

de seguridad por parte del personal. Con estos factores la organización perdería credibilidad, estructura e integridad en el área de TI.

Las pérdidas y deterioros de equipos informáticos pudieron darse por no tener un control sobre medidas de seguridad física de la información, donde la organización corría el riesgo de perder todo lo invertido en la seguridad de la información.

El ineficiente aseguramiento de la integridad, disponibilidad y confiabilidad de la información, pudo generar un desconcierto en toda la organización, al tener la información expuesta ante cualquier amenaza, lo que pudiese conllevar a tener una pérdida inminente de la información.

- **Planteamiento del problema**

¿En qué medida la implementación de los controles de la Norma ISO/IEC 27002:2013 mejora el nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte?

1.2. Objetivos

1.2.1. Objetivo general.

Implementar los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte.

1.2.2. Objetivos específicos.

- Realizar una auditoría inicial de los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana.
- Realizar un análisis de riesgo para la identificación de los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte.

- Desarrollar un plan de tratamiento de riesgo que contenga los controles de la ISO/IEC 27002:2013 identificados para la mejora del nivel de seguridad físico y lógico de la información del área de TI de la UPN
- Realizar una auditoría posterior de los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte

1.3. Hipótesis

1.3.1. Hipótesis general.

La implementación de los controles de la ISO/IEC 27002:2013 mejora significativamente el nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte

1.3.2. Hipótesis específicas.

- La realización de una auditoría inicial de los controles de la ISO/IEC 27002:2013 mejora significativamente el nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte.
- La realización de un análisis de riesgo permite la identificación de los controles de la ISO/IEC 27002:2013 para la mejora significativa del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte.
- La elaboración del plan de tratamiento de riesgo basado en los controles identificados en la norma ISO/IEC 27002:2013 permite la mejora significativa del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte.
- La realización de una auditoría posterior de los controles de la ISO/IEC 27002:2013 mejora significativamente el nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte.

1.4. Justificación

La auditoría en general es una actividad independiente y objetiva de aseguramiento, donde se obtiene el nivel de seguridad de la información, las cuales muestran la actualidad y con ello se brinda mejoras para la organización.

Todo esto permite alcanzar los objetivos propuestos en la investigación, además de mejorar el valor de los procesos y medir el nivel de riesgo de la información.

1.4.1. Justificación teórica.

La información lógica y física que las organizaciones cuentan hoy en día es enorme, la que se debe proteger mejorando el nivel de seguridad física y lógica de la organización. Nuestra investigación permite conocer el nivel de seguridad de la información para el Área de TI de la Unión Peruana del Norte, realizando una auditoría pre y post implantación de la mejora.

1.4.2. Justificación metodológica.

La metodología propuesta para la investigación combina las buenas prácticas del framework de los objetivos de control para la información y tecnología relacionada (Cobit 5) y la ISO 27001:2013; con esta propuesta se realiza el análisis situacional (Proceso DSS05 – Gestionar los Servicios de Seguridad – Cobit 5) y se implementa las mejoras del nivel de seguridad (ISO/IEC 27002:2013), propuesta que puede ser utilizada en otras organizaciones análogas.

1.4.3. Justificación práctica.

El resultado de la investigación aporta a mejorar el nivel de seguridad de la información, basada en la implementación de los controles de la ISO/IEC 27002:2013: Políticas de seguridad, seguridad lógica y seguridad física, lo que minimiza los riesgos y se optimiza el nivel de seguridad de la información

CAPÍTULO II: MARCO TEÓRICO CONCEPTUAL

2.1. Estado del arte (Antecedentes)

Mazorra, Toapanta, & Briones (2008) en su investigación, "*Implementar Política de Seguridad a Nivel de Hardware y aplicado a una Empresa Pequeña*" Guayaquil – Ecuador, tienen como objetivo general, el poder implementar una red de datos y emplear en su totalidad las políticas de seguridad bajo un nivel de hardware para que prevengan el acceso de usuarios que no son deseados en la red. Añaden también que será un modelo de políticas sobre seguridad que serán aplicadas a pequeñas empresas. El desarrollo de esta tesis consta de cuatro capítulos; en el primer capítulo tocan el tema de las tecnologías de red y describen algunas de las amenazas que son usuales para las redes de datos, incluyen también en este capítulo la mención de herramientas para la monitorización de las redes de datos tanto a un nivel de software como hardware. En el segundo capítulo realizan la elaboración de políticas de seguridad proponiendo una manera de realizar el análisis para instaurar las políticas de seguridad y luego redactar tales políticas bajo un nivel de hardware el cual les permitirá llegar a un nivel deseado de seguridad. En el tercer capítulo realizan un caso de estudio a una empresa pequeña donde se procedió a evaluar de manera completa la posición de seguridad de red mediante un minucioso análisis a sus dispositivos. Se determina que las políticas de seguridad se implementan para obtener una protección contra las amenazas. Incluso se gestiona la seguridad por medio de simulaciones periódicas y revisiones para corroborar si es que los controles siguen siendo apropiados y eficaces. En el último capítulo se estimaron los costos para la implementación del caso de estudio y posteriormente se hizo el análisis costo/beneficio. El aporte de este proyecto de tesis es de vital importancia para el desarrollo de nuestras políticas de seguridad a nivel físico, puesto que ayudan a tener un mejor enfoque sobre las medidas que se debiesen adoptar e implantar para un eficaz resguardo.

Cedeño (2017) en la tesis, "*Planes y Controles de Tratamiento de Riesgos Tecnológicos para la Gestión de Información basado en Normas de Seguridad: Caso GADPE*", Esmeraldas – Ecuador, tiene como objetivo general "Mejorar los riesgos y amenazas a los que se ve fuertemente expuesta la información de la unidad informática del Gobierno autónomo descentralizado de la provincia de Esmeraldas (GADPE) mediante la propuesta de políticas y el plan de tratamiento de riesgo basados en la norma de seguridad". Para el desarrollo de esta tesis se describieron políticas de seguridad de la información, las que permitirán obtener una rápida respuesta y una ágil detección de las amenazas e incidentes de seguridad, a la vez la elaboración y/o diseño de métricas que permitan obtener resultados comparables y reproducibles para la medición de la eficacia de los controles o grupo de controles. Por último, para la elaboración de su plan de tratamiento de riesgo se dio a través de la implantación de controles y procedimientos de monitorización para la detección a tiempo de posibles incidentes. Además de ello, mencionan que la normativa la cual se usó conlleva un conjunto de controles para el eficiente tratamiento de la información de la institución certificando su integridad, confiabilidad y disponibilidad. El aporte de este proyecto de tesis es de vital importancia para el desarrollo de la elaboración de nuestro Plan de tratamiento de riesgo, ya que se basan en el desarrollo y definición de políticas de seguridad, la cual será útil para el eficiente resguardo de la información, además de la implantación de los controles de la norma ISO 27002, los cuales permitirán minimizar y reducir los riesgos y amenazas que pudiesen surgir en la organización, estando así la información integra y segura en todas sus dimensiones.

Aguirre & Aristizabal (2013) en la tesis, "*Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda*" Pereyra – Colombia, tuvieron el objetivo de "Diseñar el sistema de gestión de seguridad de la información para el Grupo Empresarial La Ofrenda". Según lo que menciona el desarrollo del proyecto, la

implementación de sistema de gestión de seguridad de la información (SGSI) ayuda a contribuir con el funcionamiento de la organización; la norma ISO/IEC 27001 ayuda a las empresas a tratar de manera eficaz la seguridad de la información brindando controles de soporte que permite cumplir con la confidencialidad, integridad y disponibilidad de la información. Por ello, para la empresa, es importante implementar un SGSI, porque permite llevar a cabo la reorganización en todas las áreas cumpliendo con la norma, generando una estabilidad en infraestructura, donde esté a la altura de las grandes organizaciones que buscan las certificaciones de la norma. Este trabajo aportó a la investigación, porque permitió conocer, cómo gestionar un estudio de riesgo con la herramienta Cobit logrando un análisis que permita controlar las amenazas, vulnerabilidades y activos de la información.

2.2. Marco teórico

Para deducir el problema que tiene una empresa se necesita tener la capacidad para determinar las acciones que realiza la organización, es importante entender términos y definiciones que son fundamentales y que a lo largo de la investigación serán citados. Las definiciones serán el soporte de ayuda para otorgar un resultado viable a la problemática identificada. Los términos claves dentro del proyecto de investigación son:

- Controles de la Norma ISO/IEC 27002:2013
- Mejora del nivel de seguridad física y lógica de la información
- Área de TI de la Unión Peruana del Norte

A continuación, se detalla los términos o conceptos que están contenidos dentro de ellos, y que son importantes para el análisis y alcance del problema.

2.2.1. Controles de la Norma ISO/IEC 27002:2013.

2.2.1.1. Seguridad de la información.

Según Parra (2017) la información es un medio o recurso que al igual que el resto de los activos, posee un valor importante para toda organización, por lo cual tendría que ser debidamente protegida.

La seguridad de la información la resguarda de diversas amenazas, con el propósito de asegurar la continuidad del negocio, reducir el daño al mismo y reducir el retorno sobre las oportunidades e inversiones.

Córdova J. (2012) menciona que la seguridad de la información posee tres pilares importantes: la integridad, confidencialidad y disponibilidad de la información.

Confidencialidad: Según Caccuri (2012), "debe tener la capacidad de proteger la información ante el intento de acceso de divulgación a otros usuarios no autorizados. Consiste en asegurar la privacidad de los datos. Solamente los individuos, procesos o dispositivos autorizados pueden acceder a ellos".

Integridad: Según Caccuri (2012), "la información debe estar completa y no ser alterada o modificada sin autorización. La integridad se refiere a la protección de la información de acciones tanto deliberadas como accidentales".

Disponibilidad: Según Pacheco & Jara (2010), "la disponibilidad garantiza que los recursos del sistema y la información estén disponibles solo para usuarios autorizados en el momento que los necesiten."

En la Figura 1 se aprecia los tres pilares básicos de la seguridad de la información.

Figura 1: Propiedades fundamentales de la Seguridad ***(Fuente:*** infosegur)

A. Requerimientos de seguridad de la información

Según Project Management Consultores de Proyectos (2006), existen tres fuentes primordiales para los requerimientos en referencia a la seguridad de la información. La primera fuente deriva de hacer una evaluación de riesgo para la organización, al tener en cuenta los objetivos y estrategia de negocio. A través de esta evaluación de riesgos se identifican las amenazas pertenecientes a los activos, se evalúa su vulnerabilidad y su probabilidad de ocurrencia y se estima o calcula su impacto potencial. La segunda fuente son los requerimientos reguladores, requerimientos legales, requerimientos contractuales y requerimientos estatutarios que se ven en la necesidad de complacer a una organización, a los contratistas, a sus socios comerciales y proveedores de servicio y su entorno socio-cultural.

La tercera fuente es con los objetivos, conjunto particular de principios y los requerimientos comerciales para el desarrollo de la información que una organización ha procesado para mantener sus operaciones.

B. Entidades implicadas en la seguridad de la información

Según Areitio (2008), las actividades de seguridad deben ser tomadas en cuenta por todo el personal relacionado con los sistemas de información, como son:

- Desarrolladores de software y Fabricantes de productos.
- Integradores de datos en el sistema.
- Compradores, que pueden ser organizaciones o usuarios finales.
- Organizaciones de evaluación de la seguridad, como certificadores de sistemas, evaluadores de productos o acreditares de operación.
- Administradores de sistemas y de seguridad.
- Terceras partes confiables (TTP), como son las autoridades de certificación, fedatarios electrónicos con servicios de firma electrónica avanzada y sellado temporal.

- Consultores u organizaciones de servicios, por ejemplo, servicios de externalización u outsourcing de la gestión de la seguridad.

2.2.1.2. Norma ISO/IEC 27002:2013.

La ISO 27002 es una guía de recomendaciones de buenas prácticas para la gestión de la información. Otorga directrices a las normas de seguridad de la información en las prácticas de seguridad de la información y en las organizaciones, abarcando la selección, implementación y la administración de controles considerando el contexto de seguridad de la información de la organización.

Para Perú se tiene la NTP-ISO/IEC 1799, y según ISOTools Excellence (2015), "Ofrece todas las recomendaciones para poder gestionar un Sistema de Seguridad de la información (SSI), al igual que la norma internacional ISO 27001, ofrece los requisitos necesarios para que los responsables del área en concreto puedan iniciar, implantar, mantener y mejorar la seguridad en las organizaciones.". Aparte de ello se tiene NTP-ISO/IEC 27002:2017 para la seguridad de la información.

La ISO 27002 es de suma importancia para el desarrollo en la mejora del nivel de seguridad de la información, puesto que establece los controles a seguir para certificar la disponibilidad, confidencialidad e integridad de la información.

A. Historia de la Norma ISO/IEC 27002

Prada (2009) menciona que esta norma nace como evolución histórica de la norma británica BS 7799, ya en el 2000 se le conoce como ISO/IEC 17999 y en el año 2005 pasa a llamarse ISO/27002 para formar parte de la familia de la ISO 27000.

B. Contenido de la Norma ISO/IEC 27002:2013

Gutiérrez (2013) señala que en esta versión nueva de la norma se hallan los controles que intentan disminuir la posibilidad de ocurrencia y/o el impacto de los variados riesgos al cual se encuentra expuesta una organización.

Manjón (2015) menciona que con el reajuste de esta norma las organizaciones podrán hallar una guía que les sea útil para implementar los controles de seguridad en una organización y de las prácticas más eficientes para la gestión en la seguridad de la información.

La norma ISO/IEC 27002:2013 contiene 14 dominios, 35 objetivos de control y 114 controles. En la Tabla 1 se muestra los respectivos dominios de la norma ISO 27002:2013 con sus respectivos objetivos de control y cantidades de controles.

Tabla 1:
Dominios – Objetivos de Control y Controles ISO 27002:2013

ÍTEMS	DOMINIOS	OBJETIVOS DE CONTROL	Nº CONTROLES
1	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	1.1 DIRECTRICES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	2
2	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	2.1 ORGANIZACIÓN INTERNA 2.2 LOS DISPOSITIVOS MÓVILES Y EL TELETRABAJO	5 2
3	SEGURIDAD RELATIVA A LOS RECURSOS RUMANOS	3.1 ANTES DEL EMPLEO 3.2 DURANTE EL EMPLEO 3.3 FINALIZACIÓN DEL EMPLEO O CAMBIO EN EL PUESTO DE TRABAJO	2 3 1
4	GESTIÓN DE ACTIVOS	4.1 RESPONSABILIDAD SOBRE LOS ACTIVOS 4.2 CLASIFICACIÓN DE LA INFORMACIÓN 4.3 MANIPULACIÓN DE LOS SOPORTES	4 3 3
5	CONTROL DE ACCESO	5.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS 5.2 GESTIÓN DE ACCESO DE USUARIO 5.3 RESPONSABILIDADES DEL USUARIO 5.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	2 6 1 5
6	CRIPTOGRAFÍA	6.1 CONTROLES CRIPTOGRÁFICOS	2
7	SEGURIDAD FÍSICA Y DEL ENTORNO	7.1 ÁREAS SEGURAS 7.2 SEGURIDAD DE LOS EQUIPOS	6 9
8	SEGURIDAD DE LAS OPERACIONES	8.1 PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES 8.2 PROTECCIÓN CONTRA EL SOFTWARE MALICIOSO (MALWARE) 8.3 COPIAS DE SEGURIDAD 8.4 REGISTROS Y SUPERVISIÓN 8.5 CONTROL DEL SOFTWARE EN EXPLOTACIÓN 8.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA 8.7 CONSIDERACIONES SOBRE LA AUDITORIA DE SISTEMAS DE INFORMACIÓN	4 1 1 4 1 2 1

ÍTEMS	DOMINIOS	OBJETIVOS DE CONTROL	N° DE CONTROLES
9	SEGURIDAD DE LAS COMUNICACIONES	9.1 GESTIÓN DE LA SEGURIDAD DE REDES	3
		9.2 INTERCAMBIO DE INFORMACIÓN	4
10	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	10.1 REQUISITOS DE SEGURIDAD EN SISTEMAS DE INFORMACIÓN	3
		10.2 SEGURIDAD EN EL DESARROLLO Y EN LOS PROCESOS DE SOPORTE	9
		10.3 DATOS DE PRUEBA	1
11	RELACIÓN CON PROVEEDORES	11.1 SEGURIDAD EN LAS RELACIONES CON PROVEEDORES	3
		11.2 GESTIÓN DE LA PROVISIÓN DE SERVICIOS DEL PROVEEDOR	2
12	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	12.1 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS	7
13	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	13.1 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	3
		13.2 REDUNDANCIAS	1
14	CUMPLIMIENTO	14.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES	5
		14.2 REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN	3

Fuente: Enunciado adoptado de la Norma ISO 27002:2013 (AENOR, (2015))

- **Estructura piramidal (Dominios de control)**

En la Figura 2 se observa los dominios de control la Norma ISO 27002:2013 enmarcados dentro de 4 vertientes tales como: seguridad organizativa, seguridad física, seguridad lógica y seguridad legal; y bajo tres niveles: operacional, estratégico y táctico.

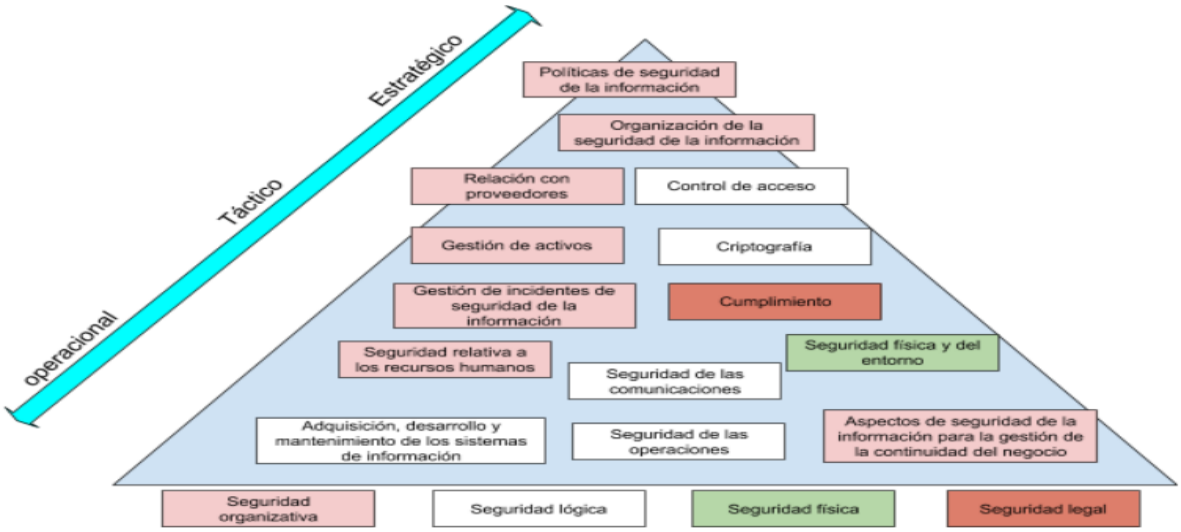


Figura 2: Estructura piramidal (Dominios de Control) (***Fuente*:** Elaboración propia)

C. Selección de controles

Según AENOR (2015), la selección de controles a depender de las determinaciones de carácter organizativo basadas sobre los criterios de aceptación de riesgo, elecciones de tratamiento de riesgo y de los enfoques generales de gestión de riesgo adaptado en la organización. También tendría que depender, de toda la legislación internacional y nacional aplicable. La selección de controles dependerá igualmente del modo en que los controles interactúen para brindar una protección en profundidad.

Dentro de esta norma algunos controles pueden considerarse como principios o normas que dirigen la gestión de la seguridad de la información, siendo así aplicables en la mayoría de las organizaciones.

D. Seguridad física

La seguridad física es importante para toda organización, puesto que se necesita proteger el acceso físico a las áreas de información, esta deducción entiende que ante cualquier eventualidad que perjudique a la información, se tenga que prever un mejor análisis de seguridad. Ante ello, la falta de análisis en las áreas de información sobre seguridad física, algunas empresas pierden credibilidad y presupuesto que no se encontraba como inversión, por ello se recomienda concientizar a las empresas sobre la importancia de la seguridad física.

Para cumplir con la necesidad que algunas empresas desconocen sobre la seguridad física, la norma ISO/IEC 27002:2013 establece controles de seguridad físicos, que indica que parámetros cumplir, para la protección segura sobre los equipos que se encuentran en el área de información, permitiendo restricciones sobre el acceso a ellos.

A continuación, de la Tabla 2 a la Tabla 4, se muestran los controles de seguridad física seleccionados para la implementación. Los controles fueron seleccionados durante la elaboración del Plan de Tratamiento de Riesgo y mediante el proceso DSS05 – “Gestionar los

servicios de Seguridad" de COBIT. A esto se les considero algunos de los controles de los dominios 5 y 8 tanto para la seguridad física como para la lógica.

En la Tabla 2 se muestra todo el contenido del Dominio 5, del cual, para nuestra implementación, se consideró el control 5.1.1

Tabla 2:
Objetivos de control y controles del dominio 5

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN		
5.1 DIRECTRICES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN **OBJETIVO:** PROPORCIONAR ORIENTACIÓN Y APOYO A LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE ACUERDO CON LOS REQUISITOS DEL NEGOCIO, LAS LEYES Y NORMAS PERTINENTES		
5.1.1	POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	**CONTROL**: UN CONJUNTO DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN DE ACUERDO CON LOS REQUISITOS DEL NEGOCIO, LAS LEYES Y NORMAS PERTINENTES
5.1.2	REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	**CONTROL:** LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEBERÍAN REVISARSE A INTERVALOS PLANIFICADOS O SIEMPRE QUE SE PRODUZCAN CAMBIOS SIGNIFICATIVOS, A FIN DE ASEGURAR QUE SE MANTENGA SU IDONEIDAD, ADECUACIÓN Y EFICACIA

Fuente: ISO 27002:2013 (AENOR, (2015))

En la Tabla 3 se muestra todo el contenido del Dominio 8, del cual, para nuestra implementación, se consideraron los controles 8.1.1 y 8.2.1

Tabla 3:
Objetivos de control y controles del dominio 8

8. GESTIÓN DE ACTIVOS		
8.1 RESPONSABILIDAD SOBRE LOS ACTIVOS **OBJETIVO:** IDENTIFICAR LOS ACTIVOS DE LA ORGANIZACIÓN Y DEFINIR LAS RESPONSABILIDADES DE PROTECCIÓN ADECUADAS		
8.1.1	INVENTARIO DE ACTIVOS	**CONTROL**: LA INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS A LA INFORMACIÓN Y A LOS RECURSOS PARA EL TRATAMIENTO DE LA INFORMACIÓN DEBERÍAN ESTAR CLARAMENTE IDENTIFICADOS Y DEBERÍA ELABORARSE Y MANTENERSE UN INVENTARIO
8.1.2	PROPIEDAD DE LOS ACTIVOS	**CONTROL:** TODOS LOS ACTIVOS QUE FIGURAN EN EL INVENTARIO DEBERÍAN TENER UN PROPIETARIO
8.1.3	USO ACEPTABLE DE LOS ACTIVOS	**CONTROL:** SE DEBERÍAN IDENTIFICAR, DOCUMENTAR E IMPLEMENTAR LAS REGLAS DE USO ACEPTABLE DE LA INFORMACIÓN Y DE LOS ACTIVOS ASOCIADOS CON LOS RECURSOS PARA EL TRATAMIENTO DE LA INFORMACIÓN
8.1.4	DEVOLUCIÓN DE ACTIVOS	**CONTROL:** TODOS LOS EMPLEADOS Y TERCERAS PARTES DEBERÍAN DEVOLVER TODOS LOS ACTIVOS DE LA ORGANIZACIÓN QUE ESTÉN EN SU PODER AL FINALIZAR SI EMPLEO, CONTRATO O ACUERDO
8.2 CLASIFICACIÓN DE LA INFORMACIÓN **OBJETIVO:** ASEGURAR QUE LA INFORMACIÓN RECIBA UN NIVEL ADECUADO DE PROTECCIÓN DE ACUERDO CON SU IMPORTANCIA PARA LA ORGANIZACIÓN		

8.2.1	CLASIFICACIÓN DE LA INFORMACIÓN	**CONTROL:** LA INFORMACIÓN DEBERÍA SER CLASIFICADA EN TÉRMINOS DE LA IMPORTANCIA DE SU RELEVANCIA FRENTE A REQUISITOS LEGALES, VALOR, SENSIBILIDAD Y CRITICIDAD ANTE REVELACIÓN O MODIFICACIÓN NO AUTORIZADAS
8.2.2	ETIQUETADO DE LA INFORMACIÓN	**CONTROL:** DEBERÍA DESARROLLARSE E IMPLEMENTARSE UN CONJUNTO DE PROCEDIMIENTOS PARA ETIQUETAR LA INFORMACIÓN, DE ACUERDO CON EL ESQUEMA DE CLASIFICACIÓN ADOPTADO POR LA ORGANIZACIÓN
8.2.3	MANIPULADO DE LA INFORMACIÓN	**CONTROL:** DEBERÍA DESARROLLARSE E IMPLEMENTARSE UN CONJUNTO DE PROCEDIMIENTOS PARA LA MANIPULACIÓN DE LA INFORMACIÓN, DE ACUERDO CON EL ESQUEMA DE CLASIFICACIÓN ADOPTADO POR LA ORGANIZACIÓN
8.3 MANIPULACIÓN DE LOS SOPORTES **OBJETIVO:** EVITAR LA REVELACIÓN, MODIFICACIÓN, ELIMINACIÓN O DESTRUCCIÓN NO AUTORIZADAS DE LA INFORMACIÓN ALMACENADA EN SOPORTES		
8.3.1	GESTIÓN DE SOPORTES EXTRAÍBLES	**CONTROL:** SE DEBERÍAN IMPLEMENTAR PROCEDIMIENTOS PARA LA GESTIÓN DE LOS SOPORTES EXTRAÍBLES, DE ACUERDO CON EL ESQUEMA DE CLASIFICACIÓN ADOPTADO POR LA ORGANIZACIÓN
8.3.2	ELIMINACIÓN DE SOPORTES	**CONTROL:** LOS SOPORTES DEBERÍAN ELIMINARSE DE FORMA SEGURA CUANDO YA NO VAYAN A SER NECESARIOS, MEDIANTE PROCEDIMIENTOS FORMALES.
8.3.3	SOPORTES FÍSICOS EN TRÁNSITO	**CONTROL:** DURANTE EL TRANSPORTE FUERA DE LOS LÍMITES FÍSICOS DE LA ORGANIZACIÓN, LOS SOPORTES QUE CONTENGAN INFORMACIÓN DEBERÍAN ESTAR PROTEGIDOS CONTRA ACCESOS NO AUTORIZADOS, USOS INDEBIDOS O DETERIORO.

Fuente: ISO 27002:2013 (AENOR, (2015))

En la Tabla 4 se muestra todo el contenido del Dominio 11, del cual, para nuestra implementación, se consideraron los controles 11.1.1 y 11.2.1

Tabla 4:
Objetivos de control y controles del dominio 11

11. SEGURIDAD FÍSICA Y DEL ENTORNO		
11.1 ÁREAS SEGURAS **OBJETIVO**: PREVENIR EL ACCESO FÍSICO NO AUTORIZADO, LOS DAÑOS E INTERFERENCIA A LA INFORMACIÓN DE LA ORGANIZACIÓN Y A LOS RECURSOS DE TRATAMIENTO DE LA INFORMACIÓN		
11.1.1	PERÍMETRO DE SEGURIDAD FÍSICA	**CONTROL**: SE DEBERÍAN UTILIZAR PERÍMETROS DE SEGURIDAD PARA PROTEGER LAS ÁREAS QUE CONTIENEN INFORMACIÓN SENSIBLE ASÍ COMO LOS RECURSOS DE TRATAMIENTO DE LA INFORMACIÓN
11.1.2	CONTROLES FÍSICOS DE ENTRADA	**CONTROL**: LAS ÁREAS SEGURAS DEBERÍAN ESTAR PROTEGIDAS MEDIANTE CONTROLES DE ENTRADA ADECUADOS, PARA ASEGURAR QUE ÚNICAMENTE SE PERMITE EL ACCESO AL PERSONAL AUTORIZADO
11.1.3	SEGURIDAD DE OFICINAS, DESPACHOS Y RECURSOS	**CONTROL**: PARA LAS OFICINAS, DESPACHOS Y RECURSOS, SE DEBERÍA DISEÑAR Y APLICAR LA SEGURIDAD FÍSICA

11.1.4	PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	**CONTROL**: SE DEBERÍA DISEÑAR Y APLICAR UNA PROTECCIÓN FÍSICA CONTRA DESASTRES NATURALES, ATAQUES PROVOCADOS POR EL HOMBRE O ACCIDENTES
11.1.5	EL TRABAJO EN ÁREAS SEGURAS	**CONTROL**: SE DEBERÍAN DISEÑAR E IMPLEMENTAR PROCEDIMIENTOS PARA TRABAJAR EN LAS ÁREAS SEGURAS
11.1.6	ÁREAS DE CARGA Y DESCARGA	**CONTROL**: DEBERÍAN CONTROLARSE LOS PUNTOS DE ACCESO TALES COMO LAS ÁREAS DE CARGA Y DESCARGA Y OTROS PUNTOS, DONDE PUEDA ACCEDER PERSONAL NO AUTORIZADO A LAS INSTALACIONES, Y SI ES POSIBLE, AISLAR DICHOS PUNTOS DE LOS RECURSOS DE TRATAMIENTO DE LA INFORMACIÓN PARA EVITAR ACCESOS NO AUTORIZADOS
11.2 SEGURIDAD DE LOS EQUIPOS **OBJETIVO**: EVITAR LA PÉRDIDA, DAÑO, ROBO O EL COMPROMISO DE LOS ACTIVOS Y LA INTERRUPCIÓN DE LAS OPERACIONES DE LA ORGANIZACIÓN		
11.2.1	EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS	**CONTROL**: LOS EQUIPOS DEBERÍAN SITUARSE O PROTEGERSE DE FORMA QUE SE REDUZCAN LOS RIESGOS DE LAS AMENAZAS Y LOS RIESGOS AMBIENTALES ASÍ COMO LAS OPORTUNIDADES DE QUE SE PRODUZCAN ACCESOS NO AUTORIZADOS
11.2.2	INSTALACIONES DE SUMINISTRO	**CONTROL**: LOS EQUIPOS DEBERÍAN ESTAR PROTEGIDOS CONTRA FALLOS DE ALIMENTACIÓN Y OTRAS ALTERACIONES CAUSADAS POR FALLOS EN LAS INSTALACIONES DE SUMINISTRO
11.2.3	SEGURIDAD DEL CABLEADO	**CONTROL**: EL CABLEADO ELÉCTRICO Y DE TELECOMUNICACIONES QUE TRANSMITE DATOS QUE SIRVE DE SOPORTE A LOS SERVICIOS DE INFORMACIÓN DEBERÍA ESTAR PROTEGIDO FRENTE A INTERCEPTACIONES, INTERFERENCIAS O DAÑOS
11.2.4	MANTENIMIENTO DE LOS EQUIPOS	**CONTROL**: LOS EQUIPOS DEBERÍAN RECIBIR UN MANTENIMIENTO CORRECTO QUE ASEGURE SU DISPONIBILIDAD Y SU INTEGRIDAD CONTINUAS
11.2.5	RETIRADA DE MATERIALES PROPIEDAD DE LA EMPRESA	**CONTROL**: SIN AUTORIZACIÓN PREVIA A LOS EQUIPOS, LA INFORMACIÓN O EL SOFTWARE NO DEBERÍAN SACARSE DE LAS INSTALACIONES.
11.2.6	SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES	**CONTROL**: DEBERÍAN APLICARSE MEDIDAS DE SEGURIDAD A LOS EQUIPOS SITUADOS FUERA DE LAS INSTALACIONES DE LA ORGANIZACIÓN, TENIENDO EN CUENTA LOS DIFERENTES RIESGOS QUE CONLLEVA TRABAJAR FUERA DE DICHAS INSTALACIONES
11.2.7	REUTILIZACIÓN O ELIMINACIÓN SEGURA DE EQUIPOS	**CONTROL**: TODOS LOS SOPORTES DE ALMACENAMIENTO DEBERÍAN SER COMPROBADOS PARA CONFIRMAR QUE TODO DATO SENSIBLE Y SOFTWARE BAJO LICENCIA SE HA ELIMINADO DE MANERA SEGURA, ANTES DE DESHACERSE DE ELLOS
11.2.8	EQUIPO DE USUARIO DESATENDIDO	**CONTROL**: LOS USUARIOS DEBERÍAN ASEGURARSE QUE EL EQUIPO DESATENDIDO TIENE LA PROTECCIÓN ADECUADA
11.2.9	POLÍTICA DE PUESTO DE TRABAJO DESPEJADO Y PANTALLA LIMPIA	**CONTROL**: DEBERÍA ADOPTARSE UNA POLÍTICA DE PUESTO DE TRABAJO DESPEJADO DE PAPELES Y MEDIOS DE ALMACENAMIENTO DESMONTABLES Y UNA POLÍTICA DE PANTALLA LIMPIA PARA LOS RECURSOS DE TRATAMIENTO DE LA INFORMACIÓN

Fuente: ISO 27002:2013 (AENOR, (2015))

E. Seguridad lógica

La seguridad lógica va de la mano con la seguridad física, porque es sumamente importante para la seguridad de la información. Ante ello, se requiere que la seguridad lógica, proteja a la información durante su tránsito en la red de la organización. Algunas organizaciones no tienen segura a la información, porque no toman conciencia sobre los daños o pérdidas que podría ocasionar si se infecta o pierde la información, se debe tomar medidas que en conjunto con la seguridad física para que protejan la información de la organización.

La norma ISO/IEC 27002:2013 contiene controles que están asociados a la seguridad lógica, es por ello que te indica cuáles son los parámetros que requiere para que la información se encuentre confiable y segura cuando esta llegue a su destinatario.

A continuación, de la Tabla 5 a la Tabla 9 se muestran los controles de seguridad lógica de la ISO/IEC 27002:2013.

En la Tabla 5 se muestra todo el contenido del Dominio 9, del cual, para nuestra implementación, se tomó gran parte del objetivo de control 9.2, en los que se tomaron los controles: 9.2.1, 9.2.2, 9.2.3, 9.2.5, 9.2.6, además del control 9.4.2 para la implementación.

Tabla 5:
Objetivos de control y controles del dominio 9

9. CONTROL DE ACCESO		
9.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO **OBJETIVO**: LIMITAR EL ACCESO A LOS RECURSOS DE TRATAMIENTO DE INFORMACIÓN Y A LA INFORMACIÓN		
9.1.1	POLÍTICA DE CONTROL DE ACCESO	**CONTROL** SE DEBERÍA ESTABLECER, DOCUMENTAR Y REVISAR UNA POLÍTICA DE CONTROL DE ACCESO BASADA EN LOS REQUISITOS DE NEGOCIO Y DE SEGURIDAD DE LA INFORMACIÓN
9.1.2	ACCESO A LAS REDES Y A LOS SERVICIOS DE RED	**CONTROL**: ÚNICAMENTE SE DEBERÍA PROPORCIONAR A LOS USUARIOS EL ACCESO A LAS REDES Y A LOS SERVICIOS DE EN RED PARA CUYO USO HAYAN SIDO ESPECÍFICAMENTE AUTORIZADOS
9.2 GESTIÓN DE ACCESO DE USUARIO **OBJETIVO**: GARANTIZAR EL ACCESO DE USUARIOS AUTORIZADOS Y EVITAR EL ACCESO NO AUTORIZADO A LOS SISTEMAS Y SERVICIOS.		
9.2.1	REGISTRO Y BAJA DE USUARIO	**CONTROL**: DEBERÍA IMPLANTARSE UN PROCEDIMIENTO FORMAL DE REGISTRO Y RETIRADA DE USUARIOS QUE HAGA POSIBLE LA ASIGNACIÓN DE LOS DERECHOS DE ACCESO

9.2.2	Provisión de acceso de usuarios	**Control**: Debería implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios
9.2.3	Gestión de privilegios de acceso	**Control**: La asignación y el uso de privilegios de acceso debería estar restringida y controlada
9.2.4	Gestión de la información secreta de autenticación de los usuarios	**Control**: La asignación de la información secreta de autenticación debería ser controlada a través de un proceso formal de gestión
9.2.5	Revisión de los derechos de acceso de usuarios	**Control**: Los propietarios de los activos deberían revisar los derechos de acceso de usuarios a intervalos regulares
9.2.6	Retirada o reasignación de los derechos de acceso	**Control**: Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deberían ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio
9.3 Responsabilidades del usuario		
Objetivo: Para que los usuarios se hagan responsables de salvaguardar su información de autenticación		
9.3.1	Uso de la información secreta de autenticación	**Control**: Se debería requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación
9.4 Control de acceso a sistemas y aplicaciones		
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones		
9.4.1	Restricción del acceso a la información	**Control**: Se debería restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida
9.4.2	Procedimientos seguros de inicio de sesión	**Control**: Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debería controlar por medio de un procedimiento seguro de inicio de sesión
9.4.3	Sistema de gestión de contraseñas	**Control**: Los sistemas para la gestión de contraseñas deberían ser interactivos y establecer contraseñas seguras y robustas
9.4.4	Uso de utilidades con privilegios del sistema	**Control**: Se debería restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación
9.4.5	Control de acceso al código fuente de los programas	**Control**: Se debería restringir el acceso al código fuente de los programas

Fuente: ISO 27002:2013 (AENOR, (2015))

En la Tabla 6 se muestra todo el contenido del Dominio 10 con su respectivo objetivo de control y controles.

Tabla 6:
Objetivos de control y controles del dominio 10

10. CRIPTOGRAFÍA		
10.1 CONTROLES CRIPTOGRÁFICOS OBJETIVO: GARANTIZAR UN USO ADECUADO Y EFICAZ DE LA CRIPTOGRAFÍA PARA PROTEGER LA CONFIDENCIALIDAD, AUTENTICIDAD Y/O INTEGRIDAD DE LA INFORMACIÓN		
10.1.1	POLÍTICA DE USO DE LOS CONTROLES CRIPTOGRÁFICOS	**CONTROL**: SE DEBERÍA DESARROLLAR E IMPLEMENTAR UNA POLÍTICA SOBRE EL USO DE LOS CONTROLES CRIPTOGRÁFICOS PARA PROTEGER LA INFORMACIÓN
10.1.2	GESTIÓN DE CLAVES	**CONTROL**: SE DEBERÍA DESARROLLAR E IMPLEMENTAR UNA POLÍTICA DE SOBRE EL USO, LA PROTECCIÓN Y LA DURACIÓN DE LAS CLAVES DE CIFRADO A LO LARGO DE TODO SU CICLO DE VIDA

Fuente: ISO 27002:2013 (AENOR, (2015))

En la Tabla 7 se muestra todo el contenido del Dominio 12, del cual, para nuestra implementación, se consideraron los controles 12.2.1 y 12.6.1

Tabla 7:
Objetivos de control y controles del dominio 12

12. SEGURIDAD DE LAS OPERACIONES		
12.1 PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES OBJETIVO: ASEGURAR EL FUNCIONAMIENTO CORRECTO Y SEGURO DE LAS INSTALACIONES DE TRATAMIENTO DE LA INFORMACIÓN		
12.1.1	DOCUMENTACIÓN DE PROCEDIMIENTOS DE LAS OPERACIONES	**CONTROL**: DEBERÍAN DOCUMENTARSE Y MANTENERSE PROCEDIMIENTOS DE OPERACIÓN Y PONERSE A DISPOSICIÓN DE TODOS LOS USUARIOS QUE LOS NECESITEN
12.1.2	GESTIÓN DE CAMBIOS	**CONTROL**: LOS CAMBIOS EN LA ORGANIZACIÓN, LOS PROCESOS DE NEGOCIO, INSTALACIONES DE TRATAMIENTO DE LA INFORMACIÓN Y LOS SISTEMAS QUE AFECTEN A LA SEGURIDAD DE INFORMACIÓN DEBERÍAN SER CONTROLADOS
12.1.3	GESTIÓN DE CAPACIDADES	**CONTROL**: SE DEBERÍA SUPERVISAR Y AJUSTAR LA UTILIZACIÓN DE LOS RECURSOS, ASÍ COMO REALIZAR PROYECCIONES DE LOS REQUISITOS FUTUROS DE CAPACIDAD, PARA GARANTIZAR EL RENDIMIENTO REQUERIDO DEL SISTEMA
12.1.4	SEPARACIÓN DE LOS RECURSOS DE DESARROLLO, PRUEBA Y OPERACIÓN	**CONTROL**: DEBERÍAN SEPARARSE LOS RECURSOS DE DESARROLLO, PRUEBAS Y OPERACIÓN, PARA REDUCIR LOS RIESGOS DE ACCESO NO AUTORIZADO O LOS CAMBIOS DEL SISTEMA EN PRODUCCIÓN
12.2 PROTECCIÓN CONTRA EL SOFTWARE MALICIOSO(MALWARE) OBJETIVO: ASEGURAR QUE LOS RECURSOS DE TRATAMIENTO DE LA INFORMACIÓN Y LA INFORMACIÓN ESTÁN PROTEGIDOS CONTRA EL MALWARE		
12.2.1	CONTROLES CONTRA EL CÓDIGO MALICIOSO	**CONTROL**: SE DEBERÍAN IMPLEMENTAR LOS CONTROLES DE DETECCIÓN, PREVENCIÓN Y RECUPERACIÓN QUE SIRVAN COMO PROTECCIÓN CONTRA EL CÓDIGO MALICIOSO, ASÍ COMO LOS PROCEDIMIENTOS ADECUADOS DE CONCIENCIACIÓN AL USUARIO

12.3 Copias de seguridad Objetivo: Evitar la pérdida de datos		
12.3.1	Copias de seguridad de la información	**Control**: Se deberían realizar copias de seguridad de la información, del software y del sistema y se deberían verificar periódicamente de acuerdo a la política de copias de seguridad acordada
12.4 Registros y supervisión Objetivo: Registrar eventos y generar evidencias		
12.4.1	Registro de eventos	**Control**: Se deberían registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información
12.4.2	Protección de la información de registro	**Control**: Los dispositivos de registro y la información del registro deberían estar protegidos contra manipulaciones indebidas y accesos no autorizados
12.4.3	Registro de administración y operación	**Control**: Se deberían registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.
12.4.4	Sincronización del reloj	**Control**: Los relojes de todos los sistemas de tratamiento de información dentro de una organización o de un dominio de seguridad, deberían estar sincronizados con una única fuente precisa y acordada de tiempo
12.5 Control de software en explotación Objetivo: Asegurar la integridad del software en explotación		
12.5.1	Instalación del software en explotación	**Control**: Se deberían implementar procedimientos para controlar la instalación del software en explotación
12.6 Gestión de la vulnerabilidad técnica Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas		
12.6.1	Gestión de las vulnerabilidades técnicas	**Control**: Se debería obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado
12.6.2	Restricción en la instalación de software	**Control**: Se deberían establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios
12.7 Consideraciones sobre la auditoria de sistemas de información Objetivo: Minimizar el impacto de las actividades de auditoria en los sistemas operativos		
12.7.1	Controles de auditoria de sistemas de información	**Control**: Los requisitos y las actividades de auditoria que implique comprobaciones en los sistemas operativos deberían ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio

Fuente: ISO 27002:2013 (AENOR, (2015))

En la Tabla 8 se muestra todo el contenido del Dominio 13 con sus respectivos objetivos de control y controles.

Tabla 8:
Objetivos de control y controles del dominio 13

13. SEGURIDAD DE LAS COMUNICACIONES		
13.1 GESTIÓN DE LA SEGURIDAD DE REDES OBJETIVO: ASEGURAR LA PROTECCIÓN DE LA INFORMACIÓN EN LAS REDES Y LOS RECURSOS DE TRATAMIENTO DE LA INFORMACIÓN		
13.1.1	CONTROLES DE RED	**CONTROL**: LAS REDES DEBERÍAN SER GESTIONADAS Y CONTROLADAS PARA PROTEGER LA INFORMACIÓN EN LOS SISTEMAS Y APLICACIONES
13.1.2	SEGURIDAD DE LOS SERVICIOS DE RED	**CONTROL**: SE DEBERÍAN IDENTIFICAR LOS MECANISMOS DE SEGURIDAD, LOS NIVELES DE SERVICIO, Y LOS REQUISITOS DE GESTIÓN DE TODOS LOS SERVICIOS DE RED Y SE DEBERÍAN INCLUIR EN CUALQUIER ACUERDO DE SERVICIOS DE RED, TANTO SI ESTOS SERVICIOS SE PRESTAN DENTRO DE LA ORGANIZACIÓN COMO SI SE SUBCONTRATAN
13.1.3	SEGREGACIÓN EN REDES	**CONTROL**: LOS GRUPOS DE SERVICIOS DE INFORMACIÓN, LOS USUARIOS Y LOS SISTEMAS DE INFORMACIÓN DEBERÍAN ESTAR SEGREGADOS EN REDES DISTINTAS
13.2 INTERCAMBIO DE INFORMACIÓN OBJETIVO: MANTENER LA SEGURIDAD EN LA INFORMACIÓN QUE SE TRANSFIERE DENTRO DE UNA ORGANIZACIÓN Y CON CUALQUIER ENTIDAD EXTERNA		
13.2.1	POLÍTICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACIÓN	**CONTROL**: DEBERÍAN ESTABLECERSE POLÍTICAS, PROCEDIMIENTOS Y CONTROLES FORMALES QUE PROTEJAN EL INTERCAMBIO DE INFORMACIÓN MEDIANTE EL USO DE TODO TIPO DE RECURSOS DE COMUNICACIÓN
13.2.2	ACUERDOS DE INTERCAMBIO DE INFORMACIÓN	**CONTROL**: DEBERÍAN ESTABLECERSE ACUERDOS PARA EL INTERCAMBIO SEGURO DE INFORMACIÓN DEL NEGOCIO Y SOFTWARE ENTRE LA ORGANIZACIÓN Y TERCEROS
13.2.3	MENSAJERÍA ELECTRÓNICA	**CONTROL**: LA INFORMACIÓN QUE SEA OBJETO DE MENSAJERÍA ELECTRÓNICA DEBERÍA ESTAR ADECUADAMENTE PROTEGIDA
13.2.4	ACUERDOS DE CONFIDENCIALIDAD O NO REVELACIÓN	**CONTROL**: DEBERÍAN IDENTIFICARSE, DOCUMENTARSE Y REVISARSE REGULARMENTE LOS REQUISITOS DE LOS ACUERDOS DE CONFIDENCIALIDAD O NO REVELACIÓN

Fuente: ISO 27002:2013 (AENOR, (2015))

En la Tabla 9 se muestra todo el contenido del Dominio 14 con sus respectivos objetivos de control y controles.

Tabla 9:
Objetivos de control y controles del dominio 14

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN		
14.1 REQUISITOS DE SEGURIDAD EN SISTEMAS DE INFORMACIÓN **OBJETIVO**: GARANTIZAR QUE LA SEGURIDAD DE LA INFORMACIÓN SEA PARTE INTEGRAL DE LOS SISTEMAS DE INFORMACIÓN A TRAVÉS DE TODO EL CICLO DE VIDA. ESTO TAMBIÉN INCLUYE LOS REQUISITOS PARA LOS SISTEMAS DE INFORMACIÓN QUE PROPORCIONAN LOS SERVICIOS A TRAVÉS DE REDES PUBLICAS		
14.1.1	ANÁLISIS DE REQUISITOS Y ESPECIFICACIONES DE SEGURIDAD DE LA INFORMACIÓN	**CONTROL**: LOS REQUISITOS RELACIONADOS CON LA SEGURIDAD DE LA INFORMACIÓN DEBERÍAN INCLUIRSE EN LOS REQUISITOS PARA LOS NUEVOS SISTEMAS DE INFORMACIÓN O MEJORAS A LOS SISTEMAS DE INFORMACIÓN EXISTENTES
14.1.2	ASEGURAR LOS SERVICIOS DE APLICACIONES EN REDES PÚBLICAS	**CONTROL**: LA INFORMACIÓN INVOLUCRADA EN APLICACIONES QUE PASAN A TRAVÉS DE REDES PÚBLICAS DEBERÍA SER PROTEGIDA DE CUALQUIER ACTIVIDAD FRAUDULENTA, DISPUTA DE CONTRATO, REVELACIÓN Y MODIFICACIÓN NO AUTORIZADAS
14.1.3	PROTECCIÓN DE LAS TRANSACCIONES DE SERVICIOS DE APLICACIONES	**CONTROL:** LA INFORMACIÓN INVOLUCRADA EN LAS TRANSACCIONES DE SERVICIOS DE APLICACIONES DEBERÍA SER PROTEGIDA PARA PREVENIR LA TRANSMISIÓN INCOMPLETA, ERRORES DE ENRUTAMIENTO, ALTERACIÓN NO AUTORIZADA DEL MENSAJE, REVELACIÓN, DUPLICACIÓN, O REPRODUCCIÓN DE MENSAJE NO AUTORIZADAS
14.2 SEGURIDAD EN EL DESARROLLO Y EN LOS PROCESOS DE SOPORTE **OBJETIVO**: GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN QUE SE HA DISEÑADO E IMPLEMENTADO EN EL CICLO DE VIDA DE DESARROLLO DE SISTEMAS DE INFORMACIÓN		
14.2.1	POLÍTICA DE DESARROLLO SEGURO	**CONTROL**: SE DEBERÍAN ESTABLECER Y APLICAR REGLAS DENTRO DE LA ORGANIZACIÓN PARA EL DESARROLLO DE APLICACIONES Y SISTEMAS
14.2.2	PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS	**CONTROL**: LA IMPLANTACIÓN DE CAMBIOS A LO LARGO DEL CICLO DE VIDA DEL DESARROLLO DEBERÍA CONTROLARSE MEDIANTE EL USO DE PROCEDIMIENTOS FORMALES DE CONTROL DE CAMBIOS
14.2.3	REVISIÓN TÉCNICA DE LAS APLICACIONES TRAS EFECTUAR CAMBIOS EN EL SISTEMA OPERATIVO	**CONTROL**: CUANDO SE MODIFIQUEN LOS SISTEMAS OPERATIVOS, LAS APLICACIONES DE NEGOCIO CRITICAS DEBERÍAN SER REVISADAS Y PROBADAS PARA GARANTIZAR QUE NO EXISTEN EFECTOS ADVERSOS EN LAS OPERACIONES O LA SEGURIDAD DE LA ORGANIZACIÓN
14.2.4	RESTRICCIONES A LOS CAMBIOS EN LOS PAQUETES DE SOFTWARE	**CONTROL**: SE DEBERÍAN DESACONSEJAR LAS MODIFICACIONES EN LOS PAQUETES DE SOFTWARE, LIMITÁNDOSE A LOS CAMBIOS NECESARIOS, Y TODOS LOS CAMBIOS DEBERÍAN SER OBJETO DE UN CONTROL RIGUROSO
14.2.5	PRINCIPIOS DE INGENIERÍA DE SISTEMAS SEGUROS	**CONTROL**: PRINCIPIOS DE INGENIERÍA DE SISTEMAS SEGUROS SE DEBERÍAN ESTABLECER, DOCUMENTAR, MANTENER Y APLICARSE A TODOS LOS ESFUERZOS DE IMPLANTACIÓN DE SISTEMAS DE INFORMACIÓN
14.2.6	ENTORNO DE DESARROLLO SEGURO	**CONTROL**: LAS ORGANIZACIONES DEBERÍAN ESTABLECER Y PROTEGER ADECUADAMENTE LOS ENTORNOS DE DESARROLLO SEGURO PARA EL DESARROLLO DEL SISTEMA Y LOS ESFUERZOS DE INTEGRACIÓN QUE CUBREN TODO EL CICLO DE VIDA DE DESARROLLO DEL SISTEMA

14.2.7	EXTERNALIZACIÓN DEL DESARROLLO DE SOFTWARE	**CONTROL**: EL DESARROLLO DE SOFTWARE EXTERNALIZADO DEBERÍA SER SUPERVISADO Y CONTROLADO POR LA ORGANIZACIÓN
14.2.8	PRUEBAS FUNCIONALES DE SEGURIDAD DE SISTEMAS	**CONTROL**: SE DEBERÍAN LLEVAR A CABO PRUEBAS DE LA SEGURIDAD FUNCIONAL DURANTE EL DESARROLLO
14.2.9	PRUEBAS DE ACEPTACIÓN DE SISTEMAS	**CONTROL**: SE DEBERÍAN ESTABLECER PROGRAMAS DE PRUEBAS DE ACEPTACIÓN Y CRITERIOS RELACIONADOS PARA NUEVOS SISTEMAS DE INFORMACIÓN, ACTUALIZACIONES Y NUEVAS VERSIONES
14.3 DATOS DE PRUEBA **OBJETIVO**: ASEGURAR LA PROTECCIÓN DE LOS DATOS DE PRUEBA		
14.3.1	PROTECCIÓN DE LOS DATOS DE PRUEBA	**CONTROL**: LOS DATOS DE PRUEBA SE DEBERÍAN SELECCIONAR CON CUIDADO Y DEBERÍAN SER PROTEGIDOS Y CONTROLADOS

Fuente: ISO 27002:2013 (AENOR, (2015))

2.2.2. Mejora del Nivel de la Seguridad Física y Lógica de la Información.

2.2.2.1. Auditoría con el framework COBIT 5.

La auditoría es una herramienta que te permite conocer el estado actual y final de la organización, la cual consiste obtener los resultados de los procesos que están siendo desarrollados por la entidad, estos resultados de la auditoría se conocen mediante un instrumento de evaluación donde indica las deficiencias y eficiencias de los procesos.

Uno de los framework que se asocia a la medición y evaluación de los procesos, es COBIT 5, la cual contiene procesos que están relacionados con la seguridad de la información y otros aspectos de seguridad, las organizaciones deben establecer los problemas que afectan las áreas donde se maneja la información, y adjudicar mediante un análisis que proceso cumple con las falencias encontradas en ellas.

COBIT 5 es un marco de referencia de negocio para la gestión y el gobierno de las Tecnologías de Información de la organización, de modo que ayuda a estas a conseguir sus objetivos para el gobierno y la gestión de TI. Además de ayudar a crear el valor óptimo desde TI, a través de la generación de beneficios, optimización de niveles de riesgo y el uso de recursos. Teniendo en consideración lo anterior, se podría decir que el COBIT 5 ayuda o apoya a las organizaciones a establecer un valor óptimo a partir de TI, manteniendo un

equilibrio entre la optimización de los niveles de riesgo, la realización de beneficios y la utilización de los recursos. En lo que concierne al gobierno de TI contiene 5 procesos y en lo que respeta a Gestión de TI encierra 32 procesos organizados separados en 4 dominios.

En la Figura 3 se muestra los 37 procesos de COBIT tanto para lo que abarcan en gestión de TI como para gobierno de TI.

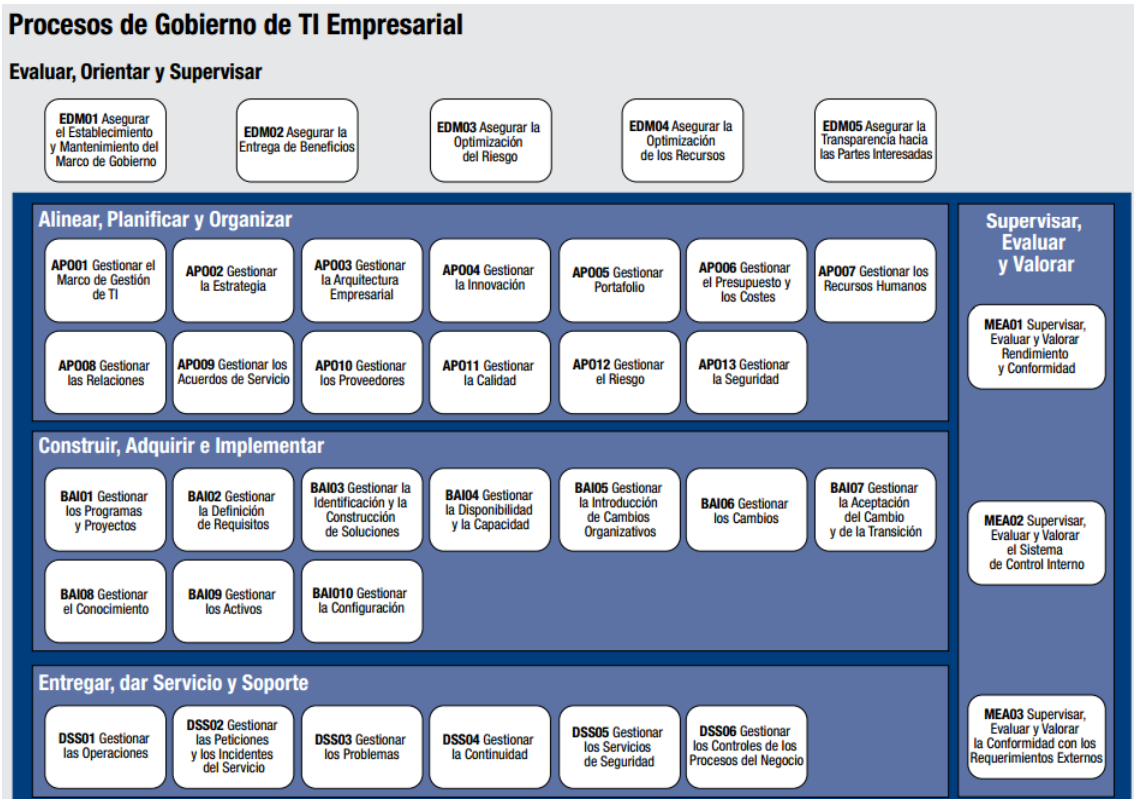


Figura 3: Procesos de Cobit ***(Fuente:*** ISACA (2012)***)***

A. Aspectos de seguridad

- APO13 Gestionar la seguridad (pertenece al proceso treceavo del dominio Alinear, Planificar y Organizar)
- DSS04 Gestionar la Continuidad (pertenece al cuarto proceso del dominio Entregar, dar Servicio y Soporte)
- **DSS05 Gestionar los servicios de seguridad (pertenece al quinto proceso del dominio Entregar, dar Servicio y Soporte)** Mendoza (2015)

- **DSS05 - Gestionar los servicios de seguridad**

Este proceso tiene el propósito de salvaguardar la información de la empresa para preservar correctamente el nivel de riesgo de la seguridad de la información de acuerdo con la política de seguridad. Establece y mantiene los roles de seguridad, como los privilegios de accesos a la información y el de realizar la supervisión de la seguridad

En la Figura 4 se aprecia el proceso COBIT DSS05 – "Gestionar los servicios de Seguridad" y sus 7 prácticas de gestión, la que se consideró para la realización de la investigación.

Figura 4*:* Proceso COBIT y sus prácticas de gestión *(**Fuente**:* ISACA (2012)*)*

❖ **DSS05.01 – "Protección contra software malicioso (Malware)"**

Esta práctica de gestión implementa y mantiene de manera efectiva como preventiva las medidas de detección, además de estar correctivas (básicamente control de virus y parches actualizados de seguridad) a lo largo de la empresa para salvaguardar los sistemas de

información y las tecnologías de softwares maliciosos (algunos ejemplos: correo basura, gusanos, virus, software espía - spyware)

- **DSS05.02 – "Gestionar la seguridad de la red y las conexiones"**

Emplea medidas de seguridad, además de procedimientos de gestión que estén relacionados para la protección de la información en cada uno de los modos de conexión.

- **DSS05.03 – "Gestionar la seguridad de los puestos de usuario final"**

Garantiza que los puestos de usuario final (se puede decir, equipo sobremesa, portátil, servidor y otros equipos, softwares móviles y de red) estén salvaguardados a un nivel que es mayor o igual al que se encuentra definido en los requerimientos de seguridad de la información almacenada, transmitida o procesada.

- **DSS05.04 – "Gestionar la identidad del usuario y el acceso lógico"**

Garantiza que cada uno de los usuarios tenga el derecho de acceso a la información, esto en función a los requerimientos de negocio, y acordar con las unidades de negocio que administren sus propios derechos de acceso hacia los procesos de negocio.

- **DSS05.05 – "Gestionar el acceso físico a los activos de TI"**

Implementa y define procedimientos para limitar, conceder y anular el acceso a edificios, áreas, locales, de acuerdo a las necesidades del negocio, incluyendo emergencias. El acceso a edificios, áreas y locales necesita estar autorizado, justificado, supervisado y registrado. Esto se aplicará a todas las personas que ingresen en los locales, incluyendo los empleados, clientes, empleados temporales, visitantes, vendedores y cualquier persona.

- **DSS05.06 – "Gestionar documentos sensibles y dispositivos de salida"**

Esta práctica de gestión implementa protecciones físicas adecuadas, para el desarrollo de las prácticas de contabilidad y la gestión de inventario, que contiene los activos sensibles de TI. Tales como títulos negociables, formularios especiales, credenciales de seguridad o impresoras de propósito especial.

❖ **DSS05.07 – "Supervisar la infraestructura para detectar eventos relacionado con la seguridad"**

Emplea herramientas de localización de intrusiones, registra la infraestructura para la detección de accesos no autorizados, y manifiesta que cualquier evento esté integrado con el registro general de eventos y gestión de incidentes.

B. Modelo de Evaluación de Procesos (PAM)

El Modelo de Evaluación de Procesos (PAM) de COBIT está diseñado para proveer a las empresas con una metodología reproducible, confiable y robusta para evaluar la capacidad de sus procesos de TI. Dichas evaluaciones normalmente se usan como parte de un programa de mejora de los procesos de una empresa y también se pueden utilizar para informar internamente a la dirección ejecutiva o la junta directiva de una empresa sobre la capacidad actual de sus procesos de TI.

- **Niveles de capacitación de los procesos**

El PAM tiene 6 niveles para evaluar la capacidad de los procesos de COBIT, tal como se muestra en la Figura 5.

Nivel del proceso	Capacitación
0 (Incompleto)	El proceso no se encuentra implementado o falla en conseguir el objetivo del proceso. A este nivel, hay poca o ninguna evidencia de un proceso sistematizado para la consecución de los objetivos del proceso.
1 (Ejecutado)	Un proceso implementado consigue el propósito del proceso.
2 (Gestionado)	El proceso ejecutado ahora es implementado de forma gestionada (planificada, monitorizada y ajustada) y los resultados son adecuadamente establecidos, controlados y mantenidos.
3 (Establecido)	El proceso gestionado ahora es implementado utilizando un proceso definido que permite conseguir los resultados del proceso.
4 (Predecible)	Un proceso establecido, opera en los límites definidos, para a conseguir los resultados del proceso.
5 (Optimizado)	Un proceso predecible, es continuamente mejorado para alcanzar los objetivos del negocio actuales y futuras.

Figura 5: Niveles de capacidad de los procesos COBIT
***(Fuente*:** COBIT 5 (ISACA (2013)))

El nivel 0 muestra que un proceso no está implementado o que falla en el objetivo de conseguir sus resultados.

Nivel de capacidad 1- Los indicadores son claros para cada proceso y evalúan como se han conseguido los atributos siguientes: El proceso consigue su propósito.

Niveles de capacidad 2 al 5 – Aquí la evaluación se basa en indicadores genérico de rendimiento del proceso. A ellos se identifican como genéricos puesto que se aplican a todo el proceso de una forma transversal, pero diferentes en los distintos niveles de capacidad.

- **Escala de calificación**

Esta escala es utilizada por los evaluadores con el propósito que guiar en la determinación, que a su juicio, es el grado de consecución. En la Figura 6 se describen cada uno de los tipos de las calificaciones y su traduccion de estas en un escala de porcentajes que permiten mostrar el grado de consecución.

N	No conseguido	0 a 15% de consecución
P	Parcialmente conseguido	>15% al 50% de consecución
L	Ampliamente conseguido	>50% al 85% de consecución
F	Totalmente conseguido	>85% al 100% de consecución

Figura 6: Escala de calificación ***(Fuente:*** COBIT 5 (ISACA (2013)))

- N (No Conseguido o Logrado): "Hay poca o ninguna evidencia de logro del atributo definido en el proceso evaluado."
- P (Parcialmente Conseguido o Logrado): "Existe alguna evidencia de un enfoque y algún logro de, el atributo definido en el proceso evaluado. Algunos aspectos de los logros del atributo pueden ser impredecibles."
- L (Ampliamente Conseguido o Logrado): "Hay evidencia de un enfoque sistemático y el logro significativo de, el atributo definido en el proceso de evaluación. Algunas debilidades relacionadas con este atributo pueden existir en el proceso evaluado."
- F (Totalmente Conseguido o Logrado): "Hay evidencia de un enfoque completo y sistemático y la plena consecución de, el atributo definido en el proceso evaluado. No existen debilidades significativas relacionadas con este atributo en el proceso evaluado."

- **Criterios de evaluación del proceso Cobit**

El proceso COBIT DSS05 – Gestionar los servicios de seguridad, cuenta con 5 criterios de evaluación para las 7 prácticas del proceso, estas 7 prácticas se asocian logrando

medir los niveles que alcanza en base a los atributos del proceso y en función de los atributos de los niveles inferiores que han sido completamente conseguidos. A continuación, en la Figura 7 se muestra los 5 criterios del proceso asociados con las 7 prácticas de gestión.

Número	Descripción	
DSS05-01	Satisfacer las necesidades del negocio respecto a la seguridad de redes y comunicaciones.	
DSS05-02	La información procesada en, almacenada en y transmitida por medio de dispositivos de punto final está protegida.	
DSS05-03	Todos los usuarios tienen un único identificador y los derechos de acceso acordes con su función en la empresa.	
DSS05-04	Se han implementado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias al ser procesada, almacenada o transmitida.	
DSS05-05	La información electrónica se ha asegurado correctamente cuando se almacena, transmite o destruye.	
Prácticas Base (BPs)		
Número	**Descripción**	**Soporta**
DSS05-BP1	**Protección contra el malware.** Implementar y mantener medidas preventivas, detectivas y correctivas (especialmente hasta actualizar los parches de seguridad y de control de virus) en toda la empresa para proteger los sistemas de información y tecnología de software malicioso (por ejemplo, virus, gusanos, software espía, correo no deseado).	DSS05-01/02
DSS05-BP2	**Administrar la seguridad de la red y la conectividad.** Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los sistemas de conectividad.	DSS05-01
DSS05-BP3	**Administrar la seguridad del punto final.** Asegurar que los puntos finales (por ejemplo, ordenadores portátiles, de escritorio, servidores y otros dispositivos móviles y de red o software) están securizados con un nivel igual o superior que los requisitos de seguridad definidos para la información procesada, almacenada o transmitida.	DSS05-02
DSS05-BP4	**Administrar la identidad de usuarios y accesos lógicos.** Asegurar que todos los usuarios tienen derechos de acceso a la información acordes con sus requisitos de negocio y coordinarse con las unidades que gestionan sus propios derechos de acceso en los procesos de negocio.	DSS05-03
DSS05-BP5	**Administrar el acceso físico a los activos de TI.** Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluidas emergencias. El acceso a los locales, edificios y áreas debe justificarse, autorizarse, registrarse y supervisarse. Esto debería aplicarse a todas las personas que entran en los locales, incluidos personal interno, personal temporal, clientes, proveedores, visitantes o cualquier tercero.	DSS05-04
DSS05-BP6	**Administrar documentos sensibles y dispositivos de salida.** Establecer protecciones físicas apropiadas, prácticas de contabilidad y una gestión de inventario sobre activos sensibles de TI como formularios especiales, instrumentos negociables, impresoras de propósito especial o tokens de seguridad.	DSS05-05
DSS05-BP7	**Supervisar la infraestructura de eventos relacionados con seguridad.** Uso de herramientas de detección de intrusiones, supervisión de la infraestructura ante accesos no autorizados y asegurar que los eventos se integran en la supervisión general de eventos y la gestión de incidentes.	DSS05-01

Figura 7: Criterios del proceso asociados con las prácticas de gestión
***(Fuente*:** COBIT 5 (ISACA (2013)))

2.2.2.2. Norma ISO 27005.

A. Introducción

Según Baca (2016), "La ISO 27005 establece las directrices para la gestión del riesgo en la seguridad de la información, además de que también apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos".

Hasta el momento, el marco que existe para la gestión de riesgos lo conforma el estándar ISO 27005. Se puede utilizar diferentes metodologías que existen bajo la estructura descrita. En esta norma para implementarlos, se requiere de un sistema de gestión de seguridad de la información.

Esta norma es oportuna para cada uno de los directores y el personal que tiene relación con la gestión del riesgo en la seguridad de la información dentro de una organización, y cuando corresponda, para las partes externas que dan soporte a dichas actividades.

B. Objeto y campo de aplicación

- Esta norma proporciona criterios para la gestión en la seguridad de la información.
- Esta norma brinda soporte a los distintos conceptos que se especifican en la norma ISO 27001.
- Esta norma está diseñada para proporcionar la implementación satisfactoria de la seguridad de la información con base en el enfoque de gestión de riesgo
- Todos los conceptos que se mencione en las normas ISO/IEC 27001 e ISO/IEC 27002 es importante para su comprensión de esta norma
- Esta norma se puede emplear a diferentes tipos de organizaciones que exista en todo el mundo como (empresas pequeñas, agencias del gobierno, empresas sin ánimo de lucro)

C. Análisis de riesgo

Según Moreno (2008), el análisis de riesgo es la herramienta que ayuda a identificar a las amenazas y vulnerabilidades que se encuentran en los activos de información, teniendo una valoración por riesgo minimizando, el impacto que podría ocasionar en la organización. La Figura 8 se puede apreciar la secuencia de pasos para realizar el análisis de riesgo que describe la norma.

Figura 8: Análisis de Riesgo *(**Fuente**:* Elaboración propia*)*

- **Identificación de activos**

➢ Un activo es aquel que tiene un valor importante para la organización, por ello se necesita protegerlo ante cualquier amenaza que pueda surgir.

➢ La identificación del activo consta de un análisis detallado que permite tener la información exacta de cada activo encontrado en la organización, este análisis contiene el tipo de activo, el propietario que está a cargo del activo y la localización donde se encuentra el activo, logrando tener la responsabilidad necesaria para el desarrollo, mantenimiento, uso y seguridad según corresponda al análisis que se realizó.

- **Identificación de amenazas**

➢ La amenaza tiene la capacidad de perjudicar y/o eliminar a los activos que se encuentran dentro de la organización. Las amenazas suelen ser de tipo natural o humano y podría ser accidental o deliberada.

➢ La identificación de las amenazas y la estimación de probabilidad de ocurrencia se logra conseguir de acuerdo a los usuarios del activo, al personal de recursos humanos y al jefe de las instalaciones, que sean expertos en seguridad física y otras organizaciones que incluyen organismos legales.

- **Identificación de vulnerabilidades**

➢ La vulnerabilidad que no tiene una amenaza, puede que no necesariamente tenga que recurrir a la implementación de los controles, pero se recomienda que se analice y se monitoree para ver los cambios que tuvo.

➢ Una vulnerabilidad también se relaciona con los activos de la organización para así determinar cuáles son los riesgos que necesita ser reducido. Se puede identificar vulnerabilidades en las siguientes áreas, tal como se aprecia en la Figura 9.

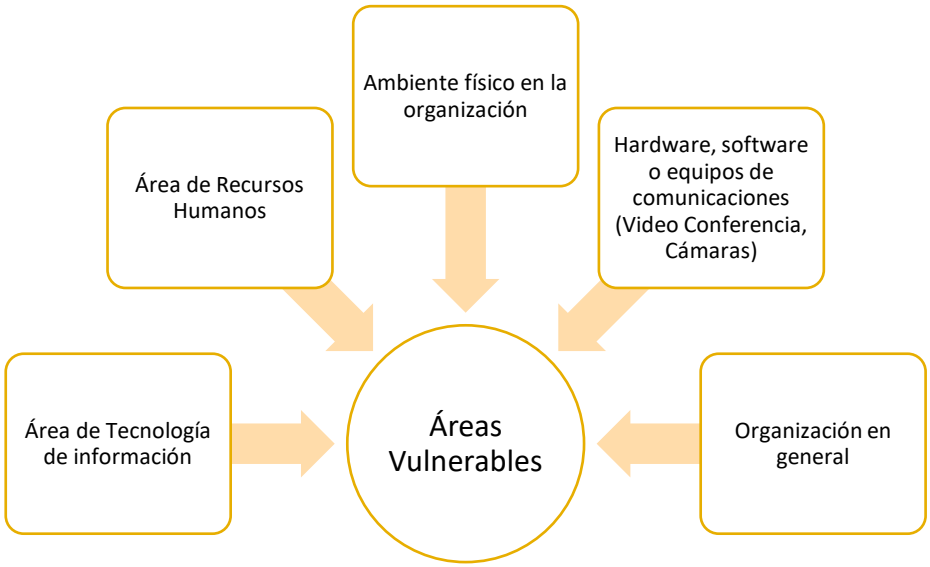


Figura 9: Áreas Vulnerables *(**Fuente**:* Moreno (2008)*)*

- **Identificación de riesgo**

El propósito de la identificación del riesgo es establecer cómo podría originarse una pérdida potencial, llegando a percibir el cómo, dónde y por qué podría ocurrir esta pérdida. Para lograr los pasos que se menciona anteriormente se tiene que analizar al detalle los datos de los activos encontrados para la actividad de estimación de riesgo.

2.2.2.3. Plan de tratamiento de riesgo.

El plan de tratamiento de riesgo, es la parte más compleja, la cual la organización debe conocer, porque estipula el tiempo que se desarrollará, y que controles de la norma ISO/IEC 27002:2013 implementar, es importante tener conocimiento del plan porque permite controlar el cumplimiento de los controles.

Las organizaciones deben estipular su plan de tratamiento de riesgo para conocer los factores principales que permitan minimizar los riesgos que se encuentran en cualquier entidad organizativa.

A. Tratamiento del riesgo en la seguridad de la información

- **Descripción del tratamiento de riesgo**

- Para el tratamiento del riesgo se necesita tener una lista de los riesgos priorizados para analizar su valor por cada riesgo (sea el impacto o el costo del riesgo), estableciendo un plan de tratamiento del riesgo para su reducción.
- Para el tratamiento de riesgo existen 4 opciones las cuales son: aceptación del riesgo, reducción del riesgo, transferencia del riesgo y evitación del riesgo.
- En algunos casos un tratamiento de riesgo puede tratar eficazmente más de un riesgo.
- En el caso de que en el análisis del tratamiento de riesgo se indica las opciones transferir, evadir y aceptar es recomendable no colocar los controles de la norma, solo en el caso que la opción sea reducir se implementa los controles que la norma menciona.

En la Figura 10 se grafica las actividades que se deben optar para el tratamiento del riesgo, tal como lo describe la norma.

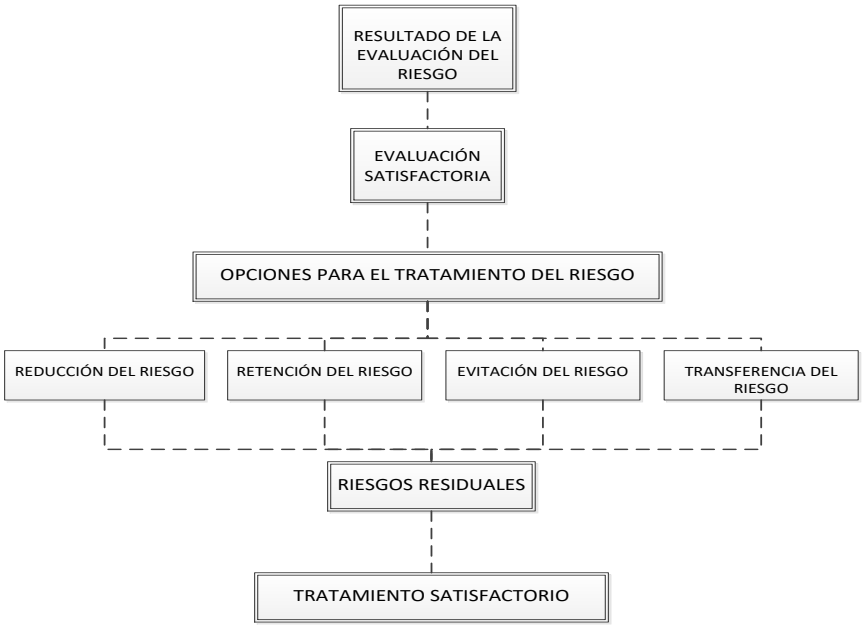


Figura 10: Actividad para el tratamiento del riesgo (***Fuente:*** Moreno (2008))

- **Reducción del riesgo**

- Es necesario seleccionar los controles justificados y adecuados, que cumplan con los requisitos identificados en el tratamiento del riesgo.
- También se debe considerar el marco temporal y el costo de ello para la implementación de los controles.
- Los controles pueden ofrecer uno o más tipos de protección: detección, prevención, minimizar el impacto, corrección, eliminación, concienciación y recuperación.
- Es necesario considerar varias restricciones cuando se selecciona los controles antes y durante la implementación.

Por lo tanto, se consideran lo siguientes restricciones, tal como se muestra en la Figura 11.

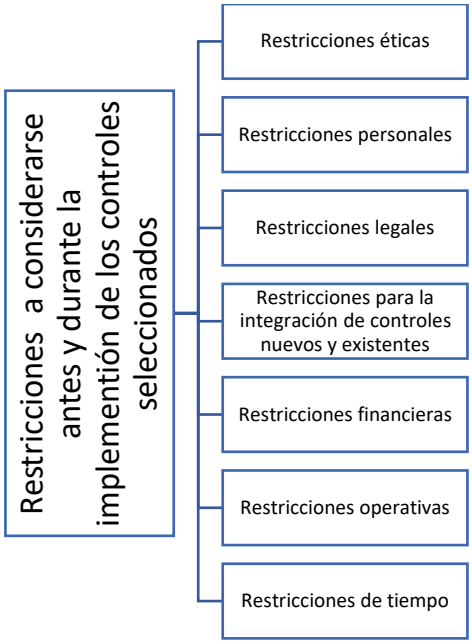


Figura 11: Restricciones a considerarse antes y durante la implementación de los controles seleccionados (***Fuente***: Moreno (2008))

- **Aceptación del riesgo**

➢ Se toma la decisión de aceptar el riesgo, dependiendo de la evaluación del riesgo.

➢ Cuando el nivel del riesgo satisface los criterios para su aceptación no se implementa los controles identificados y el riesgo se puede retener.

- **Evitación del riesgo**

➢ Es cuando los riesgos son costosos y se consideran altos para la organización, se toma una decisión de evitar por completo el riesgo, mediante el retiro de una actividad.

- **Transferencia del riesgo**

➢ Se debe transferir a otra empresa que lo trabaje de manera eficaz y eficiente el riesgo que se encontró en la evaluación.

➢ La trasferencia del riesgo implica una decisión para compartirlo con las partes externas.

➢ La transferencia se hace mediante un seguro que brindará soporte a las consecuencias o mediante una subcontratación de un asociado cuya función será monitorear el sistema de información y tomar acciones rápidas para detener el ataque.

2.2.3. Área de TI de la UPN.

A. Visión del área

Proporcionar soporte completo para cumplir con nuestro objetivo principal: " Llevar el Evangelio del Reino en todo el mundo". Entendemos por tecnología de información, como un medio eficiente y eficaz para cumplir con esta tarea.

B. Misión del área

Crear, producir, mantener y distribuir productos y servicios de calidad, que agilicen y apoyen las actividades para el cumplimiento de la misión de la IASD.

C. Objetivo del área

Mejorar los procesos del departamento de TI de la UPN, Campos e instituciones

D. Organigrama del Área

En la Figura 12 se aprecia el organigrama funcional del área de TI, el cual nos hizo llegar el jefe del área.

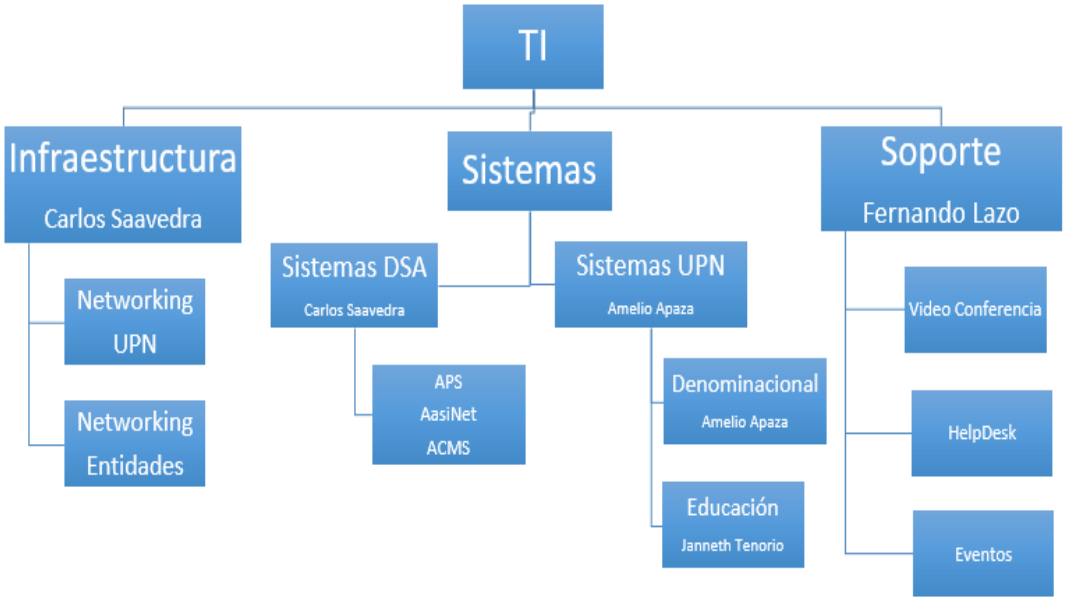


Figura 12: Organigrama funcional del área de TI de la UPN (**Fuente:** Área de TI de la UPN)

En la Tabla 10 se describen los respectivos roles del área con sus respectivas funciones, en base al organigrama brindado.

Tabla 10:
Relación de puestos y principales funciones por puesto

Nombre del Puesto		Funciones
Soporte	**Encargado de Soporte**	Realiza las conexiones de los equipos tecnológicos para recibir videoconferencias y eventos dentro y afuera de la organización, además de brindar soporte y mantenimiento a todos los equipos tecnológicos que se encuentran en la organización.
Sistemas	**Encargado del Soporte y mantenimiento de los Sistemas DSA**	Brinda soporte y mantenimiento de los sistemas DSA en los cuales están incluidos los sistemas denominados: APIS, AasiNet y ACMS
	Analistas de Sistemas – Sistemas UPN	Realizan el análisis y desarrollo de los sistemas Académicos y Denominacionales de la UPN
Infraestructura	**Jefe de Infraestructura (Jefe de TI)**	Gestiona las redes de infraestructura para brindar un soporte que beneficie el mantenimiento de la organización y de las entidades.

Fuente: Elaboración Propia

2.3. Marco conceptual

2.3.1. Información.

Según la AENOR (Asociación Española de Normalización y Certificación), la información es uno de los principales activos de las organizaciones. La defensa de este activo es una tarea esencial para asegurar la continuidad y el desarrollo del negocio, así como también es una exigencia legal (protección de la propiedad intelectual, protección de datos personales, servicios para la sociedad de la información).

2.3.2. Seguridad de la información.

Según la ISO 27001, la seguridad de la información consiste en la preservación de su, disponibilidad, integridad y confidencialidad, al igual como los sistemas implicados en su tratamiento dentro de una organización.

2.3.3. Seguridad física.

Según Grupo IWI (2009), “Se puede definir como la aplicación de barreras físicas y procedimientos de control, generalmente de prevención y detección, destinados a proteger

físicamente cualquier recurso del sistema; algunos ejemplos de estos recursos son un teclado, una copia de seguridad con toda la información que hay en el sistema o, la propia CPU del equipo."

2.3.4. Seguridad lógica.

Alegre & Garcia (2011), "Se encarga de asegurar la parte de software de un sistema informático, que se compone de todo lo que no es físico, es decir, los programas y los datos. Además, se encarga de controlar que el acceso al sistema informático, desde el punto de vista software, se realice correctamente y por usuarios autorizados, ya sea desde dentro del sistema informático, como desde fuera, es decir, desde una red externa, usando una VPN (protocolos, PPP, PPTP, etc.), la web (protocolos, http, https), transmisión de ficheros (ftp), conexión remota (ssh, telnet), etc."

2.3.5. Riesgo.

Giménez (2015) "El riesgo es una medida del daño probable que causará una amenaza, que aprovecha una vulnerabilidad para causar un daño."

2.3.6. Amenaza.

Valdivia (2015) "Se refiere a cualquier situación o evento posible con el potencial de daño, que pueda presentarse en un sistema."

2.3.7. Vulnerabilidad.

Valdivia (2015) "Se refiere a la exposición a un riesgo, fallo o hueco de seguridad detectado en algún programa o equipo."

2.3.8. Activo.

Valdivia (2015) "Se refiere a los recursos con los que cuenta una empresa o institución y que tienen valor. Pueden ser tangibles (servidores, equipos de computación, etc.) o intangibles (información, políticas, normas, procedimientos, etc.)".

2.3.9. Ataque.

Valdivia (2015) “Se refiere a llevar a cabo una amenaza.”

2.3.10. Hacker (pirata).

Bortnik (2014) menciona que según el IETF (Internet Engineering Task Force), un *hacker* es una persona que se deleita por tener una comprensión profunda del funcionamiento interno de un sistema.

2.3.11. Software malicioso: (malware).

Según SANS Securiting The Human (2014), “Es un software, un programa de computadora utilizado para llevar a cabo acciones maliciosas.”

2.3.12. Antivirus.

Valdivia (2015) “Se refiere a un programa capaz de detectar, controlar y eliminar virus informáticos y algunos códigos maliciosos (Troyanos, Works, Rootkits, Adware, Backdoor, entre otros)”

2.3.13. Criptografía.

Giménez (2015) “Es el “arte de escribir con clave secreta o de un modo enigmático”. Aplicar a un mensaje técnicas de criptografía, o de encriptación, consiste en modificarlo mediante algún procedimiento secreto o privado, de manera que el resultado sea un enigma.”

2.3.14. Copias de seguridad.

Viera (2013) “Una copia de seguridad o backup en tecnología de la información o informática, es una copia de ficheros o datos, con el fin de que estas copias adicionales puedan utilizarse para restaurar el original después de una eventual pérdida de datos”.

CAPÍTULO III: METODOLOGÍA Y MATERIALES

3.1. Metodología de investigación

La metodología de estudio consta de 5 fases donde indica que cada fase descrita consta de actividades que deben cumplirse para completar la fase. Esto permite conocer al detalle la realización de la investigación. En la Figura 13 muestra la metodología de estudio realizada para la investigación.

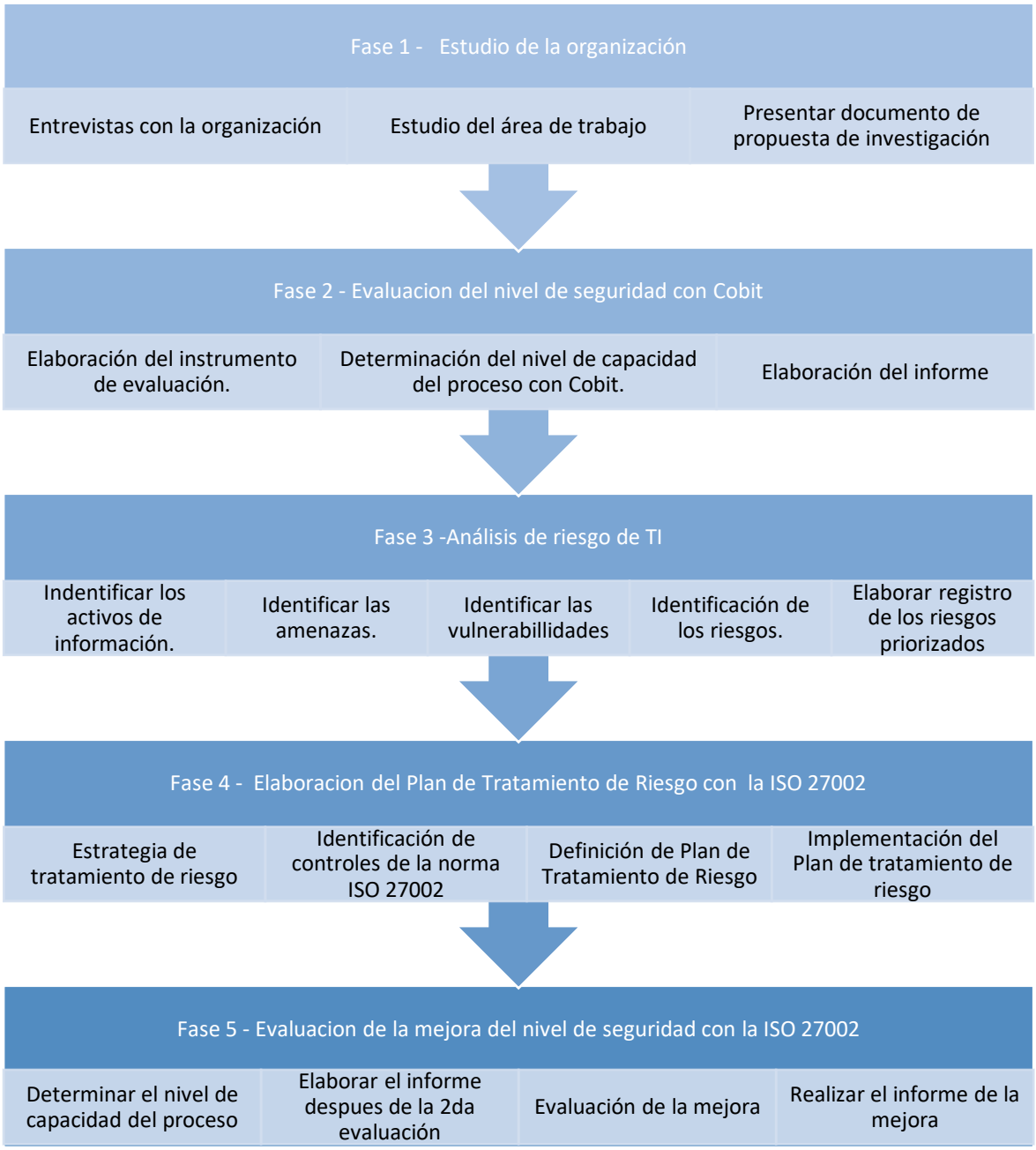


Figura 13: Metodología de Estudio (***Fuente:*** Elaboración Propia)

3.2. Actividades que contiene cada fase de la metodología

3.2.1. Fase 1: Estudio de la organización.

- **Actividad 1: Entrevistas con la organización**

Se acordará, en conjunto, con el jefe del área de TI, la primera entrevista y posteriores reuniones, donde se recopilarán la información de organización. Esto permite entender mejor el alcance y control de la información que se necesita para el desarrollo de la investigación.

- **Actividad 2: Estudio del área del trabajo**

Se define el área de trabajo. Posterior a ello, se analiza las dificultades del área, del cómo está en la problemática en general, cuáles son sus pros y sus contra, con la salvaguarda de la seguridad física y lógica de la información.

- **Actividad 3: Presentar documento de propuesta de investigación**

Se presenta un documento indicando los objetivos que se desarrollará en el transcurso del proyecto, indicando el tema de investigación y la problemática de la organización.

3.2.2. Fase 2: Evaluación del nivel de seguridad con COBIT.

- **Actividad 1: Elaboración del instrumento de evaluación**

En esta actividad se desarrolla el instrumento de evaluación en base a las prácticas de gestión del proceso DSS05 – "Gestionar los servicios de seguridad" de COBIT, que será revisado previamente por especialistas, para su debida implementación en la organización.

- **Actividad 2: Determinación del nivel de capacidad del proceso con Cobit**

Se realiza la auditoría con el instrumento elaborado en la actividad anterior, el instrumento de evaluación se aplica al jefe del área de TI para la evaluación correspondiente; después de ello, se determina el nivel de capacidad del proceso. Esta evaluación se basa en el Modelo de Evaluación del Proceso (PAM).

- **Actividad 3: Elaboración del informe**

Una vez realizada la auditoría, se elabora el informe indicando el nivel de capacidad en el que se encuentra el proceso indicado. Este informe debe contar con la aceptación y validación correspondiente del jefe de TI.

3.2.3. Fase 3: Análisis de riesgo de TI.

- **Actividad 1: Identificar los activos de información**

En esta actividad se realiza la identificación de los activos de información. Esto es vital ya que el análisis de riesgo y las decisiones que se escojan con el plan tratamiento del riesgo en la organización giran en torno a los activos de información identificados. Es importante conocer qué es un activo de información y entender sus distintas posibles características, con el fin de efectuar un excelente análisis de riesgo.

Los activos serán clasificados por su tipo o categoría, a su vez se describirá su ubicación e identificará su propietario. Junto a esto se los tasará en base a la escala de Likert para apreciar su impacto en el área de TI por sus fallas o deterioros y cómo estos afectan en la disponibilidad, confidencialidad e integridad de la información.

Todo esto será registrado y presentado al jefe del área de TI para su posterior aprobación.

- **Actividad 2: Identificar las amenazas**

En este paso se realiza la identificación de las amenazas ligadas a los activos de información. Se dice que los activos de información son vulnerables a varios tipos de amenazas, las cuales pueden ocasionar un incidente no esperado que puede ocasionar un mal a los activos y a la organización. A estas amenazas se les clasificará por su naturaleza, para poder precisar su ubicación.

Una vez que se realizase la identificación de las amenazas que pudiesen afectar a los activos, se evaluará su probabilidad de ocurrencia. Para realizar la medición de probabilidad de ocurrencia, se usará la escala de Likert.

Se considerará con detenimiento al momento tomar las decisiones en relación con el análisis de amenazas, esto para su debido resguardo. Todo esto será registrado y presentado al jefe del área para su posterior aprobación.

- **Actividad 3: Identificar las vulnerabilidades**

Consiste en identificar las vulnerabilidades de tecnología de información ligadas a los activos de información, estas no producen un mal, sino sencillamente son situaciones que pudiesen realizar de que una amenaza afectase un activo.

Para tener un mejor control de las vulnerabilidades se las relacionará con los activos priorizados. Estas dos actividades, la identificación de las vulnerabilidades y relación de activos – vulnerabilidad, serán registradas y presentadas al jefe del área de TI para su posterior aprobación.

- **Actividad 4: Identificación de los riesgos**

El cuarto paso consiste en identificar los riesgos, basado en las amenazas y vulnerabilidades identificadas. Se calculará la probabilidad de que puedan unirse y originar un riesgo. Los riesgos poseen dos factores, uno que expresa el impacto del riesgo si ocurriese, y otro que expresa la probabilidad de que el riesgo ocurra. Se evaluará el impacto económico en relación a la amenaza, para esto se usará la escala de Likert. Se utilizará esa escala para medir la posibilidad de ocurrencia que podría darse por la amenaza. Y como último, este paso consistirá en calcular la medición del riesgo, el cual se obtendrá de la multiplicación de los valores que se obtuvieron del impacto de la amenaza y su probabilidad de ocurrencia. Estos

riesgos serán priorizados en orden, en referencia a su factor de exposición al riesgo. Todo esto será registrado y presentado al jefe del área para su posterior aprobación.

- **Actividad 5: Elaborar registro de los riesgos priorizados**

En esta actividad se considera únicamente los riesgos cuyo valor obtenido por la multiplicación de la medición de probabilidad de ocurrencia y el impacto que ocasionaría, tengan un alto grado, conservando únicamente a estos para su posterior reducción con la implementación de los controles que serán definidos en la elaboración del plan de tratamiento de riesgo con la ISO/IEC 27002:2013.

3.2.4. Fase 4: Elaboración del plan de tratamiento de riesgo.

- **Actividad 1: Estrategia de tratamiento de riesgo**

Se seleccionan los diferentes tipos de estrategias en función a la naturaleza del riesgo, logrando obtener una estrategia de riesgo para cada riesgo que se encontró en el análisis.

- **Actividad 2: Identificación de los controles de la norma ISO 27002**

Para los riesgos, cuya estrategia es la reducción, se seleccionan los controles dados por la norma ISO/IEC: 27002, con el fin de implementar y lograr reducir el riesgo a un nivel aceptable.

- **Actividad 3: Definición del Plan de Tratamiento de Riesgo**

Se elaborará un plan de tratamiento indicando los costos, el tiempo y los mecanismos que serán implementados para su desarrollo de cada control seleccionado, estos documentos contendrán los objetivos, alcances y las propuestas de cada control y el tiempo que llevará la implementación.

- **Actividad 4: Implementación del Plan de Tratamiento de Riesgo**

Definido el plan de tratamiento de riesgo, se implementará los controles que fueron seleccionados para la reducción del riesgo. Esto permitirá cumplir con lo propuesto en el plan y formará una mejora.

3.2.5. Fase 5: Evaluación de la mejora del nivel de seguridad con la ISO 27002.

- **Actividad 1: Determinar el nivel de capacidad del proceso**

Aquí se desarrollará la segunda evaluación con la misma herramienta de evaluación, esto después de haber implementado los controles que fueron seleccionados para la reducción de los riesgos, la cual reflejará la mejora del proceso DSS05 – "Gestionar los servicios de Seguridad", el cual fue seleccionado para evaluar la mejora del nivel de seguridad físico y lógica de la información.

- **Actividad 2: Elaborar el informe después de la 2da evaluación**

Una vez que se realizó la auditoria, se desarrollará un informe que indique el porcentaje o nivel en la que se encuentra la seguridad de la información, después de la implementación del plan de tratamiento de riesgo en la organización. Luego se realizará el informe con el nivel de capacidad del proceso mediante el marco de referencia COBIT PAM.

- **Actividad 3: Evaluación de la mejora**

Se determinará cuáles son las mejoras dadas por la primera evaluación y la segunda evaluación, haciendo un análisis breve indicando las mejoras obtenidas.

- **Actividad 4: Realizar el informe de la mejora**

En este último punto, se desarrollará el informe final de evaluación, el cual indicará la mejora y observaciones que se obtuvo de manera general, y cuan satisfactorio le fue al área de TI al poder realizar la implementación con los controles para la mejora del nivel de seguridad lógica y física de la información. Este informe será presentado al jefe del área de TI para su aprobación y validación correspondiente.

3.3. Nivel de investigación

Según Hernández (2012), “El nivel de investigación se refiere al grado de profundidad con que se aborda un fenómeno o un evento de estudio.

Según Hernández Sampieri (2017), “Los estudios explicativos son más que la descripción de conceptos, fenómenos o el establecimiento de relaciones entre variables; más bien, están diseñadas para determinar las causas de los eventos y fenómenos físico o sociales. Como su nombre lo indica, su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta, o porque se relacionan dos o más variables.”

La investigación desarrollada es de nivel Explicativo porque la relación entre las variables es una relación de causa efecto, siendo que la variable independiente, Controles de seguridad física y lógica de la ISO/IEC 27002:2013 tienen un efecto sobre la variable dependiente Niveles de Seguridad de la información.

3.4. Tipo de investigación

Según Landeau (2007), "Los tipos de investigación se han definido de acuerdo a varios aspectos que presentan modalidades particulares de investigación, entre otras: su finalidad, a un momento específico, a las fuentes de información, al enfoque histórico, en la observación, en la experimentación, a la amplitud y el método de casos.”

Según Lara (2013), “La investigación aplicada, guarda íntima relación con la básica pues depende de los descubrimientos y avances de la investigación básica y se enriquece con ellos, pero se caracteriza por su interés en la aplicación, utilización y consecuencias prácticas de los conocimientos. La investigación aplicada busca el conocer para hacer, para actuar, para construir, para modificar”

La investigación realizada es de tipo aplicada puesto que se tuvo que hacer un estudio exhaustivo de la problemática del área de TI y de las posibles soluciones para ella, de

cómo tratarse y elaborarse, esto con el fin de obtener resultados satisfactorios en el área de TI, lo cual permitirá mejorar el nivel de seguridad física y lógica de la información.

3.5. Enfoque de la investigación

Ruiz (2012) "El enfoque de la investigación es un proceso sistemático, disciplinado y controlado y está directamente relacionada a los métodos de investigación que son dos: método inductivo generalmente asociado con la investigación cualitativa que consiste en ir de los casos particulares a la generalización; mientras que el método deductivo, es asociado habitualmente con la investigación cuantitativa cuya característica es ir de lo general a lo particular."

El enfoque de nuestra investigación es cualitativo, pues previo al análisis se realiza una auditoría, la cual permite conocer la problemática y los procesos de la organización, conociendo el nivel de seguridad de la Unión Peruana del Norte, que permite realizar con determinación el planteamiento del problema bien estructurado.

Además, se elaborará un análisis de riesgo para tener un control de lo que pueda suceder en el transcurso de la investigación.

3.6. Población

- **Población de estudio.**

Lerma (2016) "La población es el conjunto de todos los elementos de la misma especie que presentan una característica determinada o que corresponden a una misma definición, y cuyos elementos se le estudiarán sus características y relaciones. Está definida por el investigador y puede estar integrada por personas o por unidades diferentes a personas: viviendas, ventanas, tornillos, pacientes de pediatría, computadores, historias clínicas, entre otros".

Para el presente proyecto de investigación se ha definido como población al jefe del área de TI y al resto del personal del área.

3.7. Recolección de la información

- Lista de chequeo. - Se mide el estado actual de la organización
- Observaciones. - Por cada entrevista hay puntos que suelen cambiar entorno a la organización o al proyecto.
- Entrevistas. - Tomar nuevas entrevistas con el jefe de área o con el asesor para la revisión correspondida.

CAPÍTULO IV: INGENIERÍA DE LA PROPUESTA

4.1. Fase 1: Estudio de la organización

4.1.1. Actividad 1: Entrevistas con la organización.

Como primera actividad de la metodología de investigación, se tuvo el estudio de la organización, a través de entrevistas con el jefe del área de TI de la UPN. La información obtenida sirvió para la investigación, ya que en base ello se toma los puntos necesarios para explicar el propósito de estudio, para el desarrollo de la investigación.

Se realizó la reunión con el jefe del área de TI el día de 28 de marzo de 2016 a las 9:30 y tuvo una duración 45 minutos, donde se explicaron los propósitos de estudios y temas relacionados a la investigación y acuerdos para reuniones posteriores. Lo expresado por el jefe del área en las entrevistas y reuniones fueron grabados en un audio para tener un respaldo de ello. En el Anexo 1 se muestra el acta de la primera reunión, la cual valida la realización de la reunión.

4.1.2. Actividad 2: Estudio del área de trabajo.

La segunda actividad fue realizar el estudio del área de trabajo. En este punto se determinó en conjunto con el jefe del área de TI, el lugar o área de trabajo exacto de la organización en donde se realizaría la investigación; siendo el área de TI, el lugar designado para realizar nuestra investigación. Posterior a ello, se realizó una identificación preliminar de la problemática que abordaba el área de TI. Esta información se obtuvo mediante entrevistas brindadas por el jefe del área, lo expresado y dicho por el jefe del área en esta entrevista fue grabado en un audio para tener un respaldo de ello. En el Anexo 2 se visualiza el Acta de la 2da reunión en donde se detallan los puntos importantes para dicha reunión.

4.1.3. Actividad 3: Presentar documento de propuesta de investigación.

Finalizando la primera fase, se presentó el documento de la propuesta de investigación, expresando el alcance general de la investigación, esto en base a la problemática identificada.

Se plantó el objetivo principal de implementar los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la UPN. En el Anexo 3 se observa la tercera acta de reunión donde se detallan los puntos que se tomaron en cuenta para esta actividad, y en el Anexo 4 se muestra el Documento actualizado de nuestra propuesta de investigación, dirigida a la Unión Peruana del Norte. En el Anexo 9 se aprecia la topología de red de la Organización, en el Anexo 10 la estructura de cables, y por último en el Anexo 11 el servidor principal perteneciente al área de TI.

4.2. Fase 2: Evaluación del nivel de seguridad con Cobit

4.2.1. Actividad 1: Elaboración del instrumento de evaluación.

Se determinó como instrumento de evaluación una lista de chequeo (checklist) que está elaborado bajo el proceso COBIT DSS05 – Gestionar los Servicios de Seguridad; este detalla las buenas prácticas para su implementación. Este proceso cuenta con 7 prácticas de gestión y cada práctica con cierto número de actividades, las cuales ayudan a cumplir con los requisitos para obtener una seguridad de la información integra y robusta. Se elaboró un checklist organizado en 7 partes, en función a cada práctica de gestión del proceso. Estos checklist fueron validados por especialistas en el tema. En el Anexo 5 se muestra el instrumento de evaluación (checklist) elaborada en base a las 7 prácticas de gestión del proceso DSS05 – Gestionar los servicios de seguridad. En el Anexo 6 la Constancia de validación de los checklist por parte de los especialistas.

4.2.2. Actividad 2: Determinación del nivel de capacidad del proceso con Cobit.

Es aquí donde se realizó la auditoría, para ello se pactó una fecha en coordinación con el jefe del área de TI, la cual había sido estipulada para el 25 de julio de 2017.

Ya en la fecha definida se procedió a realizar la auditoría en conjunto con el jefe del área de TI, tomando en ellos las 7 checklist. La hora de inicio de la auditoría fue a las 9:30 am y tuvo una duración de 2 horas. En el transcurso de la evaluación se tocaron todos los puntos (Ítems) definidos en los checklist, siendo en algunos casos positivos y en otros negativos, puesto que en algunos casos el área de TI cumple con lo que se estipula en las prácticas de gestión y en otras no cumple con lo descrito.

Una de las cosas que se percibió, es que el área de TI cumplía una determinada parte de las actividades detalladas en los ítems, pero no contaba con un registro de ello o documentos de validación, lo cual es necesario e importante para tener un respaldo y tener un mejor control sobre estos puntos. Después de realizada la auditoría, se procesó la información para determinar la capacidad del proceso. Se consideró los elementos del modelo PAM que se relaciona con las 7 prácticas de gestión del proceso, es decir los cinco criterios de evaluación, los cuales son:

- **Criterio 1:** DSS05-O1 “Las redes y la seguridad de las comunicaciones responden a las necesidades del negocio.”
- **Criterio 2:** DSS05-O2 “La información procesada, almacenada y transmitida por dispositivos de punto final está protegida.”
- **Criterio 3:** DSS05-O3 “Todos los usuarios son identificables de forma única y tienen derechos de acceso de acuerdo con su función comercial”
- **Criterio 4:** DSS05-O4 “Se han implementado medidas físicas para proteger la información del acceso, daño e interferencia no autorizados al ser procesados, almacenados o transmitidos.”

- **Criterio 5:** DSS05-O5 “La información electrónica está debidamente protegida cuando se almacena, transmite o destruye.”

El resultado de la evaluación inicial fue de 47%, lo que según la escala de evaluación del PAM (ver Figura 6), el proceso evaluado en el área de TI de la UPN está parcialmente logrado, lo que se espera tener una mejora para la segunda evaluación ya con la implementación de los controles que serán seleccionados en función al plan de tratamiento de riesgo. En la Tabla 11 se observa la matriz de los criterios de evaluación del PAM para el proceso DSS05 - Gestionar los servicios de seguridad.

Tabla 11*:*
Criterios de evaluación del PAM para el proceso DSS05 - Gestionar los servicios de seguridad

Criterios de evaluación del modelo PAM					
Prácticas del Proceso DSS05- "Gestionar los Servicios de Seguridad"	**Criterio 1:** DSS05-O1 "Las redes y la seguridad de las comunicaciones responden a las necesidades del negocio."	**Criterio 2:** DSS05-O2 "La información procesada, almacenada y transmitida por dispositivos de punto final está protegida"	**Criterio 3:** DSS05-O3 "Todos los usuarios son identificables de forma única y tienen derechos de acceso de acuerdo con su función comercial"	**Criterio 4:** DSS05-O4 "Se han implementado medidas físicas para proteger la información del acceso, daño e interferencia no autorizados al ser procesados, almacenados o transmitidos."	**Criterio 5:** DSS05-O5 "La información electrónica está debidamente protegida cuando se almacena, transmite o destruye."
DSS05.01 "Proteger Contra Software Malicioso"	**X**	**X**			
DSS05.02 "Gestionar la seguridad de la red y las conexiones"	**X**				
DSS05.03 "Gestionar la seguridad de los puestos de usuario final"		**X**			
DSS05.04 "Gestionar la identidad del usuario y el acceso lógico"			**X**		
DSS05.05 "Gestionar el acceso físico a los activos de TI"				**X**	
DSS05.06 "Gestionar Documentos sensibles y dispositivos de salida"					**X**
DSS05.07 "Supervisar la infraestructura para detectar eventos relacionados con la seguridad"	**X**				

Fuente: Elaboración propia

En la Tabla 12 se observa el cuadro de evaluación y resultado obtenido por cada criterio de evaluación en base a la escala de evaluación del PAM.

Tabla 12:
Cuadro de evaluación y resultado obtenido por cada criterio de evaluación en base a la escala de evaluación del PAM

CRITERIOS DE EVALUACIÓN	ESCALA DE EVALUACIÓN			
	No Logrado (0-15%)	**Parcialmente logrado (15% -50%)**	**En gran medida logrado (50% - 85%)**	**Totalmente logrado (85% - 100%)**
C1) DSS05-O1 Las redes y la seguridad de las comunicaciones responden a las necesidades del negocio."			51%	
C2) DSS05-O2 "La información procesada, almacenada y transmitida por dispositivos de punto final está protegida"			59%	
C3) DSS05-O3 "Todos los usuarios son identificables de forma única y tienen derechos de acceso de acuerdo con su función comercial"		40%		
C4) DSS05-O4 "Se han implementado medidas físicas para proteger la información del acceso, daño e interferencia no autorizados al ser procesados, almacenados o transmitidos"			58%	
C5) DSS05-O5 "La información electrónica está debidamente protegida cuando se almacena, transmite o destruye."		27%		
Resultado de la evaluación del proceso		47% - Parcialmente logrado		

Fuente: Elaboración propia

Todo este proceso fue validado y aceptado por el jefe del área de TI. En el Anexo 7 se puede apreciar la primera evaluación por cada lista de chequeo.

4.2.3. Actividad 3: Elaboración del informe.

Este informe detalló los resultados que se obtuvieron en la evaluación inicial. Este documento se presentó al jefe del área de TI, quien validó y dio su aprobación al documento elaborado. En el Anexo 8 se observa el informe de auditoría inicial.

4.3. Fase 3: Análisis de riesgo de TI

4.3.1. Actividad 1: Identificar los activos de información.

La tercera fase consiste en realizar el análisis de riesgo, la cual se tomó de referencia a la ISO 27005 y el libro "*Diseño de un Sistema de Gestión de Seguridad de Información Óptica ISO 27001:2005"*(Alexander, 2007). El primer paso fue identificar los activos de información del área de TI. Para esto se tuvo una reunión con el jefe del área de TI, el cual nos hizo llegar una lista de todos sus activos que poseían en manera general. Este informe de los activos es realizado por el área de Contabilidad de la Unión Peruana del Norte.

Ya con lista de activos, y en base a lo que solicita la norma para la identificación de activos, se procedió a realizar la clasificación de los tipos de activos. En la Figura 14 se aprecia la clasificación de los tipos de activos de información.

Figura 14: Clasificación de tipos de activos de información (***Fuente***: Alberto G. Alexander (2007))

Seguidamente, se registró la ubicación física de cada activo; estos se encontraban distribuidos en las instalaciones de la organización, por lo que se tuvo que hacer un seguimiento de ello. También se identificó al propietario de cada activo. El propietario es el responsable por su cuidado, manejo y administración del activo. Finalmente, se realizó la

tasación o valoración de los activos basándonos en los 3 pilares de seguridad de la información: la integridad, confidencialidad y disponibilidad. Para realizar la tasación se usó la escala de Likert, la cual se califica del uno al cinco siendo, tal como se aprecia en la Figura 15.

Figura 15: Escala de Likert (***Fuente***: Alberto G. Alexander (2007))

Se dieron más valor a los activos que procesaban, transmitían, transportaban y almacenaban información, a diferencia de otros activos que no contaban con esas características. Esta valoración se hizo en conjunto con el jefe del área. Toda la información fue registrada en un archivo Excel, validada y aceptada por el jefe del área de TI.

El área de TI cuenta con 74 activos, de los cuales 48 fueron priorizados. En el Anexo 12 se muestra la lista general de los activos del área de TI de la UPN organizados por su descripción, propietario, ubicación, tipo de activo y valor obtenido en la valoración. En el Anexo 13 se visualiza los activos priorizados en función al valor obtenido, se consideró los activos que obtenga su valor del 3 a 5 según la escala Likert.

4.3.2. Actividad 2: Identificar las amenazas.

Se realizó la identificación de las posibles amenazas que podrían afectar a cada activo que administra el área de TI, para esto se realizó un listado y se los clasificó por su tipo, y que según el libro “Diseño de un Sistema de Gestión de Seguridad de Información” (Alexander, 2007, p.48), se tienen seis tipos de amenazas tales como se aprecia en la Figura 16

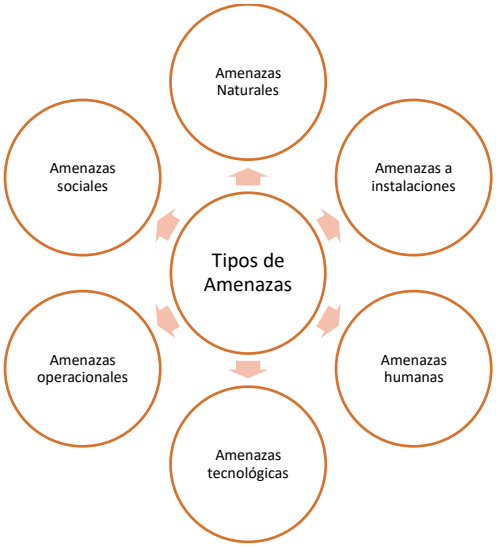


Figura 16: Tipos de Amenazas (***Fuente***: Alberto G. Alexander (2007))

Todas ellas se pueden originar de fuentes o sucesos deliberados o accidentales, seguidamente se calculó su probabilidad de ocurrencia. Para esta medición se usó la escala de Likert, dando un mayor valor a las amenazas cuyos tipos sean más propensas a darse, esto por su entorno, funciones e infraestructura que gestiona el área de TI, esto último contó con la participación del jefe del área de TI. Se identificaron un total de 26 amenazas, considerando 24 de ellas, puesto que tuvieron un mayor grado en la probabilidad de ocurrencia en los activos de información. Este listado fue validado y aceptado por el jefe del área. En el Anexo 14 se visualiza las amenazas identificadas en el área de TI de la UPN, con su respectiva medición de probabilidad de ocurrencia, las cuales se tomaron en consideración a partir del valor 3 hasta el 5, en nuestro caso el máximo valor fue 4.

4.3.3. Actividad 3: Identificar las vulnerabilidades.

Para este punto se hizo una lista de las posibles vulnerabilidades que podrían darse por cada activo, esta lista fue elaborada en base a cada activo y amenaza identificada, teniendo un listado general de 54 vulnerabilidades. Posterior a la identificación de las vulnerabilidades se evaluó la relación activo – vulnerabilidad, con el fin de tener una mejor gestión en las vulnerabilidades ligadas a los activos, y así realizar una correcta identificación

de los riesgos. Estos dos puntos fueron registrados en un archivo Excel, validados y aceptados por el jefe del área de TI. En el Anexo 15 se visualiza la lista las vulnerabilidades identificadas en el área de TI de la UPN y en el Anexo 16 se visualiza la relación de los activos con las posibles vulnerabilidades que podrían estar ligados a cada uno de ellos.

4.3.4. Actividad 4: Identificación de los riesgos.

Esta actividad consistió en la identificación de los riesgos, que se calcula con la medición de todos los activos, las cuales cada activo contiene valores asignados para cada pilar de seguridad: integridad, confidencialidad y disponibilidad. Este cálculo también debe tener el valor de la probabilidad de ocurrencia entre las amenazas y las vulnerabilidades, las cuales causan un mal a los activos de información como a la organización. Estos riesgos calculados proporcionan un medio para poder prevalecer y hallar aquellos otros riesgos que son más consecuentes para la organización. Existe un método para el cálculo de riesgo, y que según el libro "Diseño de un Sistema de Gestión de Seguridad de Información" (Alexander, 2007, p.54), trata de relacionar los factores del impacto de la amenaza junto con su probabilidad de ocurrencia. Se les realizó una medición por su probabilidad de ocurrencia y el impacto que ocasionaría si la amenaza llegase a dar. Estas mediciones se hicieron en base a la escala de Likert, de la cual, para obtener su valor total y ver su grado de riesgo, se tuvieron que multiplicar estos dos valores. En total fueron 348 riesgos identificados, donde el mínimo valor obtenido para los riesgos fue de 6 y el máximo valor obtenido fue 20, siendo este el de mayor criticidad. Esto fue registrado en un archivo Excel y compartido, validado y aceptado por el jefe del área de TI. En el Anexo 17 se visualiza la lista de los riesgos generales que se identificaron en la organización.

4.3.5. Actividad 5: Elaborar registro de los riesgos priorizados.

En este último paso de la tercera fase, se elaboró el registro de los riesgos priorizados, de los cuales se conservaron únicamente los riesgos cuyo valor obtenido por la

multiplicación de la probabilidad de ocurrencia y el impacto obtenido tenga un alto grado. Para nuestro caso se consideró el nivel de grado de evaluación a partir del valor 15 hasta el 25, siendo este último valor el más crítico, y el cual necesitaría tratarse con mucho más resguardo y con la debida importancia. En nuestro caso los riesgos con mayor alto grado fueron de valor 20. En resumen, se tuvo un total de 178 riesgos priorizados. Los cálculos realizados fueron separados por color, los cuales se dan por la multiplicación de probabilidad de ocurrencia e impacto.

Tabla 13:
Niveles de evaluación del riesgo

Probabilidad de Ocurrencia	**5**	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	**2**	**3**	**4**	**5**
		Impacto				

Fuente: Elaboración propia

En la Tabla 13 se observa el nivel evaluación de riesgo y en la Tabla 14 se describen los grados de los niveles de riesgo siendo en total de 5.

Tabla 14:
Nivel del Tratamiento del riesgo

Grado de Evaluación	Descripción
Muy Alta	El riesgo es priorizado y puede perjudicar a la organización y necesita tratarse inmediatamente para ver el alcance, ver si se implementa los controles o se trasfiere para su reducción del nivel de evaluación.
Alta	El riesgo es priorizado se debe tratarse de manera organizada, detallada y documentada en un tiempo corto definiendo controles para su implementación
Medio	El riesgo no es priorizado, se mejora el proceso con los controles, viendo si es viable en el término del costo para que la organización no se sienta afectada en un futuro.
Bajo	El riesgo no es priorizado, no requiere de un tratamiento, donde se encuentre en un nivel que puede aceptarse para la organización
Muy bajo	El riesgo no es priorizado, no requiere de un tratamiento, que no perjudique a la organización.

Fuente: Elaboración propia

En el Anexo 18 se visualiza la lista de los riesgos priorizados, tomados en cuenta de acuerdo a su valor obtenido por la multiplicación de su impacto con su probabilidad de ocurrencia.

4.4. Fase 4: Elaboración del Plan de Tratamiento de Riesgo con la ISO 27002

4.4.1. Actividad 1: Estrategia de tratamiento de riesgo.

Esta actividad consiste en seleccionar la estrategia de riesgo que la norma ISO 27005 brinda para decidir qué acciones se debe tomar frente a los riesgos. Las estrategias a seleccionar fueron: Reducir, Aceptar, Transferir y Evadir. Para la selección de la estrategia de riesgo se tomaron en cuenta: los costos, el tiempo, las evaluaciones y demás actividades que intervienen al momento de tratar un riesgo.

La estrategia de riesgo Reducir, permite la selección de controles de la norma ISO 27002, para minimizar el impacto y la ocurrencia de los riesgos.

Si la estrategia de riesgo es Evitar; se toma acciones, como el cambio de una actividad, lo que evitaría la presencia del riesgo.

Cuando la estrategia de riesgo es Transferir, la organización ve difícil reducir o controlar el riesgo a un nivel aceptable. La posibilidad de transferirla a una tercera parte es más económica, se establece condiciones en las que se transfiere. Y por último, cuando la estrategia de riesgo es Aceptar, es porque en algunas ocasiones no se encuentran los controles para reducir los riesgos, o la implementación de un control que tiene un costo mayor que las consecuencias del riesgo. En estos casos, la decisión de aceptar el riesgo y convivir con el riesgo es la más adecuada. Cuando la organización toma esta decisión se deben documentar y definir con precisión los criterios de aceptación del riesgo. Todo esto contó con la aprobación y aceptación del jefe del área de TI y con la validación de la especialista en el tema. En el Anexo 19 se puede apreciar las estrategias de riesgo que fueron definidos para cada uno de los riesgos priorizados.

4.4.2. Actividad 2: Identificación de controles de la norma ISO 27002.

Al mismo tiempo de realizar la identificación de la estrategia de riesgo, se analizó que controles de la norma ISO/IEC 27002 ayudarán a reducir los riesgos para la mejora del nivel de seguridad de la información. Estos controles permitirán mejorar la seguridad de la información, como la seguridad física y lógica de la organización, este análisis se desarrolló en conjunto con la identificación de las estrategias de riesgo, determinando qué controles serán implementados, logrando minimizar el impacto del riesgo con los activos de información. Los controles seleccionados en los riesgos priorizados fueron también evaluados por la ingeniera experta para su implementación adecuada. En el Anexo 19 se puede apreciar los controles que fueron definidos para la estrategia de riesgo Reducir, aunque no fueron tomados en su totalidad, puesto que, para reducir los riesgos de seguridad física y lógica, y luego en lo que concierne al proceso del análisis sobre las estrategias y controles, se concluyó que se deben implantar 14 controles de la norma 27002, los que se encuentran en relación con el proceso DSS05 – "Gestionar los Servicios de Seguridad". Aparte de los controles que se muestran en la lista se consideraron los controles 5.1.1 – "Políticas para la seguridad de la información", 8.1.1 – "Inventario de Activos", 8.2.1 – "Clasificación de la información", puesto que para cumplir con lo que el proceso DSS05 – "Gestionar los servicios de seguridad" es necesario incluir a estos tres controles para su buena gestión y resguardo y puesto que el proceso lo requiere. Los 14 controles seleccionados para el Plan de Tratamiento de Riesgo fueron: 5.1.1, 8.1.1, 8.2.1, 9.1.1, 9.2.1, 9.2.2, 9.2.3, 9.2.5, 9.26, 9.4.2, 11.1.2, 11.2.1, 12.2.1, 12.6.1. En algunos ítems pertenecientes a la segunda y tercera lista de chequeo, no fue posible reducir los riesgos asociados a ellos, por lo que se tuvo que transferir y aceptar el riesgo. El control que está asociado a la estrategia de riesgo Transferir es el control 10.1.1 – "Política de uso de los controles criptográficos" y los controles que están asociados a la estrategia de riesgo Aceptar son el control 13.1.1 – "Controles de Red" y el

control 13.1.2 – “Seguridad de los servicios de red”. En el Anexo 20 se observa el documento relacionado a la estrategia de riesgo Transferir, en conjunto con las políticas de criptografía. En el Anexo 21 se aprecia el documento relacionado a la estrategia de riesgo aceptar, en conjunto con las políticas de Seguridad de las comunicaciones. Las políticas que son descritas en las dos estrategias de riesgo, ayudan a establecer las medidas y parámetros, por las cuales se tendrá que cumplir con ello cuando la requieran. Todo contó con la aprobación y aceptación del jefe del área de TI y con la validación de la especialista en ello.

4.4.3. Actividad 3: Definición de Plan de Tratamiento Riesgo.

La elaboración del Plan de Tratamiento de Riesgo se hizo siguiendo un formato revisado y aprobado por el jefe de TI. Este documento cuenta con objetivos, alcance y actividades para la implementación de los controles. La implementación de los controles también se definió bajo un objetivo, presupuesto y el tiempo que se llevará a cabo en la implementación del control, esto permitirá ver el alcance y el cumplimiento de ello. El Plan de Tratamiento de Riesgo describirá todo lo desarrollado hasta antes de su implementación, permitiendo que el jefe de TI conozca los avances y las acciones que se desarrollará para reducir los riesgos que pueden afectar los activos de información. Esto contó con la aprobación y aceptación del jefe del área de TI y con la validación de la especialista en el tema. En el Anexo 22 se muestra el Plan de Tratamiento de Riesgo que fue definido en base a los 14 controles seleccionados de la norma ISO/IEC 27002:2013.

4.4.4. Actividad 4: Implementación del Plan de Tratamiento de Riesgo.

La implementación del Plan de Tratamiento de Riesgo inició con la aplicación de los 14 controles seleccionados, los cuales contienen las medidas y establecimientos óptimos para el aseguramiento de la información. A continuación, se detallarán lo que se realizó por cada control:

- **Control 5.1.1 – "Políticas para la seguridad de la información":** Este fue el primer control establecido, el cual consta de normas y reglas que se tiene que cumplir en toda el área. La definición de estas normas permite tener un mejor funcionamiento en la seguridad de la información, en el ámbito físico y lógico en el área de TI de la Unión Peruana del Norte, los sistemas de información y los equipos que almacenan, procesan y transmiten información. Para su desarrollo se optó por tener como referencia el "Manual de políticas de Seguridad de la Información" (ICETEX, 2014), que aportó en la toma de documentación y definición de las políticas de seguridad. Este documento está dirigido a todo el personal del área de TI y fue aprobado por la Dirección de TI y validado por la especialista en el tema. En el Anexo 23 se visualiza el Manual de Políticas de Seguridad de la Información del Área de TI de la UPN.
- **Control 8.1.1 – "Inventario de activos":** Para la realización del inventario de activos de información, es importante identificar el conjunto de activos de información, entendiendo a un activo como cualquier elemento que conlleve valor para la organización. Esto se dio puesto que para la sexta práctica de gestión del proceso DSS05, requiere de un inventariado, donde se detallen los dispositivos y/o activos que el área de TI gestiona, esto cuando el activo salga fuera de la organización. Se realizó un registro en un archivo Excel del inventario de activos, similar a lo que se realizó en el análisis de riesgo, pero de una manera más detallada, donde se obtuvo 5 atributos de clasificación, las cuales se aprecian en la Tabla 15.

Tabla 15:
Atributos de Clasificación para los Activos de Información

Código Atributo de Clasificación	Descripción
ACL1	Activo que es de mucha importancia y de criticidad para la organización y para sus operaciones internas
ACL2	Activo que está restringido a personas externas a la organización
ACL3	Activo que está restringido a un personal limitado que no labora en el área de TI, pero que labora dentro de la organización.
ACL4	Activo que puede ser alterado para corrupción y/o fraudes
ACL5	Activo que es de conocimiento público para cualquier persona, ya sea externa o interna a la organización

Fuente: Elaboración propia

Todo esto contó con la aprobación y aceptación del jefe del área de TI y con la validación de la especialista en el tema. En el Anexo 29 se aprecia el Inventariado de Activos, y en el Anexo 47 el Inventariado de dispositivos y/o Activos de salida.

- **Control 8.2.1 – "Clasificación de la Información":** Se realizó la clasificación de la información puesto que es necesario asegurar que la información reciba los niveles de protección adecuados para su debido resguardo y correcto manejo de la información. La Guía de Clasificación de la información fue elaborada para cumplir con algunas de las actividades de la segunda, cuarta y sexta práctica de gestión del proceso DSS05 que requieren de la clasificación la información. Dentro del contenido de la Guía de Clasificación está definido un objetivo, un alcance y responsabilidades a tomarse en cuenta por parte de los propietarios de los activos de información; además, contiene definiciones básicas de términos relacionados a la clasificación de la información, una definición concisa de lo que es la Clasificación de la Información. Se incluyó también un análisis sobre los requisitos de información, que están dados o definidos en base a la confidencialidad, integridad y disponibilidad de la información. Se propuso optar por 4 niveles de clasificación los cuales son: Público, Uso Interno, Restringida, Altamente restringida. A su vez se definieron a los encargados de clasificar la información. Asimismo, se concretaron los puntos por los cuales se iban a manejar y tratar la información. Por último, se realizó una matriz donde se detalló los procedimientos de clasificación para los diferentes niveles de clasificación que se adoptaron. Para esto se tomó como referencia a Angarita & Tabares (2012) "*Análisis de riesgos para el proceso administrativo: Departamento de informática en la empresa de Acueducto y Alcantarillado de Pereira S.A E.S.P, basados en la norma ISO 27005*" (Proyecto de Grado). Universidad Tecnológica de Pereira, Colombia, la cual fue de gran ayuda para el desarrollo de esta guía, todo esto contó con la debida aprobación del jefe del área de TI y contó con la validación de la especialista en el tema. En el Anexo 30 se aprecia la Guía de

Clasificación de la Información y en el Anexo 31 el registro de Inventariado de la Clasificación de la información de los activos.

- **Control 9.1.1 – "Políticas de Control de Acceso":** De la misma forma que se estableció el Manual de Políticas de Seguridad de la Información, se realizó el Manual de Política de Control de Acceso Lógico, que conllevan a tener normas dentro de los sistemas de información que el área de TI maneja en la organización, además de medias o acciones a tomarse en cuenta para limitar el acceso a los medios y recurso de información de usuarios no autorizados, esto y más temas concernientes al control de acceso lógico está definido dentro del Manual de Políticas de Control de Acceso Lógico. Realizar esto era necesario para cumplir con las prácticas de gestión del proceso DSS05 que a nivel de acceso lógico remarcaban. Este Manual de Políticas fue aprobado por la dirección de TI, y fue publicado y distribuido a todos los miembros del área de TI y contó con la validación de la especialista en el tema. En el Anexo 24 se visualiza el Manual de Política de Control de Acceso Lógico establecido para el Área de TI de la UPN.

- **Control 9.2.1 – "Registro y baja de usuario", Control 9.2.2 – "Provisión de acceso de usuario", Control 9.2.3 – "Gestión de privilegios de acceso", Control 9.2.5 – "Revisión de los derechos de acceso de usuario", Control 9.2.6 – "Retirada o reasignación de los derechos de acceso":** Se consideraron 5 controles para la realización del procedimiento denominado "Procedimiento Seguro sobre la gestión de Acceso de Usuarios", puesto que para realizar una eficaz y segura Gestión de acceso a la información, se requiere tomar en consideración las actividades y tareas que se mencionan dentro del informe, las cuales fueron definidas en relación a lo descrito en los cinco controles, los que ayudan a tener íntegra y segura el acceso a la información.

Esto fue diseñado, puesto que para cumplir con algunas de las actividades de la cuarta práctica de Gestión del proceso DSS05 requerían de este procedimiento. Dentro del

contenido del informe está definido quienes cooperaron en elaboración de este procedimiento, el diagrama del procedimiento con sus listas de tareas, un informe conciso del procedimiento elaborado, los roles que intervienen o interactúan en el procedimiento, además de una descripción general del flujo, donde se detalla la actividad que realiza, el rol que interactúa en el procedimiento, las tareas contenidas dentro de la actividad, y los documentos o entregables que se generan, y por último, se realiza las contingencias, que es lo posible o aquello que puede, o no, concretarse. Este procedimiento fue revisado por docentes especializados para su evaluación, levantando observaciones que fueron validadas mediante firma por un documento de conformidad por parte del especialista. En el Anexo 27 se aprecia el Informe del Procedimiento Seguro sobre la Gestión de Acceso de Usuarios y en el Anexo 50 la Validación del procedimiento por parte de los especialistas.

- **9.4.2 – "Procedimientos seguros de inicio de sesión":** El motivo por el cual se optó realizar el procedimiento denominado "Procedimiento para el seguro inicio de sesión a los sistemas", fue para minimizar y/o reducir la oportunidad de acceso no autorizado a los sistemas de información, este procedimiento revela el mínimo de información sobre el sistema, además de no proporcionar ayuda innecesaria a usuarios sin autorización, para ello se requiere tomar en consideración las actividades y tareas que se mencionan dentro del informe, las cuales fueron realizadas y definidas en relación a lo descrito en este control. El desarrollo de este procedimiento también se dio, puesto que para cumplir con algunas de las actividades de la cuarta práctica de Gestión del proceso DSS05 que hacían referencia a la segura autenticación en las aplicaciones, requerían de este procedimiento. Dentro del contenido del informe está definido quienes cooperaron en elaboración de este procedimiento, el diagrama del procedimiento con sus listas de tareas, un informe conciso del procedimiento elaborado, los roles que intervienen o interactúan en el procedimiento, además de una descripción general del flujo, donde se detalla la actividad que realiza, el rol que

interactúa en el procedimiento, las tareas contenidas dentro de las actividades, y los documentos o entregables que se generan, y por último las contingencias. Este procedimiento fue revisado por docentes especializados para su evaluación, levantando observaciones que fueron validadas mediante firma por un documento de conformidad por parte del especialista. En el Anexo 28 se aprecia el Informe del Procedimiento Seguro de inicio de sesión y en el Anexo 50 la Validación del procedimiento por parte de los especialistas

- **Control 11.1.2 – "Controles físicos de entrada" & Control 11.2.1 – "Emplazamiento y protección de equipos":** En este punto los dos controles están contenidos dentro de las políticas de seguridad de la información y no cuentan con un formato en específico, puesto que con lo que se definió en las políticas de seguridad de la información ayudan a cumplir con lo establecido e instaurado en ambos controles, esto además ayuda a cumplir con lo establecido en la quinta practica de gestión del proceso DSS05.

Con lo que sí se desarrolló, fue en la elaboración de un formato de solicitud de peticiones de acceso a las instalaciones de la organización por parte de terceros (visitas u operarios) dirigida al área de TI. Se brindaron capacitaciones a los usuarios de TI y otras áreas del entorno a la seguridad física; además, se elaboró un formato de registro de visitas y operarios que ingresan a las instalaciones de la organización, añadiendo a ello la elaboración de medios de identificación físico (fotocheck). Todo esto contó con la debida aprobación del jefe del área de TI de la Unión Peruana del Norte con la validación de la especialista en el tema.

En el Anexo 39 se aprecia el formato de ficha de capacitaciones sobre la importancia de la seguridad física, en el Anexo 40 el formato de registro de capacitación sobre la importancia de la seguridad física, en el Anexo 41 el Formato de Solicitud de Peticiones de Acceso a las instalaciones, en el Anexo 42 el Formato de registro de las peticiones formales de acceso, en el Anexo 43 el Formato de registro de visitas u operarios a las instalaciones del

área de TI de la UPN, en el Anexo 44 el Formato de registro del personal no autorizado y que no lleve identificación en las instalaciones de la UPN, y por último en el Anexo 45 el diseño de fotocheck elaborado para los visitantes y operarios & Señalizaciones de seguridad.

- **Control 12.2.1 – "Controles contra el código malicioso":** El motivo por el cual se optó realizar el procedimiento denominado "Procedimiento para la protección contra el código malicioso", fue para asegurar y salvaguardar que los recursos y/o activos que procesan y transmiten información estén asegurados contra el código malicioso, así mismo, implementar medidas de detección, recuperación y prevención, que sirvan como resguardo contra el código malicioso, tal como el uso de un software para la detección de código malicioso, además de una adecuada concienciación a los usuarios sobre seguridad. Para ello se requiere tomar en consideración las actividades y tareas que se mencionan dentro del informe, las cuales fueron definidas en relación a lo descrito en este control. El desarrollo de este procedimiento también se dio, puesto para cumplir con las actividades de la primera práctica de Gestión del proceso DSS05, se requiere de este procedimiento. Dentro del contenido del informe está definido quienes cooperaron en elaboración de este procedimiento, el diagrama del procedimiento con sus listas de tareas, un informe conciso del procedimiento elaborado, los roles que intervienen o interactúan en el procedimiento, además de una descripción general del flujo, donde se detalla la actividad que realiza, el rol que interactúa en el procedimiento, las tareas contenidas dentro de las actividades, y los documentos o entregables que se generan, y por ultimo las contingencias.

Este procedimiento fue revisado por docentes especializados para su evaluación, levantando observaciones que fueron validadas mediante firma por un documento de conformidad por parte del especialista. En el Anexo 26 se aprecia el Informe del Procedimiento para la protección contra el código malicioso, y en el Anexo 50 la Validación del procedimiento por parte de los especialistas. En el Anexo 32 se visualiza la

Documentación general sobre el software antivirus que el área de TI maneja. En el Anexo 33 se visualiza el formato de la ficha de capacitaciones sobre el código malicioso, y en el Anexo 34 se observa el formato registro de las capacitaciones y entrenamiento sobre el software malicioso y por último en el Anexo 35 el formato de Registro de Amenazas identificadas en las evaluaciones de los activos relacionadas a los códigos maliciosos.

- **Control 12.6.1 – "Gestión de vulnerabilidades técnicas":** El motivo por el cual se optó realizar el procedimiento denominado "Procedimiento para la gestión de vulnerabilidades técnicas", fue para reducir y minimizar los riesgos y amenazas resultantes de la explotación de las vulnerabilidades técnicas. Las actividades que se realizan en este procedimiento, permiten obtener información eficaz acerca de las vulnerabilidades técnicas de los softwares utilizados, además de adoptar medidas oportunas para afrontar los riesgos asociados a los softwares. Otro punto es que permite definir y establecer funciones a los usuarios en torno a las medidas adoptadas, y de realizar un seguimiento y verificación de las medidas que se adoptaron para la correcta gestión de vulnerabilidades técnicas, todo esto se definió en relación a lo descrito en este control. El desarrollo de este procedimiento también se dio, puesto para cumplir con algunas de las actividades de la primera práctica de Gestión del proceso DSS05, requerían de este procedimiento.

Dentro del contenido del informe, está definido quienes cooperaron en elaboración de este procedimiento, el diagrama del procedimiento con sus listas de tareas, un informe conciso del procedimiento elaborado, los roles que intervienen o interactúan en el procedimiento, además de una descripción general de flujo, donde se detalla la actividad que realiza, el rol que interactúa en el procedimiento, las tareas contenidas dentro de las actividades, y los documentos o entregables que se generan, y por ultimo las contingencias.

Este procedimiento fue revisado por docentes especializados para su evaluación, levantando observaciones que fueron validadas mediante una firma de un documento de

conformidad por parte del especialista. En el Anexo 25 se aprecia el Informe del Procedimiento para la gestión de vulnerabilidades técnicas y en el Anexo 50 la Validación del procedimiento por parte de los especialistas.

Del mismo modo, se desarrolló formatos en Word y formatos de registros en Excel para poder cumplir en lo establecido en algunos de los ítems de las listas de chequeo. Cada formato fue realizado por los investigadores (nosotros) y contó con la aprobación del jefe de área de TI y nuestra asesora, los cuales se ven reflejados en los Anexos, del cual en el Anexo 36 se aprecia el Formato de Registro de dispositivos autorizados a la información y a la red, en el Anexo 37 el Formato para la eliminación de Equipos Tecnológicos y mecanismos para la eliminación de la información, en el Anexo 38 el Formato de Registro de los derechos de acceso según los roles y responsabilidades de los usuarios, en el Anexo 46 el Manual de perfil de acceso físico al área de TI, en el Anexo 48 el Formato de Registro de Inventariado de documentos sensibles, y en el Anexo 49 el Formato de Registro de Inventariado de conciliación de documentos sensibles y dispositivos de salida. Se cumplió en mayor porcentaje lo que indica la norma y por ello se cumplió en gran parte con la lista de chequeo. Todo esto de la misma forma contó con la validación y aceptación del jefe del área de TI y la especialista en el tema.

4.5. Fase 5: Evaluación de la mejora del nivel de seguridad con la ISO 27002

4.5.1. Actividad 1: Determinar el nivel de capacidad del proceso.

Luego de la implementación de los controles del plan de tratamiento de riesgo se realizó la segunda evaluación en base a la misma herramienta, que fue diseñada durante la primera evaluación, con el fin de obtener resultados satisfactorios por medio de la implementación de los controles. Al igual que en la primera evaluación, esta se realizó en conjunto con el jefe del área de TI, durante el desarrollo de esta auditoría se pudo apreciar un cambio significativo en las actividades las cuales ellos no cumplían, y que ahora por lo

realizado en la implementación, se logró tener una mejora. Esta auditoría tuvo una duración de 2 horas. Los resultados de esta evaluación fueron compartidos con el jefe del área de TI, el cual dio su aprobación y validación correspondiente, al igual que la especialista en el tema. Al igual que en la primera auditoria, se determinó el nivel de capacidad mediante el PAM de COBIT.

En la Tabla 16 se observa el cuadro de evaluación y resultado obtenido por cada criterio de evaluación en base a la escala de evaluación del PAM.

Tabla 16:
Cuadro de evaluación y resultado obtenido por cada criterio de evaluación en base a la escala de evaluación del PAM

CRITERIOS DE EVALUACIÓN	**ESCALA DE EVALUACIÓN**			
	No Logrado (0-15%)	**Parcialmente logrado (15% -50%)**	**En gran medida logrado (50% - 85%)**	**Totalmente logrado (85% - 100%)**
C1) DSS05-O1 Las redes y la seguridad de las comunicaciones responden a las necesidades del negocio."			73%	
C2) DSS05-O2 "La información procesada, almacenada y transmitida por dispositivos de punto final está protegida"			84%	
C3) DSS05-O3 "Todos los usuarios son identificables de forma única y tienen derechos de acceso de acuerdo con su función comercial"				90%
C4) DSS05-O4 "Se han implementado medidas físicas para proteger la información del acceso, daño e interferencia no autorizados al ser procesados, almacenados o transmitidos"				100%
C5) DSS05-O5 "La información electrónica está debidamente protegida cuando se almacena, transmite o destruye."			73%	
Porcentaje Alcanzado		**84% En gran medida logrado**		

Fuente: Elaboración propia

En el Anexo 51 se observa la segunda evaluación por cada lista de chequeo.

4.5.2. Actividad 2: Elaborar el informe después de la 2da evaluación.

Este informe contiene los resultados de la segunda evaluación, así como en la primera evaluación. Se utilizó los criterios de evaluación para medir el nivel de seguridad en el área de TI de la Unión Peruana del Norte, este informe contó con la aprobación del jefe de TI y la especialista en el tema. Este informe pasó previa revisión para medir con exactitud la seguridad de la información. En el Anexo 52 se aprecia el segundo informe de auditoría.

4.5.3. Actividad 3: Evaluación de la mejora.

En esta actividad se realizó la comparación de las dos auditorías realizadas, analizando las diferentes acciones que se desarrolló en cada evaluación, la cual constó con los dos informes del Proceso de Autoevaluación de Cobit (PAM). Se analizó en qué lista de evaluación se encontró la mejora, además se evaluó si existió una mejora en la seguridad de la información de la Unión Peruana del norte. En el capítulo 5 se tiene un mejor detalle y resultados de lo que se planteó realizar en el proyecto.

4.5.4. Actividad 4: Realizar el informe de la mejora.

Como última etapa de la fase y de la metodología en general, se realizó la documentación general del informe de la mejora, llegando a ver los resultados obtenidos y que de gran manera ayudaron a cumplir con el objetivo establecido en la investigación, el cual fue el de mejorar el nivel de seguridad física y lógica de información. Los resultados fueron satisfactorios para el área de TI puesto que hubo una gran mejora en el nivel de seguridad de la información. Esto fue validado por el jefe del área de TI, el cual dio su aprobación y su conformidad correspondiente por el desarrollo completo de la investigación en general. En el Anexo 53 se observa el Informe de la mejora, y en el Anexo 54 el Acta de Conformidad con los resultados obtenidos en el proyecto por parte del Área de TI de la Unión Peruana del Norte, lo cual certifica que el proyecto en su totalidad tuvo una buena aceptación y sobre toda una mejora en nivel de seguridad lógica y física y de la información.

CAPÍTULO V: RESULTADOS DE LA INVESTIGACIÓN

5.1. Criterios de evaluación del Modelo de Evaluación de Procesos (PAM)

Este capítulo presenta los resultados obtenidos de la primera y segunda evaluación, se hace esta comparación para saber cuáles son los resultados de mejora para la seguridad de la información, aquí se explicó criterio por criterio, donde el proceso DSS05 cuenta con 5 criterios de evaluación, las cuales se asocian a las 7 prácticas del proceso. A continuación se detalla el resultado de cada criterio.

5.1.1. Criterio 01 DSS05.01: "Las redes y la seguridad de las comunicaciones responden a las necesidades del negocio".

El primer criterio de evaluación está definido por 3 Prácticas (listas chequeo), las cuales son: Práctica 01, Práctica 02 y Práctica 07. Estas prácticas contienen el valor alcanzado durante la primera evaluación del proceso Cobit. Ahí se define qué ítems no fueron alcanzados, y qué controles permiten mejorar el desarrollo de este criterio:

- **Práctica 01: "Proteger Contra Software Malicioso"**

Para el cumplimiento de esta práctica se elaboraron 8 ítems, las cuales permitirán cumplir con el desarrollo del proceso DSS05, del cual 5 ítems de ellos fueron realizados por el área de TI de la UPN y 3 de ellos no lo realizan. Los ítems restantes que faltan cumplir son:

a) Actividad 2: Que no existe un procedimiento de prevención frente al ataque de un código malicioso.

b) Actividad 5: Que no se realiza evaluaciones para detectar vulnerabilidades antes de que sean una amenaza.

c) Actividad 6: Que no existe un registro de amenaza identificadas en las evaluaciones.

- **Práctica 02: "Gestionar la seguridad de la red y las conexiones"**

Para el cumplimiento de esta práctica se elaboraron 8 ítems, las cuales permitirán cumplir con el desarrollo del proceso DSS05, del cual 5 ítems de ellos fueron realizados por el área de TI de la UPN y 3 de ellos no lo realizan. Los ítems restantes que faltan cumplir son:

a) Actividad 4: Que la información de la empresa no se encuentra clasificada según su criticidad e importancia.

b) Actividad 5: Que la información no está cifrada para su tránsito en la red según su clasificación.

c) Actividad 8: Que no realiza pruebas de intrusión para ver el nivel de seguridad que se encuentra la red.

- **Práctica 07: "Supervisar la infraestructura para detectar eventos relacionados con la seguridad**"

Para el cumplimiento de esta práctica se elaboraron 7 ítems, las cuales permitirán cumplir con el desarrollo del proceso DSS05, del cual 2 ítems de ellos fueron realizados por el área de TI de la UPN y 5 de ellos no lo realizan. Los ítems restantes que faltan cumplir son:

a) Actividad 01: Que no se registran los eventos relacionados con la seguridad, considerando el nivel de la información.

b) Actividad 02: Que los registros de seguridad no son guardados durante un periodo apropiado para ayudar en futuras investigaciones.

c) Actividad 03: Que la naturaleza y características de los incidentes potenciales relacionados con la seguridad no están definidas.

d) Actividad 06: No existe un procedimiento que recopile la evidencia de los incidentes de seguridad.

e) Actividad 07: Que los empleados no conocen los resultados de la recopilación de la evidencia de un incidente de seguridad.

Finalmente, como se puede apreciar en la Figura 17, se encuentran los resultados obtenidos por cada práctica: Práctica 01, Práctica 02 y Práctica07, estableciendo que porcentaje positivo y negativo se encuentra en cada una de ellas.

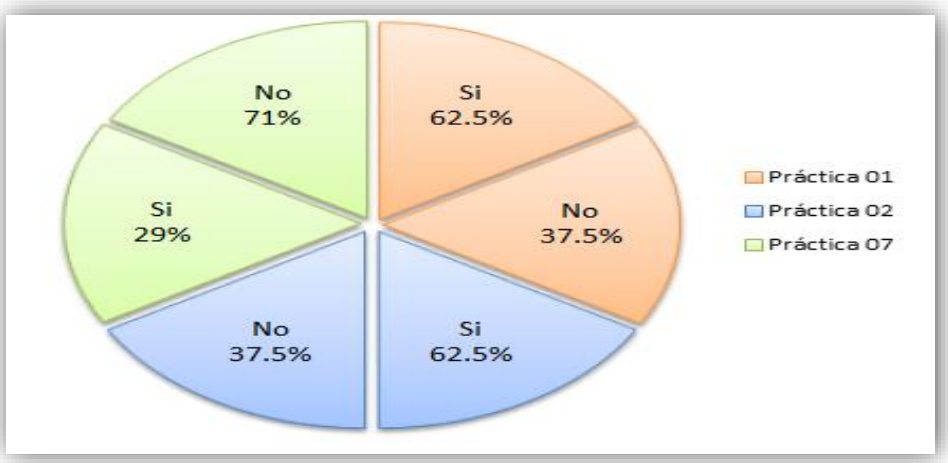


Figura 17: Resultados de las 3 Prácticas: Práctica 01, Práctica 02 y Práctica07
(*Fuente:* Elaboración Propia**)**

Como resultado de la primera evaluación del primer criterio, se logró tener un 51% tal como muestra la Figura 18, donde el rango de medición alcanzado del PAM es **"En gran medida logrado".**

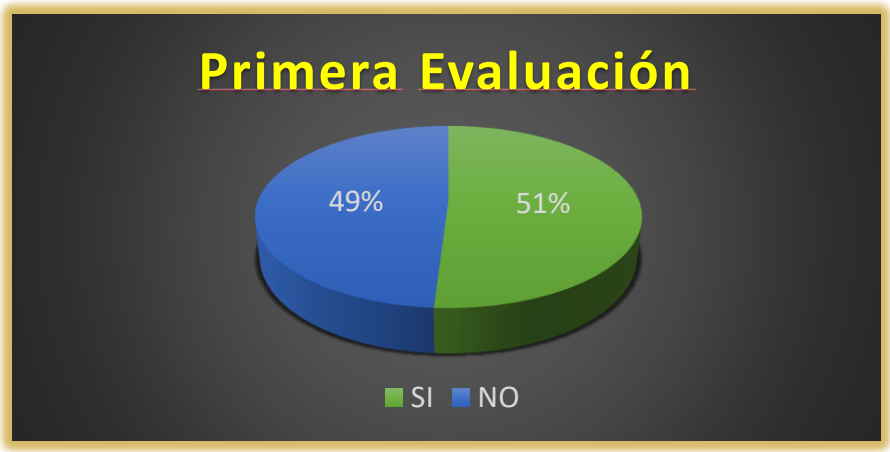


Figura 18: resultado de la primera evaluación del primer criterio de Cobit
(*Fuente*: Elaboración Propia**)**

Reducción del criterio DSS05.01: "Supervisar la infraestructura para detectar eventos relacionados con la seguridad"

- **Práctica 01: "Proteger Contra Software Malicioso"**

a) Para cumplir con la actividad 2, se implementó el control **12.2.1**: **"Controles contra código malicioso",** que permite cumplir con lo descrito en la actividad. Esta implementación hizo que el ítem cambie a positivo en la segunda evaluación, logrando mejorar con lo expuesto.

b) La actividad 5 tuvo que implementar el siguiente control **12.6.1: "Gestión de las vulnerabilidades técnicas",** esta implementación permitió cumplir con la actividad de forma positiva, logrando mejorar lo realizado en la primera evaluación.

c) Por último, la actividad 6 se requirió hacer la implementación del control **5.1.1: "Políticas de seguridad de la información",** fue descrita como norma y se realizó un registro que permita cumplir con la actividad mencionada.

- **Práctica 02: "Gestionar la seguridad de la red y las conexiones"**

a) Para cumplir con la actividad 04 de la Práctica 02 se implementó el control **8.2.1: "Clasificación de la información"**, que permitió mejorar la lista de evaluación

b) Para la actividad 05 no se implementó el control seleccionado **10.1.1: "Política de uso de los controles criptográficos",** no lo puede realizar la organización ya que está fuera de presupuesto para los investigadores y por ende merece gestionarse por otra entidad capaz de desarrollar tal actividad y por tal motivo se mantiene en negativo en la evaluación.

c) Para la actividad 08 tampoco se implementó el control seleccionado **13.1.2: "Seguridad de los servicios de red"** puesto que se requieren inversión y la organización no tiene el presupuesto necesario para gestionar tal servicio, pero se le entregó un documento de normas para cumplir con el control en un futuro y por ello se mantienen en negativo en la evaluación.

➢ **Práctica 07: "Supervisar la infraestructura para detectar eventos relacionados con la seguridad"**

a) En esta práctica solo se redujo la actividad 03, que fue implementado por el control **5.1.1: "Políticas para la seguridad de la información",** fue puesto como norma y también se obtuvo el registro necesario, esto permite que mejore la Práctica 07.

b) Para las demás actividades 01, 02, 06 y 07 también se utilizó el control mencionado en la parte superior, con la diferencia que fueron descritos como normas de seguridad en la organización, pero no se pudo tener el registro para cumplir con la práctica y por ende los ítems se mantienen en negativo.

Con la implementación de los controles mencionados en este primer criterio de evaluación, se logra mejorar un **22%**, logrando alcanzar un **73%** en la segunda evaluación tal como muestra la Figura 19, donde el rango alcanzado es **"En gran medida logrado"**, cumpliendo con el objetivo trazado.

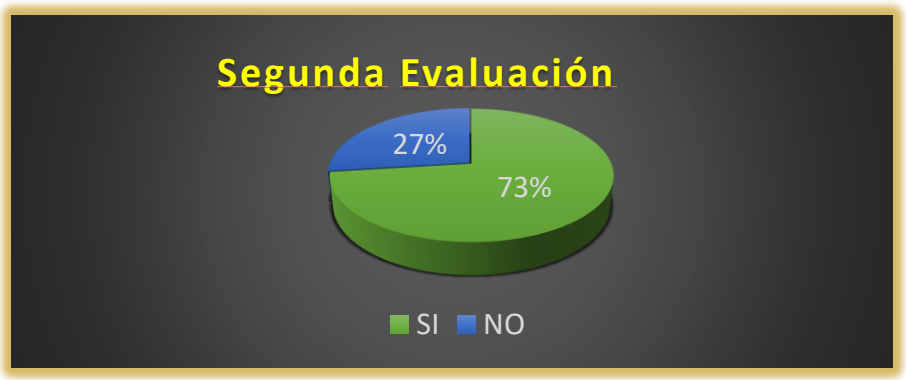


Figura 19: *resultado de la segunda evaluación del primer criterio de Cobit*
(*Fuente:* Elaboración Propia**)**

5.1.2. Criterio 02 DSS05.02: "La información procesada, almacenada y transmitida por dispositivos de punto final está protegida".

El segundo criterio de evaluación está definido por 2 Prácticas (listas chequeo), las cueles son: Práctica 01 y Práctica 03. Estas prácticas contienen el valor alcanzado durante la

primera evaluación del proceso Cobit. Ahí se define qué ítems no fueron alcanzados y qué controles permiten mejorar el desarrollo de este criterio.

- **Práctica 01: "Proteger Contra Software Malicioso"**

Esta práctica contiene 8 ítems que indican las actividades de esta práctica de gestión, que permite conocer si se cumple con lo descrito por cada ítem. De la cual para esta práctica 5 ítems fueron realizados por el área de TI de la UPN y 3 de ellos no lo realizan, los ítems restantes las cuales falta cumplir son:

a) Actividad 02: Que no existe un procedimiento de prevención frente al ataque de un código malicioso.

b) Actividad 05: Que no se realiza evaluaciones para detectar vulnerabilidades antes de que sean una amenaza.

c) Actividad 06: Que no existe un registro de amenaza identificadas en las evaluaciones.

- **Práctica 03: "Gestionar la seguridad de los puestos de usuario final"**

Esta práctica está conformada por 9 ítems que indican que actividades deben cumplirse, teniendo como objetivo mejorar el nivel de seguridad, la organización cumple con 5 ítems y la diferencia no lo realizan, los ítems restantes las cuales falta cumplir son:

a) Actividad 01: El sistema operativo de todas las computadoras (portátiles, de escritorio y servidores), no cuentan con la última actualización publicada

b) Actividad 03: No se cifra la información almacenada de la organización según su clasificación

c) Actividad 06: No se implementa el filtrado de tráfico de red en dispositivos de usuario final.

d) Actividad 07: Que la integridad de la información no es protegida en los puestos de usuario final

Finalmente, como se puede apreciar en la Figura 20, se encuentra los resultados obtenidos por cada práctica: Práctica 01 y Práctica 03, estableciendo qué porcentaje positivo y negativo se encuentra en cada una de ellas.

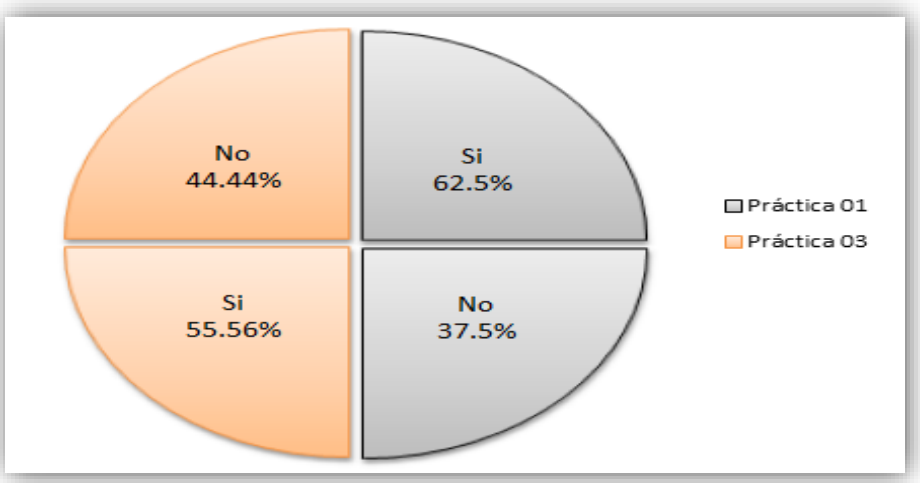


Figura 20: Porcentajes de las 2 listas de evaluación: Práctica 01 y Práctica03
(*Fuente*: Elaboración Propia**)**

El resultado durante la primera evaluación del segundo criterio fue: un **59%** tal como se muestra en la Figura 21 donde el rango de medición del PAM es **"En gran medida logrado"**.

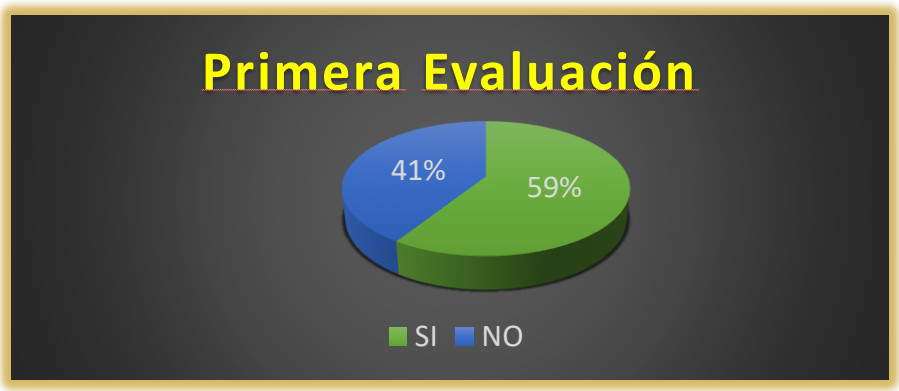


Figura 21: resultado de la primera evaluación del segundo criterio de Cobit
(*Fuente*: Elaboración Propia**)**

Reducción del criterio DSS05.02: "La información procesada, almacenada y transmitida por dispositivos de punto final está protegida"

- **Práctica 01: "Proteger Contra Software Malicioso"**

a) La reducción de esta práctica está definida en el primer criterio de evaluación, donde se detalla los controles implementados para mejorar la seguridad de la información, ahí indica que se hizo para cumplir con la práctica mencionada.

- **Práctica 03: "Gestionar la seguridad de los puestos de usuario final"**

a) Para la actividad 01, se implementó el control **5.1.1: "Políticas de seguridad de la información"** logrando crear la norma y el registro necesario cumpliendo con la actividad y mejorando la Practica 03.

b) Para la actividad 03 no se implementó nada puesto que el control seleccionado **10.1.1: "Política de uso de los controles criptográficos"** no lo puede realizar la organización ya que está fuera de presupuesto para los investigadores y por ende merece gestionarse por otra entidad capaz de desarrollar tal actividad y por tal motivo se mantiene en negativo en la evaluación.

c) Para la actividad 06 y 07 tampoco se implementó el control seleccionado **13.1.1: "Controles de red"** puesto que se requieren inversión y la organización no tiene el presupuesto necesario para gestionar tal servicio, pero se le entrego un documento de normas para cumplir con el control en un futuro y por ello se mantienen en negativo en la evaluación.

Con la implementación de los controles mencionados en este segundo criterio, se logra mejorar un **25%**, logrando alcanzar un **84%** durante la segunda evaluación, tal como se muestra en la Figura 22, donde el rango alcanzado es **"En gran medida logrado"**, cumpliendo con el objetivo trazado.

Figura 22: resultado de la segunda evaluación del segundo criterio de Cobit
(*Fuente*: Elaboración Propia**)**

5.1.3. Criterio 03 DSS05.03: "Todos los usuarios son identificables de forma única y tienen derechos de acceso de acuerdo con su función comercia".

El tercer criterio de evaluación solo está compuesto por una Práctica (listas chequeo), la cual es la Práctica 04. La práctica en mención contiene el porcentaje alcanzado durante la primera evaluación, ahí se define que ítems no fueron alcanzados y que controles permiten mejorar el desarrollo de este criterio.

- **Práctica 04: "Gestionar la identidad del usuario y el acceso lógico"**

  Esta práctica contiene 10 ítems que indican las actividades de la práctica de gestión mencionada, donde permite conocer si cumple o no con lo descrito por cada ítem. De la cual para esta práctica 4 ítems fueron realizados por el área de TI de la UPN y 6 de ellos no lo realizan. Los ítems que faltan cumplir son:

a) **Actividad 01**: Se mantiene los derechos de acceso de los usuarios de acuerdo al proceso de negocio.

b) **Actividad 05**: Las unidades de negocio gestionan la autenticación con aplicaciones para ver si los accesos a los activos de información fueron bien administrados.

c) **Actividad 06** Los cambios efectuados en los perfiles de usuario se registra y monitorea solo con la aprobación del responsable del área

d) Actividad 08: Se revisa periódicamente los privilegios asignados a las cuentas del usuario.

e) Actividad 09: Se identifica unívocamente todas las actividades de proceso realizadas por el usuario.

f) Actividad 10: Se mantiene un registro del acceso lógico a la información altamente sencilla.

Finalmente, como se puede apreciar en la Figura 23, se encuentra el resultado obtenido de la primera evaluación por el tercer criterio, estableciendo que porcentaje positivo y negativo e encuentra. El resultado del tercer criterio de evaluación fue: un **40%** donde el rango de medición del PAM es **"Parcialmente Logrado".**

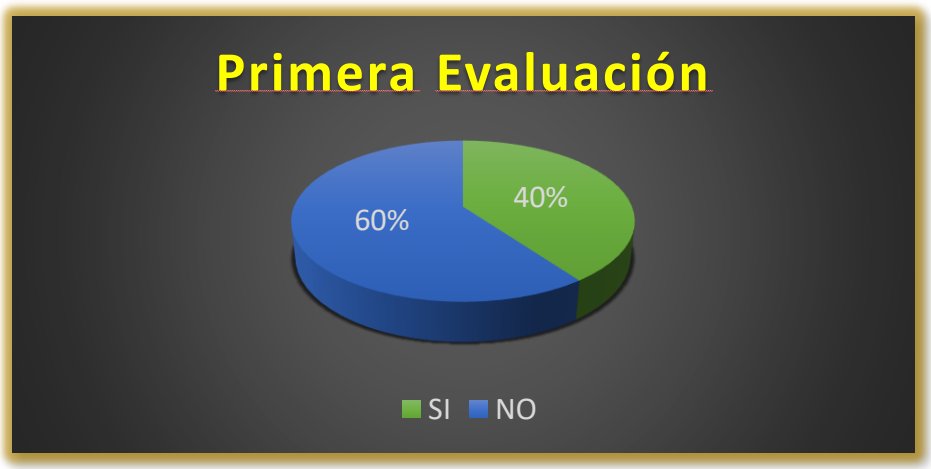


Figura 23: resultado de la primera evaluación del tercer criterio de Cobit
(*Fuente*: Elaboración Propia**)**

Reducción del criterio DSS05.03: "Todos los usuarios son identificables de forma única y tienen derechos de acceso de acuerdo con su función comercia"

Para la actividad 01 y 09 se implementó el control **9.1.1: "Políticas de control de acceso"**, dado que para la primera práctica sí cumple con lo establecido y existe un registro de ello, eso beneficia que la segunda evaluación sea positiva para la organización, pero en la práctica 09 se realizó la norma de las políticas, pero no existe un registro de ello, y eso permite que todavía se mantenga en negativo la actividad mencionada.

a) Para la actividad 05 se implementó el control **9.4.2:" Procedimientos seguros de inicio de sesión"**. La implementación del control mencionado permite cumplir con la actividad, y hace que la segunda evaluación sea positiva y mejore a la organización.

b) Las actividades 06 y 08 se necesitó unir 5 controles que son: **9.2.1: "Registro y baja de usuario"**, **9.2.2: "Provisión de acceso de usuario"**, **9.2.3: "Gestión de privilegios de acceso"**, **9.2.5: "Revisión de los derechos de acceso de usuario"** y **9.2.6: "Retirada o reasignación de los derechos de acceso"**, para cumplir con las actividades, esto permite tener un cambio positivo en la segunda evaluación.

c) Por último, la actividad 10 se implementó el control **5.1.1: "Políticas de seguridad de la información"** logrando crear la norma (política) y el registro necesario cumpliendo con la actividad y mejorando la Práctica 04.

Con la implementación de los controles mencionados en este tercer criterio de evaluación, se logra mejorar un **50%** en la segunda evaluación, logrando alcanzar un **90%** de mejora tal como muestra la Figura 24, donde el rango alcanzado es **"Totalmente logrado"**, cumpliendo con el objetivo trazado.

Figura 24: resultado de la segunda evaluación del tercer criterio de Cobit
(*Fuente:* Elaboración Propia**)**

5.1.4. Criterio 04 DSS05.04: “Se han implementado medidas físicas para proteger la información del acceso, daño e interferencia no autorizados al ser procesados, almacenados o transmitidos”.

El cuarto criterio de evaluación solo está compuesto por una Práctica (listas chequeo), la cual es la Práctica 05. La práctica contiene el porcentaje logrado en la primera evaluación, donde define qué ítems no fueron alcanzados y qué controles permiten lograr el desarrollo de este criterio.

- **Práctica 05: “Gestionar el acceso físico a los activos de TI”**

Esta práctica contiene 12 ítems que indican las actividades de la práctica de gestión, que permite conocer si cumple o no con lo descrito por cada ítem. De la cual para esta práctica 7 ítems fueron realizados por el área de TI de la UPN y 5 de ellos no lo realizan, los ítems restantes que faltan cumplir son:

a) Actividad 02: No se gestiona las concesiones de acceso a áreas de instalación y procesamiento.

b) Actividad 03: No son completadas las peticiones formales de acceso

c) Actividad 06: No se registra y supervisa el acceso a las ubicaciones de TI. (visitantes, proveedores, personal, etc.).

d) Actividad 07: El personal del área de TI no mantiene visible la identificación en todo momento (fotochet, placa o tarjeta).

e) Actividad 11: No se establecen restricciones en el perímetro tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores para restringir el acceso a ubicaciones de TI sensibles.

Finalmente, como se puede apreciar en la Figura 25, se encuentra el resultado obtenido en la primera evaluación por el cuarto criterio, estableciendo que porcentaje positivo y negativo se encuentra.

El resultado del cuarto criterio de evaluación fue: un **58%** donde el rango de medición del PAM es **"En gran medida logrado".**

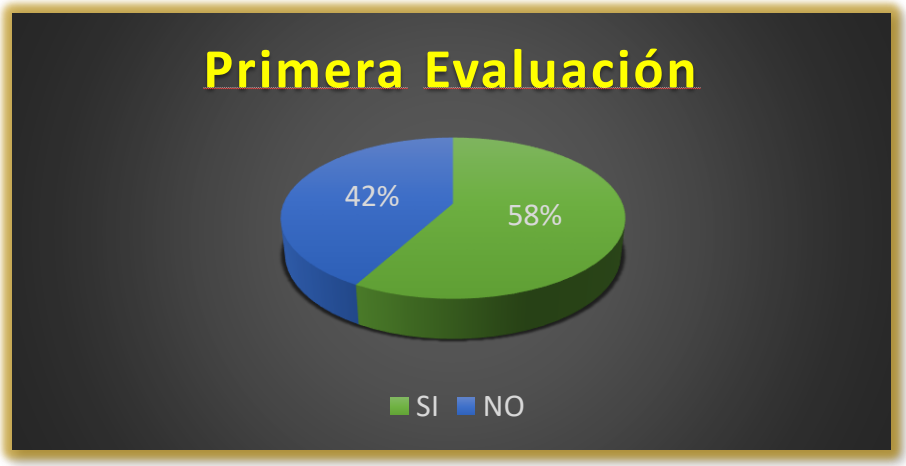


Figura 25: resultado de la primera evaluación del cuarto criterio de Cobit
(*Fuente:* Elaboración Propia**)**

Reducción del criterio DSS05.04: "Se han implementado medidas físicas para proteger la información del acceso, daño e interferencia no autorizados al ser procesados, almacenados o transmitidos"

a) Para las actividades 02, 06 y 07**,** se implementó el control **11.1.2: "Controles físicos de entrada"**, estableciendo lo que el control indica, cumpliendo con las actividades, esto permite un cambio positivo en la segunda evaluación.

b) Para la actividad 03, se implementó el control **5.1.1: "Políticas de seguridad de la información"** logrando crear la norma (política) y el registro necesario cumpliendo con la actividad y mejorando la Práctica 05.

c) Por último, para la actividad 11, se implementó el control **11.2.1: "Controles físicos de entrada"**, que permiten mejorar la actividad descrita y beneficia a la organización.

Con la implementación de los controles mencionados y de la inversión establecida en este cuarto criterio, se logra mejorar un **42%** en la segunda evaluación, logrando alcanzar el **100%** de mejora tal como indica la Figura 26, donde el rango alcanzado es **"Totalmente logrado"**, cumpliendo con el objetivo trazado.

Figura 26: resultado de la segunda evaluación del cuarto criterio de Cobit
(*Fuente:* Elaboración Propia**)**

5.1.5. Criterio 05 DSS05.05: "La información electrónica está debidamente protegida cuando se almacena, transmite o destruye".

El quinto criterio de evaluación solo está compuesto por una Práctica (listas chequeo), la cual es la Práctica 06. La práctica contiene el porcentaje logrado en la primera evaluación, donde define que ítems no fueron alcanzados y que controles permiten lograr el desarrollo de este criterio:

- **Práctica 06: "Gestionar Documentos sensibles y dispositivos de salida"**

Esta práctica contiene 11 ítems que indican las actividades de la práctica de gestión, que permite conocer si cumple o no con lo descrito por cada ítem. De la cual para esta práctica 3 ítems fueron realizados por el área de TI de la UPN y 8 de ellos no lo realizan, los ítems restantes que faltan cumplir son:

a) Actividad 01: No cuenta con procedimientos para recepción de documentos especiales**.**

b) Actividad 02: No cuenta con procedimientos para el uso de documentos especiales.

c) Actividad 04: No asignan privilegios de acceso a documentos sensibles de acuerdo a su importancia.

d) Actividad 06: No **e**xiste un inventario de dispositivos de salida**.**

e) Actividad 07: No realizan un inventario de conciliaciones de documentos sensibles y dispositivos de salida**.**

f) Actividad 08: Existe controles de seguridad físicas para los formularios especiales**.**

g) Actividad 09: Existe controles de seguridad física para los dispositivos sensibles**.**

h) Actividad 11: Se tiene un modelo de arquitectura de la información**.**

Finalmente, como se puede apreciar en la Figura 27, se encuentra el resultado obtenido por el quinto criterio, estableciendo que porcentaje positivo y negativo se encuentra. El resultado del quinto y último criterio de evaluación fue: un **27%** donde el rango de medición del PAM es **"Parcialmente logrado".**

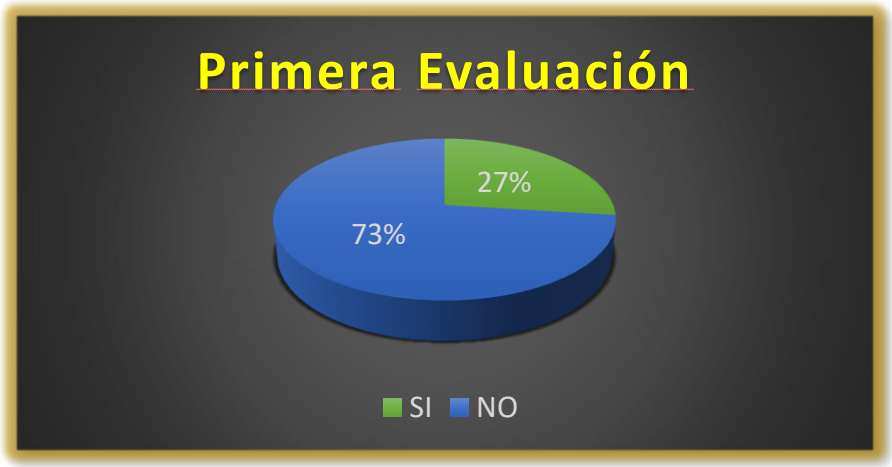


Figura 27: resultado de la primera evaluación del quinto criterio de Cobit
(***Fuente***: Elaboración Propia)

Reducción del criterio DSS05.05: "La información electrónica está debidamente protegida cuando se almacena, transmite o destruye"

a) Para las actividades 01, 02 y 04**,** se implementó el control **8.2.1: "Clasificación de la información"**. Este control beneficia en el cumplimiento de las actividades mencionadas, permitiendo que en se genere un resultado positivo en la segunda evaluación.

b) Para la actividad 06 y 07, se implementó el control 8**.1.1: "Inventario de activos"**. La implementación permite mejorar las actividades mencionadas para lograr una mejora en la lista de evaluación.

c) Para las actividades 08 y 09 se implementó el **control 11.1.2: "Controles físicos de entrada"**. Estas fueron colocadas mediante políticas de seguridad, pero aún no se encuentra registro de las normas descritas en las políticas; por tal motivo, al no existir registro las actividades quedan en negativo.

d) Para la actividad 11, se implementó también el control mencionado en la Práctica 07, con la diferencia que fue descrito como norma de seguridad en la organización, pero faltaba aún tener un registro de ello, por ende, los ítems se mantienen en negativo.

Con la implementación de los controles en el quinto y último criterio de evaluación, se logra mejorar un 46 % en la segunda evaluación, esto permite alcanzar un **73%** de mejora tal como indica la Figura 28, la cual el rango alcanzado es **"En gran medida logrado"**, cumpliendo con el objetivo trazado.

Figura 28: resultado de la segunda evaluación del quinto criterio de Cobit (***Fuente***: Elaboración Propia)

5.2. Comparativa de Resultados de la Primera evaluación con la Segunda evaluación

Durante la etapa de auditoria se realizaron dos evaluaciones para medir el nivel de la seguridad de la información en el área de TI de la Unión Peruana del Norte, donde se permite conocer al detalle cómo se cumplieron los criterios de evaluación del PAM de Cobit.

La Figura 29 detalla el resultado alcanzado en ambas evaluaciones, que es el promedio de los 5 criterios de evaluación. En la primera evaluación de color azul, cada criterio está por debajo del 100%, lo que indica que en conjunto logran alcanzar un 47%, que significa que se encuentra el nivel de seguridad "**Parcialmente logrado**", la segunda escala de medición del PAM, luego vemos que en la segunda evaluación de color anaranjado, hay un incremento en el porcentaje por cada criterio de evaluación, luego de la implementación de los controles, alcanzando un 84% en el nivel de seguridad "**En gran medida logrado**", mejorando la seguridad de la información de la Unión Peruana del Norte. Esto permite cumplir con el objetivo trazado en la investigación.

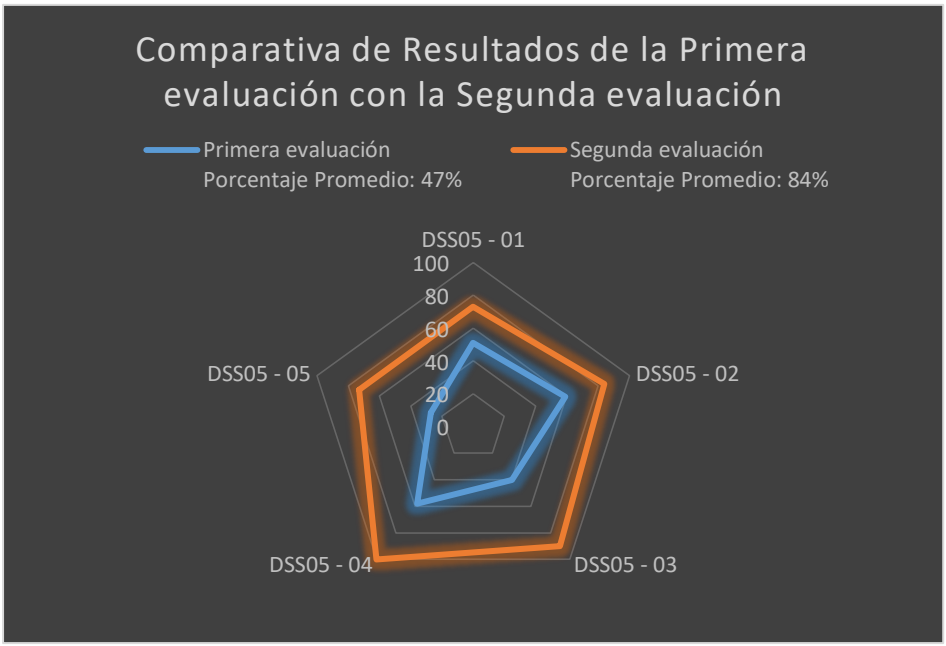


Figura 29: Resultados de la Primera evaluación con la Segunda evaluación (***Fuente:*** Elaboración propia)

Conclusiones:

- La implementación de los controles de la ISO/IEC 27002:2013 mejoró significativamente el nivel de seguridad de la información, puesto que durante la primera evaluación se obtuvo un resultado inicial de 47% y en la segunda evaluación ya con los controles implementados se obtuvo un resultado de 84%. Donde concluyó que la diferencia encontrada entre ambos resultados, mejoró en un 37% de la seguridad física y lógica de la información.
- La auditoría inicial permitió conocer cuáles son las fallas de los procesos del área de TI. Esto requiere que se implemente los controles de la ISO/IEC 27002: 2013 mejorando los procesos del negocio, haciendo que se tenga un mejor control de sus funciones.
- El desarrollo del análisis de riesgo permitió identificar que controles de la ISO/IEC 27002: 2013 se asocia al riesgo detectado, lo que implica que el riesgo cuyo valor de criticidad en nivel alto, sea tratado con mayor importancia.
- La elaboración del plan de tratamiento de riesgo permitió implementar los controles de la norma ISO/IEC 27002:2013 identificados, las cuales redujeron el impacto que ocasionan los riesgos en el área de TI, para de esta manera tener íntegra y segura a la información.
- La auditoría posterior que se realizó con los controles de la ISO/IEC 27002:2013, permitió conocer si la organización cumple con el objetivo, la cual consistió en mejorar la seguridad física y lógica de la información.
- El proceso Cobit es un marco de referencia que cumple con los parámetros de seguridad de la información, que está alineado a las buenas prácticas y otros estándares.
- La Unión Peruana del Norte, con la mejora que se le está brindando en seguridad física y lógica, cumple con los parámetros que la norma y el proceso de evaluación requiere. Con ello busca optimizar los recursos que se encuentren dentro de ello, haciendo que la información y la infraestructura se encuentren factibles.

Recomendaciones

- Se recomienda que el área de TI de la Unión Peruana del Norte adquiera el paquete de documentación de la ISO 27001, donde encontrará más información, plantillas de documentos requeridos para la certificación de la ISO 27001, videos y consultorías en vivo, etc. Esto con el fin de poder ampliar y reforzar sus conocimientos en los temas referentes a la seguridad de la información tanto a un nivel físico como lógico.
- Se recomienda brindar capacitaciones y charlas en temas referidos a la encriptación de la información al área de TI de la UPN, puesto que actualmente ellos transfieren este proceso de encriptación de la información a unos expertos en el tema. Con esto, ellos lograrán brindar una seguridad más eficiente y seguras en los sistemas de información y/o aplicaciones.
- Se recomienda que se implementen los controles restantes de los 24 que se llevaron a cabo en el Plan de Tratamiento (PTR), para así tener segura la información en su totalidad, y así se eviten futuros riesgos que pudiesen perjudicar a la organización.
- Se recomienda que el área de TI de la Unión Peruana del Norte emplee el framework Cobit para la evaluación y cumplimiento de las actividades en general que realizan.
- Seguir con las capacitaciones brindadas al personal, en temas relacionados a la seguridad, protección y/o resguardo de la información para la buena gestión de la información.
- Revisar constantemente el cumplimiento de las políticas establecidas y a la vez lo establecido en el plan de tratamiento de riesgo por parte del personal, esto para un eficaz y eficiente aseguramiento de la información y un mejor control en la información.

Referencias

AENOR. (2015). *Norma española UNE-ISO/IEC 27002.* Madrid: AENOR.

Aguirre, J. D., & Aristizabal, C. (2013). *DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL GRUPO EMPRESARIAL LA OFRENDA.* Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf?sequence=1

Alegre, M., & Garcia, A. (2011). *SEGURIDAD INFORMATICA ED.11 Paraninfo.* Madrid: Paraninfo.

Alexander, A. G. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información Óptica ISO 27001:2005.* Bogota: Alfaomega Colombiana S.A.

ANGARITA VIVAS , A. A., & TABARES ISAZA, C. A. (Diciembre de 2012). Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/3914/T0058A581.pdf?sequence=1&isAllowed=y

Areitio, J. (2008). Entidades implicadas en la seguridad. En J. Areitio, *Seguridad de la Informacion Redes. informática y sistemas de información* (págs. 4-5). Madrid: Paraninfo.

Baca Urbina, G. (2016). *Introducción a la Seguridad Informática.* México: Grupo Editorial Patria.

BORTNIK, S. (27 de Octubre de 2014). *A la RAE: un hacker NO es un pirata informático*. Obtenido de welivesecurity Noticias, opiniones y análisis de la comunidad de seguridad de ESET: https://www.welivesecurity.com/la-es/2014/10/27/rae-hacker-no-es-pirata-informatico/

Caccuri, V. (2012). *Computación para docentes.* Buenos Aires: Fox Andina.

Cedeño Rosero, D. A. (Julio de 2017). *INFORME FINAL: "PLANES Y CONTROLES DE TRATAMIENTO DE RIESGOS TECNOLÓGICOS".* Obtenido de Repositorio Digital PUCESE: https://repositorio.pucese.edu.ec/bitstream/123456789/1148/1/CEDE%C3%91O%20ROSERO%20DAVID%20ABSALON.pdf

Córdova, J. (13 de Marzo de 2012). *Seguridad Informática y de la Información*. Obtenido de http://www.inseguridadinformatica.com/2012/03/introduccion-la-seguridad-de-la.html

Giménez, J. F. (2015). *Seguridad en equipos informáticos. IFCT0510.* Málaga: IC Editorial.

Grupo IWI. (2009). *Implantación de la LOPD en la empresa. Medidas de seguridad.* España: Vértice.

Gutiérrez, C. (12 de Diciembre de 2013). *ISO/IEC 27002:2013 y los cambios en los dominios de control*. Obtenido de Welivesecurity Noticias, opiniones y análisis de la comunidad de seguridad ESET: https://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/

Hernandez Sampieri, R. (2017). *Fundamentos de Investigación.* Ciudad de México: McGRAW - HILL/INTERAMERICANA EDITORES, S.A. .

Hernández, M. (12 de Diciembre de 2012). *Tipos y Niveles de investigación.* Obtenido de Metodología de la investigación: http://metodologiadeinvestigacionmarisol.blogspot.pe/2012/12/tipos-y-niveles-de-investigacion.html

ICETEX. (Octubre de 2014). *MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.* Obtenido de www.icetex.gov.co: https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf

infosegur. (s.f.). *Objetivos de la seguridad informática*. Obtenido de infosegur wordpress: https://infosegur.wordpress.com/tag/integridad/

ISACA. (2012). *Cobit 5: "Procesos Catalizadores".* Rolling Meadows: ISACA.

ISACA. (2013). *Guía de Auto-Evaluación: Usando COBIT 5.* Rolling Meadows: ISACA.

ISO 27001. (2012). *El portal de ISO 27001 en Español*. Obtenido de ISO 27000.es: http://www.iso27000.es/sgsi.html

ISOTools Excellence. (18 de Marzo de 2015). *NTP-ISO/IEC 17799: Norma Técnica Peruana.* Obtenido de SGSI Blog especializado en Sistemas de Gestión : https://www.pmg-ssi.com/2015/03/ntp-isoiec-17799-norma-tecnica-peruana/

Landeau, R. (2007). *Elaboración de trabajos de investigación.* Caracas: Alfa.

Lara Muñoz, E. M. (2013). *Fundamentos de Investigación Un enfoque por competencias* . C.V Mexico: AlfaOmega Grupo Editor, S.A.

Lerma, H. D. (2016). *Metodología de la investigación.* Bogota: Ecoe.

Manjón, J. M. (2015). *Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013.* Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/43102/6/manjonikoTFM0615memoria.pdf

Mazorra, M. A., Toapanta, H. J., & Briones, L. L. (2008). *"Implementar Políticas de Seguridad a Nivel de Hardware y Aplicado a una Empresa Pequeña".* Obtenido de http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/16532/Tesis.pdf?sequence=1&isAllowed=y

Mendoza, M. Á. (4 de Agosto de 2015). *COBIT para la seguridad en las organizaciones*. Obtenido de Welivesecurity Noticias, opiniones y análisis de la comunidad de seguridad ESET: https://www.welivesecurity.com/la-es/2015/08/04/practicas-cobit-seguridad-organizaciones/

Moreno, F. (2008). *Proyecto de norma técnica colombiana NTC-ISO 27005*. Colombia.

Pacheco, F., & Jara, H. (2010). *Hackers al descubierto.* Creative Andina Corp.

Parra Carrero, A. M. (Mayo de 2017). *PROYECTO Diagnóstico de la Gestion de Acceso de Usuarios en la Superintendencia de Servicios Publicos DomiciliariosNorma*. Obtenido de Repositorio Institucional UniLibre: http://repository.unilibre.edu.co/bitstream/handle/10901/10950/trabajo%20de%20grado.pdf?sequence=1

Prada, N. M. (2009). *Proyecto de Grado: "Diseño de un sistema de gestión de seguridad de la información, alineado con la norma ISO/IEC 27002, para el área de tecnología de una empresa del sector financiero.* Bogota.

Project Management Consultores de Proyectos. (2006). *Project Management Consultores*. Obtenido de Sistemas de Gestión de la Seguridad de la Informacion: ISO 27001: http://www.pmconsultores.com/portal/content.asp?ContentId=%20667

Romo Villafuerte, D., & Valarezo Constante, J. (14 de Agosto de 2012). *Repositorio Digital-UPS.* Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/3163/1/UPS-GT000319.pdf

Ruiz, M. (2012). *Enfoques cuantitativo, cualitativo y mixto*. Obtenido de eumed.net Enciclopedia Virtual: http://www.eumed.net/tesis-doctorales/2012/mirm/cualitativo_cuantitativo_mixto.html

Saavedra, C. (29 de Marzo de 2016). Entrevista personal. (S. Gavidia, & D. Torres, Entrevistadores)

SANS Securiting The Human. (Febrero de 2014). *OUCH! ¿Qué es el malware?* Obtenido de SANS Securiting The Human: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201402_sp.pdf

Valdivia, C. (2015). *Redes telemáticas.* Madrid: Paraninfo.

Viera, L. (2013). *Aplicaciones informáticas de la gestión comercial.* Málaga: IC Editorial.

Anexos

Anexo 1: Acta de Reunión N°1

ACTA DE REUNION

ACTA No. 1 de 2016	FECHA: 28/03/2016	HORA INICIO: 9:30 TERMINACIÓN 10:15	LUGAR: UPN - Chaclacayo

OBJETIVO DE LA REUNIÓN: *Entrevista con la Organización*

RESPONSABLES DE LA REUNION: *Gavidia Mamani Samuel - Torres Torres Luis*

CONVOCADOS / ASISTENTES

NOMBRES Y APELLIDOS	CARGO – DEPENDENCIA	ASISTIO SI	ASISTIO NO
Ing. Carlos Saavedra	*Jefe TI - UPN*	X	
Gavidia Mamani Samuel	*Investigador*	X	
Torres Torres Luis Daniel	*Investigador*	X	

AGENDA

1. **Entrevistar al jefe de área de TI de la UPN:**
2. **Acuerdo para la Próxima reunión**

DESARROLLO DE LA AGENDA

1. **Entrevistar al jefe de área de TI de la UPN:**

   Se recopiló información de la organización mediante la entrevista brindada, lo que nos permitió tener un mejor alcance y control de la información que se necesita para el desarrollo de nuestra investigación.

2. **Acuerdo para la Próxima reunión:**

   Estudio del área de trabajo

Firma *Jefe TI - UPN*

Código: PROC-1 Versión: 01 Pág. 1 de 8

Anexo 2: Acta de Reunión N°2

ACTA DE REUNION

ACTA No. 2 de 2016	FECHA: 04/04/2016	HORA INICIO: 10:00 TERMINACIÓN 11:00	LUGAR: UPN - Chaclacayo
OBJETIVO DE LA REUNIÓN: Hacer un estudio del área de trabajo.			
RESPONSABLES DE LA REUNION: Gavidia Mamani, Samuel			

CONVOCADOS / ASISTENTES

NOMBRES Y APELLIDOS	CARGO – DEPENDENCIA	ASISTIO	
		SI	NO
Ing. Carlos Saavedra	*Jefe TI - UPN*	X	
Gavidia Mamani Samuel	*Investigador*	X	
Torres Torres Luis Daniel	*Investigador*		X
Amelio Apaza	*Sector Educativo - financiero*	X	
Janeth Tenorio	*Sector Educativo - Académico*	X	

AGENDA

3. **Identificación de la Problemática**
4. **Acuerdo para la Próxima reunión**

DESARROLLO DE LA AGENDA

3. **Identificación de la Problemática:**

Se hizo una entrevista al jefe del área de TI y se hizo una identificación preliminar de la problemática del área.

4. **Acuerdo para la Próxima reunión:**

Presentar documento de propuesta de Investigación

Firma *Jefe TI – UPN*

Versión: 01

Pág. 2 de 8

Anexo 3: Acta de Reunión N°3

ACTA DE REUNION

ACTA No. 3 de 2016	FECHA: 18/05/2016	HORA INICIO: 10:20 TERMINACIÓN 10:50	LUGAR: UPN - Chaclacayo
OBJETIVO DE LA REUNIÓN: Presentación de la propuesta de investigación			
RESPONSABLES DE LA REUNION: Gavidia Mamani Samuel - Torres Torres Luis Daniel			

CONVOCADOS / ASISTENTES

NOMBRES Y APELLIDOS	CARGO – DEPENDENCIA	ASISTIO	
		SI	NO
Ing. Carlos Saavedra	*Jefe TI - UPN*	X	
Gavidia Mamani Samuel	*Investigador*	X	
Torres Torres Luis Daniel	*Investigador*	X	

AGENDA

5. **Establecimiento del objetivo de investigación**
6. **Acuerdo para la Próxima reunión**

DESARROLLO DE LA AGENDA

5. **Establecimiento del objetivo de investigación:**

Se tuvo una reunión con el jefe de TI, en donde se planteó en nuestra propuesta de investigación . Esto fue presentado a su vez en un documento.

6. **Acuerdo para la Próxima reunión:**

Entrega del Organigrama del Área de TI, su POA, Topología de Red y visitas a sus instalaciones

Firma *Jefe TI – UPN*

Versión: 01

Pág. 3 de 8

Anexo 4: Documento de propuesta de Investigación (Actualizado)

Ñaña, Villa Unión, 24 de julio de 2017

Señores
Administración
UNIÓN PERUANA DEL NORTE
Lima - Chaclacayo
Presente.-

Apreciados señores de la Administración:

Reciba un caluroso saludo y mis deseos de éxitos en las responsabilidades que desempeña, anhelando que Dios siempre lo bendiga.

Tengo a bien presentarles a los bachilleres **SAMUEL GAVIDIA MAMANI y DANIEL TORRES TORRES**, egresados de la E.P Ingeniería de Sistemas de la Facultad de Ingeniería y Arquitectura de la Universidad Peruana Unión, quienes están desarrollando la tesis titulada "**Implementación de los controles de la ISO 27002 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Universidad Peruana Unión**" con el objetivo de optar el título profesional de Ingeniería de Sistemas.

Por lo expuesto, solicito a su despacho la autorización y acceso para la realización del proyecto de la tesis mencionada.

Desde ya agradezco su gentil atención a la presente y el apoyo que brinda en forma generosa a nuestros estudiantes.

Cordialmente,

UNIVERSIDAD PERUANA UNION
EAP DE INGENIERÍA DE SISTEMAS
DIRECTOR

Dra. Erika Inés Acuña Salinas
DIRECTORA E.P INGENIERÍA DE SISTEMAS
FACULTAD DE INGENIERÍA Y ARQUITECTURA

Anexo 5: Listas de chequeos (Checklist)

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad		Código de checklist	2017DS01
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo	System Auditors	
Área a Auditar	Área de tecnologías de información (TI)	Auditor	Luis Torres Torres	
Práctica de Gestión del Proceso	DSS05.01 Proteger Contra Software Malicioso			

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	El usuario final está capacitado sobre qué es un software malicioso.			
2	Existe un procedimiento de prevención frente al ataque de un software malicioso.			
3	Existe una herramienta de protección actualizada para el usuario final y también para la seguridad perimetral.			
4	Se programa la actualización del software antivirus según las políticas del área.			
5	Se realiza evaluaciones para detectar vulnerabilidades antes de que sean una amenaza.			
6	Existe un registro de amenaza identificadas en las evaluaciones.			
7	Existe alguna aplicación instalada que analice y evalúe el contenido del tráfico entrante para prevenir software malicioso.			
8	Existe política de permisos para instalar cualquier software			

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad		Código de checklist	2017DS02
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo	System Auditors	
Área a Auditar	Área de tecnologías de información (TI)	Auditor	Luis Torres Torres	
Práctica de Gestión del Proceso	DSS05.02 Gestionar la seguridad de la red y las conexiones			

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	Existe una política de seguridad para la red y conexiones.			
2	Solo los dispositivos autorizados tienen acceso a la información y a la red de la empresa.			
3	Existen políticas y herramientas que controlen el tráfico entrante y saliente de la red.			
4	La información de la empresa está clasificada según su criticidad e importancia.			
5	La información está cifrada para su tránsito en la red según su clasificación.			
6	Tienen conexiones certificadas de red.			
7	Los equipos de red son configurados siguiendo la política de seguridad definida.			
8	Se realiza pruebas de intrusión para ver el nivel de seguridad que se encuentra la red.			

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad		Código de checklist	2017DS03
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo	System Auditors	
Área a Auditar	Área de tecnologías de información (TI)	Auditor	Luis Torres Torres	
Práctica de Gestión del Proceso	DSS05.03 Gestionar la seguridad de los puestos de usuario final			

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	El sistema operativo de todas las computadoras (portátiles, de escritorio y servidores), cuenta con la última actualización publicada.			
2	Se tiene mecanismos de bloqueo que permita el libre acceso a la información y red de la empresa.			
3	Se cifra la información almacenada de la organización según su clasificación.			
4	Se controla los accesos al dispositivo de usuario final.			
5	Se configura la red a través de un servidor DHCP.			
6	Se implementa el filtrado de tráfico de red en dispositivos de usuario final.			
7	La integridad de la información es protegida en los puestos de usuario final.			
8	Se cuenta con equipos de protección física a los dispositivos de usuario final (Ups, estabilizadores).			
9	Cuando se deteriora un dispositivo se elimina físicamente y lógicamente de todo el contenido de la información que se encuentra dentro.			

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad		Código de checklist	2017DS04
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo	System Auditors	
Área a Auditar	Área de tecnologías de información (TI)	Auditor	Luis Torres Torres	
Práctica de Gestión del Proceso	DSS05.04 Gestionar la identidad del usuario y el acceso lógico			

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	Se mantiene los derechos de acceso de los usuarios de acuerdo al proceso de negocio.			
2	Se alinea la gestión de identidades y derecho de acceso a los roles y responsabilidades definidos.			
3	Se identifica los activos de la información por roles funcionales			
4	Mediante una clasificación de seguridad se realiza la autenticación en el acceso del usuario final a los activos de información.			
5	Las unidades de negocio gestionan la autenticación con aplicaciones para ver si los accesos a los activos de información fueron bien administrados.			
6	Los cambios efectuados en los perfiles de usuario se registran y monitorea solo con la aprobación del responsable del área.			
7	Separan cuentas de usuarios privilegiadas.			
8	Se revisa periódicamente los privilegios asignados a las cuentas del usuario.			
9	Se identifica unívocamente todas las actividades de proceso realizadas por el usuario.			
10	Se mantiene un registro del acceso lógico a la información altamente sencilla.			

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad		Código de checklist	2017DS05
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo	System Auditors	
Área a Auditar	Área de tecnologías de información (TI)	Auditor	Samuel Gavidia	
Práctica de Gestión del Proceso	DSS05.05 Gestionar el acceso físico a los activos de TI			

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	Se gestiona las peticiones de acceso a las instalaciones de procesamiento.			
2	Se gestiona las concesiones de acceso a áreas de instalación y procesamiento.			
3	Son completadas las peticiones formales de acceso			
4	Las peticiones formales de acceso son autorizados por la dirección de TI.			
5	Los perfiles de acceso físico al área de TI están definidas y actualizadas. (Basándose en las funciones y responsabilidades del usuario).			
6	Se registra y supervisa el acceso a las ubicaciones de TI. (Visitantes, proveedores, personal, etc.).			
7	El personal del área de TI mantiene visible la identificación en todo momento (fotocheck, placa o tarjeta).			
8	Se escolta a los visitantes en todo momento mientras estén en la ubicación.			
9	Se alerta al personal de seguridad si se encuentra a un individuo que va sin la compañía de alguien que pertenezca a la organización.			
10	Se alerta al personal de seguridad si se encuentra a un individuo que no lleva visible algo que lo identifique como visitante o empleado.			
11	Se establecen restricciones en el perímetro tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores para restringir el acceso a ubicaciones de TI sensibles.			
12	Se tiene informado al personal sobre la importancia de la seguridad física.			

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad		Código de checklist	2017DS06
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo	System Auditors	
Área a Auditar	Área de tecnologías de información (TI)	Auditor	Samuel Gavidia	
Práctica de Gestión del Proceso	DSS05.06 Gestionar Documentos sensibles y dispositivos de salida			

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	Existen procedimientos para la recepción de documentos especiales.			
2	Existen procedimientos para el uso de documentos especiales.			
3	Existen procedimientos para la eliminación de documentos especiales.			
4	Se asigna privilegios de acceso a documentos sensibles de acuerdo a su importancia.			
5	Existe un inventario de documentos sensibles.			
6	Existe un inventario de dispositivos de salida.			
7	Se realiza un inventario de conciliaciones de documentos sensibles y dispositivos de salida.			
8	Existen controles de seguridad físicas para los formularios especiales.			
9	Existen controles de seguridad física para los dispositivos sensibles.			
10	Se tiene los mecanismos necesarios para eliminar cualquier dispositivo de memoria o papeles lleno de información.			

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad		Código de checklist	2017DS07
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo	System Auditors	
Área a Auditar	Área de tecnologías de información (TI)	Auditor	Samuel Gavidia	
Práctica de Gestión del Proceso	DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad			

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	Se registran los eventos relacionados con la seguridad, considerando el nivel de la información.			
2	Los registros de seguridad son guardados durante un periodo apropiado para ayudar en futuras investigaciones.			
3	La naturaleza y características de los incidentes potenciales relacionados con la seguridad están definidas.			
4	La naturaleza y característica de los incidentes potenciales relacionados con la seguridad están comunicadas con el personal.			
5	Se revisa regularmente los registros de eventos para la detección de incidentes potenciales.			
6	Existe un procedimiento que recopile la evidencia de los incidentes de seguridad.			
7	Los empleados conocen los resultados de la recopilación de la evidencia de un incidente de seguridad.			

Anexo 6: Constancia de Validación de la lista de chequeos por parte de los especialistas

Constancia de Validación

Quien suscribe, Erika Acuña Salinas, con documento de identidad N°40153362, de profesión en Ingeniería de Sistemas con Grado de doctora ejerciendo actualmente como Directora EAP Ingeniería de Sistemas en la Universidad Peruana Unión.

Por medio de la presente hago constar que he revisado con fines de validación el Instrumento (Lista de Chequeo) que está en base al proceso DSS05-Gestionar los Servicios de Seguridad del framework Cobit 5 para la realización de la auditoria que será realizada para el área de TI de la UPN.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	EXCELENTE	BUENO	REGULAR	DEFICIENTE
Presentación del Instrumento		X		
Calidad de redacción de los Ítems		X		
Relevancia del contenido		X		
Factibilidad de aplicación		X		
Pertinencia		X		

Fecha:

Firma

Constancia de Validación

Quien suscribe, Elías Cuellar Rodríguez, con documento de identidad N°40964219, de profesión en Ingeniería de Sistemas con Grado de licenciado ejerciendo actualmente como Director de digeti en la Universidad Peruana Unión.

Por medio de la presente hago constar que he revisado con fines de validación el Instrumento (Lista de Chequeo) que está en base al proceso DSS05-Gestionar los Servicios de Seguridad del framework Cobit 5 para la realización de la auditoria que será realizada para el área de TI de la UPN.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	EXCELENTE	BUENO	REGULAR	DEFICIENTE
Presentación del Instrumento		X		
Calidad de redacción de los Ítems		X		
Relevancia del contenido	X			
Factibilidad de aplicación	X			
Pertinencia		X		

Fecha:

Firma

Anexo 7: Resultado de la evaluación de las listas de chequeos

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad		Código de checklist	2017DS01
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo	System Auditors	
Área a Auditar	Área de tecnologías de información (TI)	Auditor	Luis Torres Torres	
Práctica de Gestión del Proceso	DSS05.01 Proteger Contra Software Malicioso			

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	El usuario final está capacitado sobre qué es un software malicioso.	x		Lo hace pero no tiene documentación
2	Existe un procedimiento de prevención frente al ataque de un software malicioso.		x	No tiene
3	Existe una herramienta de protección actualizada para el usuario final y también para la seguridad perimetral.	x		Lo hace pero no tiene documentación
4	Se programa la actualización del software antivirus según las políticas del área.	x		Lo hace pero no tiene documentación formal
5	Se realiza evaluaciones para detectar vulnerabilidades antes de que sean una amenaza.		x	No lo realizan
6	Existe un registro de amenaza identificadas en las evaluaciones.		x	No lo realizan
7	Existe alguna aplicación instalada que analice y evalúe el contenido del tráfico entrante para prevenir software malicioso.	x		Firewall, si tiene un formato interno
8	Existe política de permisos para instalar cualquier software	x		Formato interno, falta política por perfil de usuario

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad		Código de checklist	2017DS02
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo	System Auditors	
Área a Auditar	Área de tecnologías de información (TI)	Auditor	Luis Torres Torres	
Práctica de Gestión del Proceso	DSS05.02 Gestionar la seguridad de la red y las conexiones			

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	Existe una política de seguridad para la red y conexiones.	x		Poseen un formato interno
2	Solo los dispositivos autorizados tienen acceso a la información y a la red de la empresa.	x		Solo el área en forma interna, mas no cuentan con documentación
3	Existen políticas y herramientas que controlen el tráfico entrante y saliente de la red.	x		Si Poseen, pero no cuentan con documentación
4	La información de la empresa está clasificada según su criticidad e importancia.		x	No se especifica ni hay un respaldo
5	La información está cifrada para su tránsito en la red según su clasificación.		x	La información no se encuentra cifrada
6	Tienen conexiones certificadas de red.	x		Si se encuentran certificadas
7	Los equipos de red son configurados siguiendo la política de seguridad definida.	x		No está en base a una iso, sino en una política interna como iglesia
8	Se realiza pruebas de intrusión para ver el nivel de seguridad que se encuentra la red.		x	No lo realizan

ASOCIACIÓN IGLESIA ADVENTISTA DEL SÉPTIMO DÍA PERUANA DEL NORTE – TECNOLOGÍA DE INFORMACIÓN

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad			Código de checklist	2017DS03
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo		System Auditors	
Área a Auditar	Área de tecnologías de información (TI)		Auditor	Luis Torres Torres	
Práctica de Gestión del Proceso	DSS05.03 Gestionar la seguridad de los puestos de usuario final				

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	El sistema operativo de todas las computadoras (portátiles, de escritorio y servidores), cuenta con la última actualización publicada.		x	No cuentan con la última actualización todos los dispositivos que hay en el área de TI
2	Se tiene mecanismos de bloqueo que permita el libre acceso a la información y red de la empresa.	x		Lo realizan en forma virtual internamente
3	Se cifra la información almacenada de la organización según su clasificación.		x	No está cifrada en su totalidad
4	Se controla los accesos al dispositivo de usuario final.	x		Lo realizan mediante dominios
5	Se configura la red a través de un servidor DHCP.	x		Si lo realizan y se encuentra documentada
6	Se implementa el filtrado de tráfico de red en dispositivos de usuario final.		x	No lo realizan
7	La integridad de la información es protegida en los puestos de usuario final.		x	Les falta implementar
8	Se cuenta con equipos de protección física a los dispositivos de usuario final (Ups, estabilizadores).	x		Si lo conllevan y se encuentra documentada
9	Cuando se deteriora un dispositivo se elimina físicamente y lógicamente de todo el contenido de la información que se encuentra dentro.	x		Lo realizan pero como área, mas no cuentan con documentación

ASOCIACIÓN IGLESIA ADVENTISTA DEL SÉPTIMO ... TECNOLOGÍA DE INFORMACIÓN

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad			Código de checklist	2017DS04
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo		System Auditors	
Área a Auditar	Área de tecnologías de información (TI)		Auditor	Luis Torres Torres	
Práctica de Gestión del Proceso	DSS05.04 Gestionar la identidad del usuario y el acceso lógico				

ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	Se mantiene los derechos de acceso de los usuarios de acuerdo al proceso de negocio.		x	Les falta definir políticas que mantengan los derechos de acceso a los usuarios de acuerdo al proceso de negocio
2	Se alinea la gestión de identidades y derecho de acceso a los roles y responsabilidades definidos.	x		Si lo realizan, pero les falta hacer un registro de ello
3	Se identifica los activos de la información por roles funcionales	x		Si lo realizan, además de poseer un formato interno
4	Mediante una clasificación de seguridad se realiza la autenticación en el acceso del usuario final a los activos de información.	x		Si lo realizan, pero no tienen documentación
5	Las unidades de negocio gestionan la autenticación con aplicaciones para ver si los accesos a los activos de información fueron bien administrados.		x	No lo realizan
6	Los cambios efectuados en los perfiles de usuario se registran y monitorea solo con la aprobación del responsable del área.		x	No lo realizan
7	Separan cuentas de usuarios privilegiadas.	x		Lo realizan, pero no tienen documentación
8	Se revisa periódicamente los privilegios asignados a las cuentas del usuario.		x	No realizan ninguna revisión de los privilegios asignados las cuentas de usuario
9	Se identifica unívocamente todas las actividades de proceso realizadas por el usuario.		x	No lo identifican
10	Se mantiene un registro del acceso lógico a la información altamente sencilla.		x	No lo realizan

ASOCIACIÓN IGLESIA ADVENTISTA DEL SÉPTIMO ... TECNOLOGÍA DE INFORMACIÓN

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad		Código de checklist	2017DS05
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo		System Auditors
Área a Auditar	Área de tecnologías de información (TI)	Auditor		Samuel Gavidia
Práctica de Gestión del Proceso	DSS05.05 Gestionar el acceso físico a los activos de TI			

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	Se gestiona las peticiones de acceso a las instalaciones de procesamiento.	x		Se gestionan las peticiones de acceso, pero no cuentan con un formato para su gestión
2	Se gestiona las concesiones de acceso a áreas de instalación y procesamiento.		x	No lo realizan
3	Son completadas las peticiones formales de acceso		x	Les falta implementar
4	Las peticiones formales de acceso son autorizados por la dirección de TI.	x		si son autorizados, pero no son registradas en ningún documento
5	Los perfiles de acceso físico al área de TI están definidas y actualizadas. (Basándose en las funciones y responsabilidades del usuario).	x		Si lo realizan, pero les falta hacer un registro de ello
6	Se registra y supervisa el acceso a las ubicaciones de TI. (Visitantes, proveedores, personal, etc.).		x	No registran ni supervisan el acceso a las ubicaciones de TI
7	El personal del área de TI mantiene visible la identificación en todo momento (fotocheck, placa o tarjeta).		x	No poseen algo que los identifique
8	Se escolta a los visitantes en todo momento mientras estén en la ubicación.	x		Si escoltan a los visitantes, pero no realizan un registro de ello
9	Se alerta al personal de seguridad si se encuentra a un individuo que va sin la compañía de alguien que pertenezca a la organización.	x		Si se alerta al personal de seguridad, pero no hay un registro de ello
10	Se alerta al personal de seguridad si se encuentra a un individuo que no lleva visible algo que lo identifique como visitante o empleado.	x		Lo realizan, pero no hay un registro formal
11	Se establecen restricciones en el perímetro tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores para restringir el acceso a ubicaciones de TI sensibles.		x	No lo realizan
12	Se tiene informado al personal sobre la importancia de la seguridad física.	x		Lo realizan, pero no cuentan con un registro de ello

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad		Código de checklist	2017DS06
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo		System Auditors
Área a Auditar	Área de tecnologías de información (TI)	Auditor		Samuel Gavidia
Práctica de Gestión del Proceso	DSS05.06 Gestionar Documentos sensibles y dispositivos de salida			

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	Existen procedimientos para la recepción de documentos especiales.		x	No existe ninguna recepción de documentos
2	Existen procedimientos para el uso de documentos especiales.		x	No conllevan ningún procedimiento para el uso de documentos especiales
3	Existen procedimientos para la eliminación de documentos especiales.	x		Si existe tales procedimientos, pero les falta hacer un registro de ello
4	Se asigna privilegios de acceso a documentos sensibles de acuerdo a su importancia.		x	Si lo realizan, pero les falta hacer un registro de ello
5	Existe un inventario de documentos sensibles.	x		No lo realizan ni hay un sustentación de ello
6	Existe un inventario de dispositivos de salida.		x	No realizan ningún inventariado de dispositivos de salida
7	Se realiza un inventario de conciliaciones de documentos sensibles y dispositivos de salida.		x	No lo realizan en su totalidad
8	Existen controles de seguridad físicas para los formularios especiales.		x	No existe ningún control de seguridad física para los dispositivos especiales
9	Existen controles de seguridad física para los dispositivos sensibles.		x	No existe ningún control de seguridad física para los dispositivos sensibles
10	Se tiene los mecanismos necesarios para eliminar cualquier dispositivo de memoria o papeles lleno de información.	x		No existe un registro de ello, pero si hay un mecanismo para la eliminación de ellos
11	Se tiene un modelo de arquitectura de la información.		x	No poseen ningún modelo para la arquitectura de la información

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad			Código de checklist	2017DS07
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo		System Auditors	
Área a Auditar	Área de tecnologías de información (TI)	Auditor		Samuel Gavidia	
Práctica de Gestión del Proceso	DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad				

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	Se registran los eventos relacionados con la seguridad, considerando el nivel de la información.		x	No hay ningún registro de ello
2	Los registros de seguridad son guardados durante un periodo apropiado para ayudar en futuras investigaciones.		x	No existe ningún registro de ello
3	La naturaleza y características de los incidentes potenciales relacionados con la seguridad están definidas.		x	No hay ningún registro ni respaldo que defina los incidentes potenciales relacionados con la seguridad
4	La naturaleza y característica de los incidentes potenciales relacionados con la seguridad están comunicadas con el personal.	x		Si se tiene evidencias y están registradas
5	Se revisa regularmente los registros de eventos para la detección de incidentes potenciales.	x		Si lo realizan
6	Existe un procedimiento que recopile la evidencia de los incidentes de seguridad.		X	No conllevan ningún procedimiento
7	Los empleados conocen los resultados de la recopilación de la evidencia de un incidente de seguridad.		x	Los empleados no conocen los resultados de la recopilación de las evidencias de un incidente de seguridad que pueda ocurrir

Anexo 8: Informe de Auditoria

INFORME DE AUDITORÍA			
Proceso COBIT	DSS05 - Gestionar servicios de seguridad	**Fecha Auditada**	25/07/17
Área Auditada	Área de tecnología de información (TI) de la Unión Peruana del Norte	**Fecha de entrega de informe**	03/08/17

I. Datos generales de la auditoría:

- **Alcance:**

El alcance de la auditoría fue el Área de TI de la Unión Peruana del Norte. La revisión realizada abarcó los servicios de seguridad según lo especifican las prácticas de gestión del proceso DSS05 - Gestionar los servicios de seguridad del COBIT 5.

- **Criterio de Auditoría:**
  - **COBIT 5**
  - **Proceso DSS05 –** Gestionar los Servicios de Seguridad
  - **Prácticas del Proceso:** Actividades del proceso para su evaluación.
    - DSS05.01 – Proteger contra software malicioso.
    - DSS05.02 – Gestionar la seguridad de la red y las conexiones.
    - DSS05.03 – Gestionar la seguridad de los puestos de usuario final.
    - DSS05.04 – Gestionar la identidad del usuario y el acceso lógico.
    - DSS05.05 – Gestionar el accesos físico a los activos de TI.
    - DSS05.06 – Gestionar documentos sensibles y dispositivos de salida.
    - DSS05.07 – Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

- **Objetivo de la Auditoría**

  Verificar si los servicios de seguridad implementados en el área de TI de la Unión Peruana del Norte cumplen con lo especificado en las prácticas de gestión del proceso DSS05 - Gestionar servicios de seguridad del COBIT 5.

- **Dependencia Auditada**
  - Área de TI de la Unión Peruana del Norte

- **Equipo Auditor**
  - Luis Daniel Torres Torres
  - Samuel Gavidia Mamani

II. Modelo de Evaluación de Procesos (PAM)

El Modelo de Evaluación de Procesos (PAM) de COBIT está diseñado para proveer a las empresas con una metodología reproducible, confiable y robusta para evaluar la capacidad de sus procesos de TI. Dichas evaluaciones normalmente se usan como parte de un programa de mejora de los procesos de una empresa y también se pueden utilizar para informar internamente a la dirección ejecutiva o la junta directiva de una empresa sobre la capacidad actual de sus procesos de TI.

El PAM tiene 6 niveles para evaluar la capacidad de los procesos de COBIT, tal como se muestra en la Figura 1. En la auditoría realizada evaluamos la capacidad del proceso DSS05 - Gestionar los servicios de seguridad en el Nivel 1 - Proceso realizado.

ID del Atributo de Proceso	Niveles de Capacidad y Atributos de Proceso
	Nivel 0: Proceso incompleto
	Nivel 1: Proceso realizado
PA 1.1	Rendimiento del proceso
	Nivel 2: Proceso gestionado
PA 2.1	Gestion del rendimiento
PA 2.2	Gestión de productos del trabajo
	Nivel 3: Proceso consolidado
PA 3.1	Definición de proceso
PA 3.2	Despliegue del proceso
	Nivel 4: Proceso predecible
PA 4.1	Medición del proceso
PA 4.2	Control del proceso
	Nivel 5: Proceso optimizado
PA 5.1	Innovación del proceso
PA 5.2	Optimización del proceso

Figura 1 - Niveles de evaluación del PAM

Los resultados obtenidos en la evaluación del proceso se ubican en la Escala de Evaluación del PAM para determinar cuál es el porcentaje de logro alcanzado en el nivel que se evaluó. La Figura 2 muestra esta escala de evaluación.

Abreviación	Descripción	% Logro
N	No alcanzado	0 a 15% de logro
P	Parcialmente alcanzado	>15% a 50% de logro
L	Ampliamente alcanzado	>50% a 85% de logro
F	Completamente alcanzado	>85% a 100% de logro

Figura 2 - Escala de evaluación del PAM

Para cada proceso de COBIT 5, el PAM define Criterios de Evaluación que se relacionan con las Prácticas de Gestión del proceso evaluado. Para el proceso DSS05 Gestionar los Servicios de Seguridad, el PAM especifica los criterios de evaluación y su relación con las prácticas de gestión que se muestran en la Figura 3.

	Criterios de evaluación del modelo PAM				
Prácticas del Proceso DSS05- Gestionar los Servicios de Seguridad	**Criterio 1:** DSS05-O1 Las redes y la seguridad de las comunicaciones responden a las necesidades del negocio.	**Criterio 2:** DSS05-O2 La información procesada, almacenada y transmitida por dispositivos de punto final está protegida.	**Criterio 3:** DSS05-O3 Todos los usuarios son identificables de forma única y tienen derechos de acceso de acuerdo con su función comercial.	**Criterio 4:** DSS05-O4 Se han implementado medidas físicas para proteger la información del acceso, daño e interferencia no autorizados al ser procesados, almacenados o transmitidos.	**Criterio 5:** DSS05-O5 La información electrónica está debidamente protegida cuando se almacena, transmite o destruye.
DSS05.01 Proteger Contra Software Malicioso	X	X			
DSS05.02 Gestionar la seguridad de la red y las conexiones	X				
DSS05.03 Gestionar la seguridad de los puestos de usuario final		X			
DSS05.04 Gestionar la identidad del usuario y el acceso lógico			X		
DSS05.05 Gestionar el acceso físico a los activos de TI				X	
DSS05.06 Gestionar Documentos sensibles y dispositivos de salida					X
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad	X				

Figura 3 - Criterios de evaluación del PAM para el proceso DSS05 - Gestionar los servicios de seguridad

III. Resultados de la auditoría

A continuación se presentan los resultados obtenidos en la evaluación inicial:

CRITERIOS DE EVALUACIÓN	ESCALA DE EVALUACIÓN			
	No Logrado (0-15%)	Parcialmente logrado (15% -50%)	En gran medida logrado (50% - 85%)	Totalmente logrado (85% - 100%)
C1) DSS05-O1 Las redes y la seguridad de las comunicaciones responden a las necesidades del negocio.			51%	
C2) DSS05-O2 La información procesada, almacenada y transmitida por dispositivos de punto final está protegida.			59%	
C3) DSS05-O3 Todos los usuarios son identificables de forma única y tienen derechos de acceso de acuerdo con su función comercial.		40%		
C4) DSS05-O4 Se han implementado medidas físicas para proteger la información del acceso, daño e interferencia no autorizados al ser procesados, almacenados o transmitidos.			58%	
C5) DSS05-O5 La información electrónica está debidamente protegida cuando se almacena, transmite o destruye.		27%		

Resultado de la evaluación del proceso	47% - Parcialmente logrado

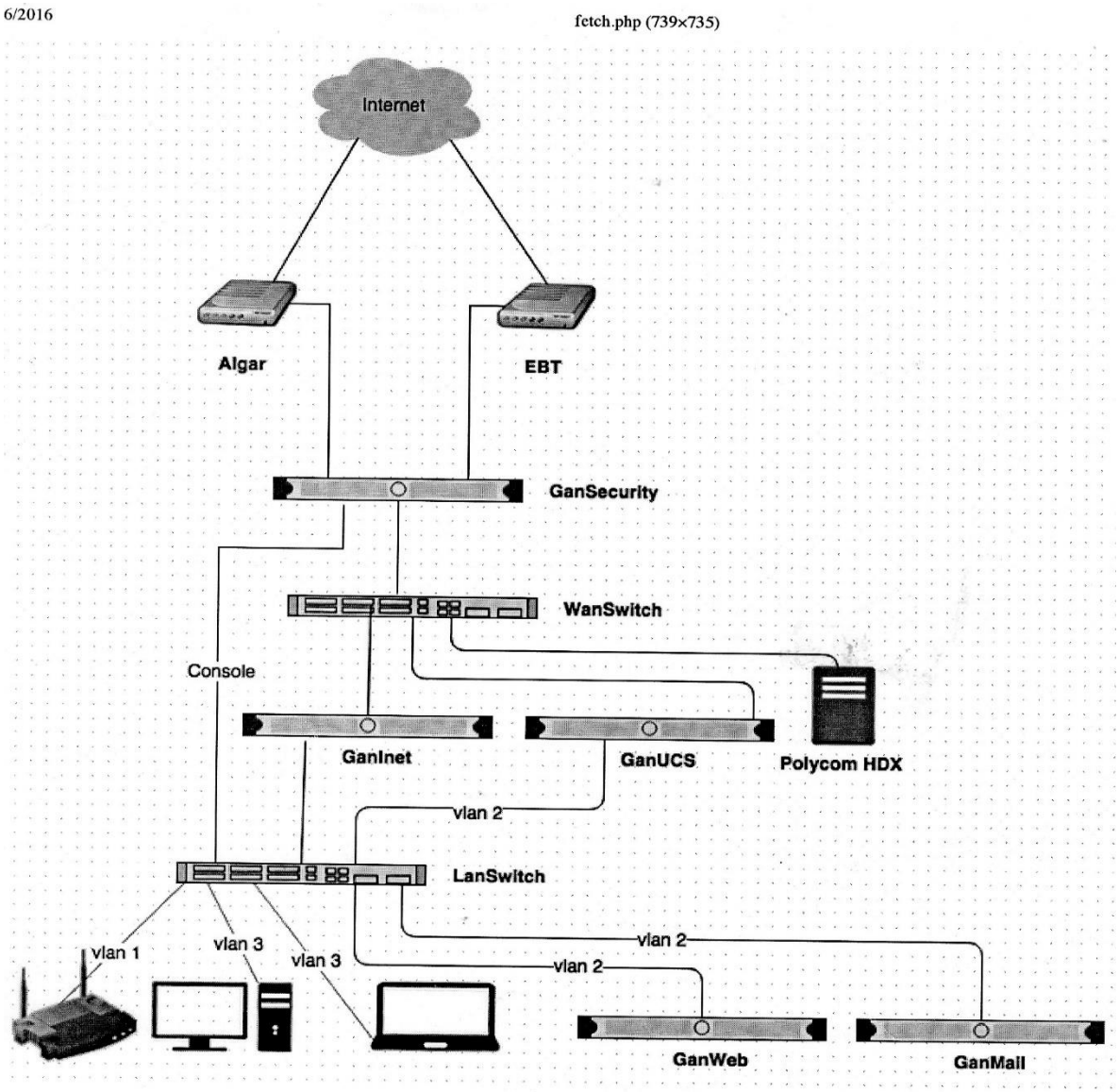
De acuerdo a la Escala de Calificación del PAM, la Gestión de los Servicios de Seguridad en el Área de TI de la Unión Peruana del Norte alcanza el 47% lo que significa que el proceso se encuentra parcialmente logrado.

Samuel Gavidia Mamani
46763932

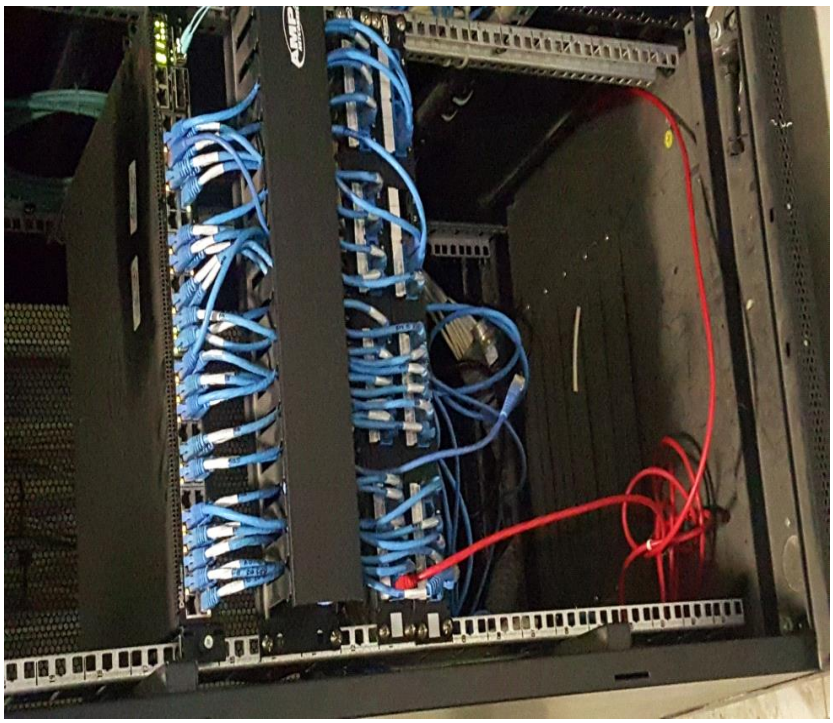
Luis Daniel Torres Torres
72368970

UPN CARLOS SAAVEDRA VASCONEZ
GERENTE T.I
DNI: 40981832

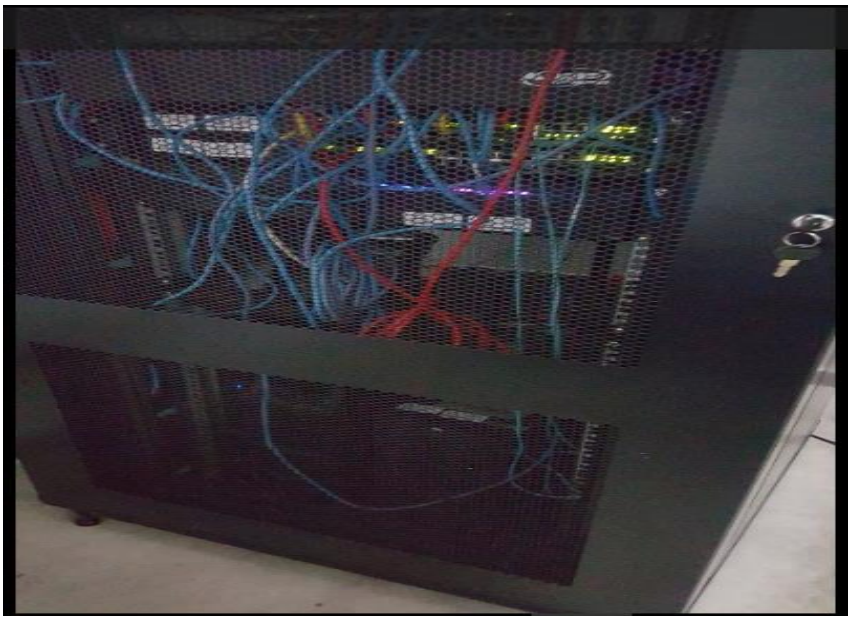
Anexo 9: Topología de Red de la Organización



Anexo 10: Estructura de cables



Anexo 11: Servidor principal



Anexo 12: Lista de Activos generales del área de TI

Aspecto del análisis		Identificacion de Activos				Código de análisis			2017AVA01
Empresa de estudio		Unión Peruana del Norte				Empresa a cargo			System Auditors
Área de estudio		Área de tecnologías de información (TI)				Encargado			amuel Gavidia Mama
ID	Activo	Descripcion del activo	Propietario	Ubicación	Tipo de Activo	Tasación o Valoracion			
						D	I	C	Valor
ACT-01	Estabilizador - UPS	UPS TRIPP SmathOnLine servidores	Arq. Karen Cruzado	sótano(Cuarto de UPS)	A.Físicos	3	2	2	2
ACT-02	Grupo Electrógeno	Transformador de aislamiento de 12 KVA flash power	Arq. Karen Cruzado	sótano(Cuarto de UPS)	A.Físicos	3	2	2	2
ACT-03	Contratos	Documento de compromiso del personal de trabajo	Omar Campos/ Martin Saldaña	Área de Talento Humano y Legales (3er Piso)	A. Documentos de Papel	4	2	2	3
ACT-04	Licencias	Software Microsoft	Carlos Saavedra	Área de Ti (3er Piso)	A. Software	4	3	3	3
ACT-05	Licencias	Antivirus Gdata versión 2017	Carlos Saavedra	Área de Ti (3er Piso)	A. Software	4	4	4	4
ACT-06	Licencias	Adobe Creative Cloud versión 2017	Carlos Saavedra	Área de Ti (3er Piso)	A. Software	4	3	3	3
ACT-07	Sistema DSA	Software que le asigna la iglesia al área de TI	Carlos Saavedra	Área de Ti (3er Piso)	A. Software	4	4	4	4
ACT-08	Sistema UPN - Académico	Sistema que se brinda a colegios de la iglesia	Janeth Tenorio	Área de Ti (3er Piso)	A. Software	4	4	4	4
ACT-09	Sistema UPN - Gerencial	Sistema que se brinda a misiones y gerencia de la iglesia	Amelio Apaza	Área de Ti (3er Piso)	A. Software	4	4	4	4
ACT-10	Videoconferencia	Charlas o capacitaciones que se obtiene del exterior o local.	Fernando Lazo	Sala de Reuniones(2er Piso)	A. Servicio	3	2	2	2
ACT-11	Helpdesk	Soporte y Mantenimiento	Fernando Lazo	Área de Ti - mesa de soporte (3er Piso)	A. Servicio	4	2	2	3
ACT-12	Back-Ups	Copia de respaldo de base de datos	Carlos Saavedra	Área de TI (3er Piso)	A. Software	5	5	5	5
ACT-13	Back-Ups	Copia de respaldo de software	Janeth Tenorio / Amelio Apaza	Área de TI (3er Piso)	A. Software	5	5	5	5
ACT-14	Red y conectividad	Conexiones certificadas para la instalación	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	5	5	5	5
ACT-16	Jefe de TI	Brinda seguridad al área de TI e infraestructura	Carlos Saavedra	Área de TI (3er Piso)	A. Personal	5	4	4	4
ACT-17	Analista de Sistemas	Realiza el análisis y desarrollo de los sistemas académicos	Janeth Tenorio	Área de TI (3er Piso)	A. Personal	5	4	4	4
ACT-18	Analista de Sistemas	Realiza el análisis y desarrollo de los sistemas gerenciales	Amelio Apaza	Área de TI (3er Piso)	A. Personal	5	4	4	4
ACT-19	Disco Duro - HD	Disco duro externo wster digital	Carlos Saavedra	Sala de Computo	A. Físicos	4	4	4	4
ACT-20	Servidor	Servidor Packcable HP Proliant DL 160 GB Intel	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	4	4	4
ACT-21	Micrófono Inalámbrico	Micrófono shure GGX 24 E	Carlos Saavedra	Sala de Computo	A. Físicos	2	1	1	1
ACT-22	Servidor	Servidor HP Proliant DL 120GB 6 Intel XEON 343	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	4	4	4
ACT-23	Amplificador	Ecualizador 2bx 1215 0101590 con cables	Carlos Saavedra	Sala de Computo	A. Físicos	3	2	2	2
ACT-24	Amplificador	Compreso SBX 166 cables	Carlos Saavedra	Sala de Computo	A. Físicos	3	2	2	2
ACT-25	Adaptador	Adaptador de video Kramer 4x1 vga mechanical Sh	Carlos Saavedra	Sala de Computo	A. Físicos	3	2	2	2
ACT-26	IPAD	IPAD MAT Apple	Carlos Saavedra	Sala de Computo	A. Físicos	3	2	2	2
ACT-27	Equipo de control de asistencia	Equipo de control de asistencia	Carlos Saavedra	Sala de Computo	A. Físicos	4	3	3	3
ACT-28	Impresora	Impresora Epson Matricial LX300+II	Carlos Saavedra	Sala de Computo	A. Físicos	3	2	2	2
ACT-29	Impresora	Impresora Epson TMU - 220A ticketera	Carlos Saavedra	Sala de Computo	A. Físicos	3	2	2	2
ACT-30	Monitor	Monitor Led Samsung 20" VGA S20A300N interfaz	Carlos Saavedra	Sala de Computo	A. Físicos	3	2	2	2
ACT-31	Monitor	Monitor Led Samsung 20" vga	Carlos Saavedra	Sala de Computo	A. Físicos	3	2	2	2
ACT-32	Aire acondicionado	Aire acondicionado Split	Carlos Saavedra	Sala de Computo	A. Físicos	3	1	1	2
ACT-33	CPU - Servidor	Servidor central telefónica	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	4	4	4
ACT-34	CPU - Servidor	Servidor correo power edge R720	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	5	5	5
ACT-35	Switch	Power connect 6224P puertos GbE conmutador Admin	Carlos Saavedra	Sala de Computo	A. Físicos	4	3	3	3
ACT-36	Switch	Switch dlink DES 1210 19" para telefonía	Carlos Saavedra	Sala de Computo	A. Físicos	4	3	3	3
ACT-37	Accesorio Informática	Kit transmisión simple y 2 consolas 8 canales	Carlos Saavedra	Sala de Computo	A. Físicos	4	3	3	3

ACT-38	Lector de Código de Barras	Lector código de barras Heron D130 black USB Ki	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	3	2	2	2
ACT-39	Laptop	Laptop Dell Tes. Asistente oper.	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	5	4	4	4
ACT-40	proyector	Proyector Epson power Lite 4200	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	3	1	1	2
ACT-41	Notebook	Notebook DELL serie 3000 14" i5	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	5	4	4	4
ACT-42	Silla operativa	Global UPHOLSTERY-MOD. MESH TEA negro	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	2	1	1	1
ACT-43	mueble	Closet con puertas grande con 4 divisiones	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	2	1	1	1
ACT-44	Software	software control de asistencia premium	Carlos Saavedra	Área de TI (3er Piso)	A. Software	4	2	3	3
ACT-45	Escritorio	Escritorio con cajonera en T modular dos personas	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	2	1	1	1
ACT-46	Impresora	Ticketera impresora inmovilizado	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	3	1	1	2
ACT-47	Laptop	Mac book	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	5	4	4	4
ACT-48	Monitor	Monitor DELL P2317H - HBGBPB2	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	3	2	2	2
ACT-49	Monitor	Monitor DELL P2317H - 5BGBPB2	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	3	2	2	2
ACT-50	Monitor	Monitor DELL P2317H - DBGBPB2	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	3	2	2	2
ACT-51	Monitor	Monitor DELL P2317H - 9BGBPB2	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	3	2	2	2
ACT-52	Monitor	Monitor DELL P2317H - 8BGBPB2	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	3	2	2	2
ACT-53	Laptop	Latitude 5470 - i5 8 GB 1 TB HD - 126 VZF2	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	5	4	4	4
ACT-54	Laptop	Latitude E5470 - I7 16 GB 1 TB FHD	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	5	4	4	4
ACT-55	Laptop	Latitude E5470 - I7 16 GB 1 TB FHD	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	5	4	4	4
ACT-56	Switch	Switch Dell networking N1524P	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	4	3	3	3
ACT-57	Servidor de Base de datos	Servidor Dell Poweredge R630	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	5	5	5
ACT-58	Servidor de archivos	Servidor Dell Poweredge R630	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	5	5	5
ACT-59	Servidor Firewall	Servidor Dell Poweredge R230	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	5	5	5
ACT-60	Servidor DHCP	Servidor Dell Poweredge R230	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	4	4	4
ACT-61	Servidor Web	Servidor Dell Poweredge R230	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	4	4	4
ACT-62	CPU - Centro de datos	Server HP Proliant DL 4 Core 2.4 GZ free BSD	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	5	5	5
ACT-63	Servidor Redundante	Servidor Dell poweredge Intel xeon	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	4	4	4
ACT-64	Switch General Corp	Switch Dell networking N3048P	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	5	5	5
ACT-65	silla de visita	BR-1061VC01 Modelo variety negro	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	2	1	1	1
ACT-66	cámara de video vigilancia	Cámaras de video/01 Switch vigilancia	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	4	4	4
ACT-67	servidor Redundante	Servidor DELL power Intel	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	4	4	4
ACT-68	Accesorio Informática	Switch Dell networking - N1524P	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	4	3	3	3
ACT-69	Accesorio Informática	Switch Dell networking - N1524P	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	4	3	3	3
ACT-70	Accesorio Informática	Switch Dell networking - N1524P	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	4	3	3	3
ACT-71	Switch	SWITCH D-Link web Smart	Carlos Saavedra	Sede - Switcher 3er piso	A. Físicos	4	3	3	3
ACT-72	Switch	SWITCH D-Link web Smart	Carlos Saavedra	Sede - Switcher 3er piso	A. Físicos	4	3	3	3
ACT-73	Manuales de Usuario	Documento que brinda asistencia técnica a los usuarios que usan los sistemas de información	Janeth Tenorio / Amelio Apaza	Área de Ti (3er Piso)	A. Información	4	3	3	3
ACT-74	Base de datos	Gestor de Base de datos SQL Server	Carlos Saavedra	Área de Ti (3er Piso)	A. Software	5	5	5	5

Anexo 13: Activos Priorizados

ACTIVOS PRIORIZADOS									
ID	Activo	Descripción del activo	Propietatario	Ubicación	Tipo de Activo	Tasacción o valoración			
						D	I	C	Valor
AP-1	Base de datos	Gestor de Base de datos SQL Server	Carlos Saavedra	Área de Ti (3er Piso)	A Software	5	5	5	5
AP-2	Back-Ups	Copia de respaldo de base de datos	Carlos Saavedra	Área de TI (3er Piso)	A. Software	5	5	5	5
AP-3	Back-Ups	Copia de respaldo de software	Janeth Tenorio / Amelio Apaza	Área de TI (3er Piso)	A. Software	5	5	5	5
AP-4	CPU - Servidor	Servidor correo power edge R720	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	5	5	5
AP-5	CPU - Centro de datos	Server HP Proliant DL 4 Core 2.4 GZ free BSD	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	5	5	5
AP-6	Red y conectividad	Conexiones certificadas para la instalación	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	5	5	5	5
AP-7	Servidor de Base de datos	Servidor Dell Poweredge R630	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	5	5	5
AP-8	Servidor de Archivos	Servidor Dell Poweredge R630	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	5	5	5
AP-9	Servidor Firewall	Servidor Dell Poweredge R230	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	5	5	5
AP-10	Switch General Corp	Switch Dell networking N3048P	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	5	5	5
AP-11	Jefe de TI	Brinda seguridad al área de TI e infraestructura	Carlos Saavedra	Área de TI (3er Piso)	A. Personal	5	4	4	4
AP-12	Analista de Sistemas	Realiza el análisis y desarrollo de los sistemas académicos	Janeth Tenorio	Área de TI (3er Piso)	A. Personal	5	4	4	4
AP-13	Analista de Sistemas	Realiza el análisis y desarrollo de los sistemas gerenciales	Amelio Apaza	Área de TI (3er Piso)	A. Personal	5	4	4	4
AP-14	Servidor	Servidor Packcable HP Proliant DL 160 GB Intel	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	4	4	4
AP-15	Servidor	Servidor HP Proliant DL 120GB 6 Intel XEON 343	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	4	4	4
AP-16	CPU - Servidor	Servidor central telefónica	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	4	4	4
AP-17	Laptop	Laptop Dell Tes. Asistente oper.	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	5	4	4	4
AP-18	Notebook	Notebook DELL serie 3000 14" i5	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	5	4	4	4
AP-19	Laptop	Mac book	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	5	4	4	4
AP-20	Laptop	Latitude 5470 - i5 8 GB 1 TB HD - 126 VZF2	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	5	4	4	4
AP-21	Laptop	Latitude E5470 - I7 16 GB 1 TB FHD	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	5	4	4	4
AP-22	Laptop	Latitude E5470 - I7 16 GB 1 TB FHD	Carlos Saavedra	Área de TI (3er Piso)	A. Físicos	5	4	4	4
AP-23	Servidor DHCP	Servidor Dell Poweredge R230	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	4	4	4
AP-24	Servidor Web	Servidor Dell Poweredge R230	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	4	4	4

AP-25	Servidor Redundante	Servidor Dell poweredge Intel xeon	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	4	4	4
AP-26	Cámara de Video Vigilancia	Cámaras de video/01 Switch vigilancia	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	4	4	4
AP-27	Servidor Redundante	Servidor DELL power Intel	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	5	4	4	4
AP-28	Licencias	Antivirus Gdata versión 2017	Carlos Saavedra	Área de Ti (3er Piso)	A. Software	4	4	4	4
AP-29	Sistema DSA	Software que le asigna la iglesia al área de TI	Carlos Saavedra	Área de Ti (3er Piso)	A. Software	4	4	4	4
AP-30	Sistema UPN - Académico	Sistema que se brinda a colegios de la iglesia	Janeth Tenorio	Área de Ti (3er Piso)	A. Software	4	4	4	4
AP-31	Sistema UPN - Gerencial	Sistema que se brinda a misiones y gerencia de la iglesia	Amelio Apaza	Área de Ti (3er Piso)	A. Software	4	4	4	4
AP-33	Disco Duro - HD	Disco duro externo wster digital	Carlos Saavedra	Sala de Computo	A. Físicos	4	4	4	4
AP-34	Equipo de control de asistencia	Equipo de control de asistencia	Carlos Saavedra	Sala de Computo	A. Físicos	4	3	3	3
AP-35	Switch	Power connect 6224P puertos GbE conmutador Admin	Carlos Saavedra	Sala de Computo	A. Físicos	4	3	3	3
AP-36	Switch	Switch dlink DES 1210 19" para telefonía	Carlos Saavedra	Sala de Computo	A. Físicos	4	3	3	3
AP-37	Switch	Switch Dell networking N1524P	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	4	3	3	3
AP-38	Accesorio Informática	Switch Dell networking - N1524P	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	4	3	3	3
AP-39	Accesorio Informática	Switch Dell networking - N1524P	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	4	3	3	3
AP-40	Accesorio Informática	Switch Dell networking - N1524P	Carlos Saavedra	Sede - Data Center Sótano	A. Físicos	4	3	3	3
AP-41	Switch	SWITCH D-Link web Smart	Carlos Saavedra	Sede - Switcher 3er piso	A. Físicos	4	3	3	3
AP-42	Switch	SWITCH D-Link web Smart	Carlos Saavedra	Sede - Switcher 3er piso	A. Físicos	4	3	3	3
AP-43	Manuales de Usuario	Documento que brinda asistencia técnica a los usuarios que usan los sistemas de información	Janeth Tenorio / Amelio Apaza	Área de Ti (3er Piso)	A. Informació	4	3	3	3
AP-44	Software	software control de asistencia premium	Carlos Saavedra	Área de TI (3er Piso)	A. Software	4	2	3	3
AP-45	Helpdesk	Soporte y Mantenimiento	Fernando Lazo	Área de Ti - mesa de soporte (3er Piso)	A. Servicio	4	2	2	3
AP-46	Contratos	Documento de compromiso del personal de trabajo	Omar Campos/ Martin Saldaña	Área de Talento Humano y Legales (3er Piso)	A. Documentos de Papel	4	2	2	3
AP-47	Estabilizador - UPS	UPS TRIPP SmathOnLine servidores	Arq. Karen Cruzad	sótano(Cuarto de UPS)	A. Físicos	4	2	2	3
AP-48	Grupo Electrógeno	Transformador de aislamiento de 12 KVA flash power	Arq. Karen Cruzad	sótano(Cuarto de UPS)	A. Físicos	4	2	2	3

Anexo 14: Lista de Amenazas identificadas

ID	Descripción de la amenaza	Tipo de Amenaza	Probabilidad de Ocurrencia
AME-1	Virus/ Malware	Amenaza Tecnológica	4
AME-2	Hacking	Amenaza Tecnológica	4
AME-3	Fallas de red	Amenaza Tecnológica	4
AME-4	Fallas de servidores	Amenaza Tecnológica	4
AME-5	Falla en la base de datos	Amenaza Tecnológica	4
AME-6	Falla en las aplicaciones	Amenaza Tecnológica	4
AME-7	Falla en telefonía	Amenaza Tecnológica	4
AME-8	Incumplimiento en el mantenimiento del sistema de información	Amenazas de software	4
AME-9	Copia fraudulenta del software	Amenazas de software	4
AME-10	Espionaje remoto	Amenazas Tecnológicas	4
AME-11	Perdida de datos	Amenazas deliberadas	4
AME-12	Desborde de Huaycos	Amenaza Natural	3
AME-13	Sismos	Amenaza Natural	3
AME-14	Explosión de conexiones	Amenaza a instalaciones	3
AME-15	Fallas internas de los equipos	Amenaza a instalaciones	3
AME-16	Corto Circuito	Amenaza a instalaciones	3
AME-17	Pérdida de personal clave	Amenazas Humanas	3
AME-18	Sabotaje por parte de personal	Amenazas Sociales	3
AME-19	Crisis financiera (presupuesto)	Amenazas Operacionales	3
AME-20	Uso no autorizado del equipo	Amenazas deliberadas	3
AME-21	Incumplimiento en la disponibilidad del personal	Amenazas deliberadas	3
AME-22	Hurto de medios o documentos	Amenazas deliberadas	3
AME-23	Falsificación de derechos	Amenazas deliberadas	3
AME-24	Falla en el sistema de suministro de agua o de aire acondicionado	Amenaza a instalaciones	3
AME-25	Fuga de Gas	Amenaza a instalaciones	2
AME-26	Huelgas	Amenazas Humanas	2

Anexo 15: Lista de vulnerabilidades

Aspecto del análisis	Identificación de Vulnerabilidades	**Código de análisis**	2017AVA03
Empresa de estudio	Unión Peruana del Norte	**Empresa a cargo**	System Auditors
Área de estudio	Área de tecnologías de información (TI)	**Encargado**	Luis Torres Torres

ID	**Descripción de las vulnerabilidades en la Organización**
Vul-01	Faltas de políticas para el mantenimiento de los dispositivos
Vul-02	Inadecuada protección al equipo
Vul-03	Información no encriptada
Vul-04	Passwords débiles
Vul-05	Password sin modificarse
Vul-06	Falta de políticas para el control de acceso
Vul-07	Validación de usuario por perfil (Autenticación inadecuada)
Vul-08	Falta de monitoreo en los contratos del personal
Vul-09	Falta de capacitación de seguridad al personal
Vul-10	Falta de evaluaciones para detectar vulnerabilidades
Vul-11	Falta de criticidad en la información
Vul-12	Falta de procedimiento de prevención frente a un ataque de software malicioso
Vul-13	No eliminar el acceso a los sistemas de información, al personal que no labora
Vul-14	Incumplimiento del contrato
Vul-15	Carencia de procedimiento que asegure la entrega de activos al termino del contrato de trabajo
Vul-16	Susceptibilidad de equipos a variaciones de voltaje
Vul-17	Protección inapropiada en los almacenes
Vul-18	Falta de gestión para la concesión de acceso a las instalaciones
Vul-19	No concluir por completo las peticiones formales de acceso
Vul-20	Falta de restricciones en el perímetro que permita el libre acceso a ubicaciones de TI sensibles
Vul-21	No supervisar el acceso a las instalaciones de TI
Vul-22	No tener una identificación visible en la organización
Vul-23	Carencia de mecanismos que aseguren el envió y recepción de mensajes
Vul-24	Falta de protección en las redes públicas
Vul-25	No realizar una copia de respaldo (back-up)
Vul-26	Carencia de tareas segregadas
Vul-27	Control de cambio inadecuado
Vul-28	Políticas incompletas para el uso de criptografía
Vul-29	Carencia de ensayos de software
Vul-30	Documentación pobre de software
Vul-31	Carencia de copia de respaldo (Back - Up) en la nube
Vul-32	Carencia de validación de datos procesados
Vul-33	Falta de capacitación para el debido manejo(recepción y uso) de documentos especiales
Vul-34	Inadecuada asignación de privilegios de accesos a los documentos sensibles
Vul-35	Inexistente registro de dispositivos de salida
Vul-36	Inexistente registro de documentos especiales
Vul-37	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
Vul-38	Falta de políticas para el desarrollo seguro
Vul-39	Falta de un registro de eventos relacionados con la seguridad
Vul-40	Falta de definición de incidentes potenciales que afecten a la seguridad
Vul-41	Falta de un procedimiento que reúna las evidencias de los incidentes de seguridad
Vul-42	Falta de conocimiento de los empleados sobre las evidencias de un incidente de seguridad
Vul-43	Falta de monitorización de incidentes de seguridad
Vul-44	Falta de protección criptográficas
Vul-45	No realizar pruebas de intrusión
Vul-46	Falta de filtrado de red en dispositivos de usuario final
Vul-47	No tener la ultima actualización del sistema operativo
Vul-48	No tener cifrada la información almacenada en la organización
Vul-49	Falta de autenticación en las aplicaciones
Vul-50	Falta de registro de monitoreo en los perfiles de usuario
Vul-51	No se revisa los privilegios asignados a los usuarios
Vul-52	Falta de identificación de las actividades realizadas por el usuario
Vul-53	No tener la ultima actualización del antivirus
Vul-54	Falta de recursos economicos

Anexo 16: Relación Activo – Vulnerabilidad

Aspecto del análisis	Relación Activos - Vulnerabilidades	**Código de análisis**	2017AVA04
Empresa de estudio	Unión Peruana del Norte	**Empresa a cargo**	System Auditors
Área de estudio	Área de tecnologías de información (TI)	**Encargados**	Samuel Gavidia Mamani Luis Daniel Torres Torres

Activos	**Vulnerabilidades**
Base de Datos	No eliminar el acceso a los sistemas de información, al personal que no labora
	Falta de evaluaciones para detectar vulnerabilidades
	Password sin modificarse
	Inadecuada protección al equipo
Copia de respaldo Base de Datos	No realizar una copia de respaldo (back-up)
	Carencia de copia de respaldo (Back - Up) en la nube
Copia de respaldo software	No realizar una copia de respaldo (back-up)
	Carencia de copia de respaldo (Back - Up) en la nube
	Carencia de ensayos de software
	Documentación pobre de software
CPU - Servidor de correo	Falta de políticas para el control de acceso
	No realizar pruebas de intrusión
	Carencia de mecanismos que aseguren el envio y recepción de mensajes
	Validación de usuario por perfil (Autenticación Inadecuada)
	Inadecuada protección al equipo
	Protección inapropiada en los almacenes
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Susceptibilidad de equipos a variaciones de voltaje
	Falta de políticas para el mantenimiento de los dispositivos
	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles
	No supervisar el acceso a las instalaciones a TI
CPU - Centro de datos	No realizar pruebas de intrusión
	Falta de políticas para el control de acceso
	Validación de usuario por perfil (Autenticación Inadecuada)
	Protección inapropiada en los almacenes
	Inadecuada protección al equipo
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Susceptibilidad de equipos a variaciones de voltaje
	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles
	No supervisar el acceso a las instalaciones a TI
	Falta de políticas para el mantenimiento de los dispositivos
Red y Conectividad	Carencia de mecanismos que aseguren el envio y recepción de mensajes
	Falta de Protección en las redes publicas
	No realizar pruebas de intrusión
	Falta de políticas para el control de acceso
	Información no encriptada
	políticas incompletas para el uso de criptografía
	Falta de filtrado de red en dispositivos de usuario final
	Inadecuada protección al equipo
	Susceptibilidad de equipos a variaciones de voltaje

Servidores Dell Poweredge R630 - Base de Datos	Protección inapropiada en los almacenes
	Falta de políticas para el mantenimiento de los dispositivos
	Inadecuada protección al equipo
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Susceptibilidad de equipos a variaciones de voltaje
	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles
	No supervisar el acceso a las instalaciones a TI
	Carencia de validación de datos procesados
	Password sin modificarse
Servidores Dell Poweredge R630 - Archivos	Protección inapropiada en los almacenes
	Falta de políticas para el mantenimiento de los dispositivos
	Inadecuada protección al equipo
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Susceptibilidad de equipos a variaciones de voltaje
	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles
	No supervisar el acceso a las instalaciones a TI
	No tener cifrada la información almacenada en la organización
Servidores Dell Poweredge R230 - Firewall	Protección inapropiada en los almacenes
	Falta de políticas para el mantenimiento de los dispositivos
	Inadecuada protección al equipo
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Susceptibilidad de equipos a variaciones de voltaje
	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles
	No supervisar el acceso a las instalaciones a TI
	Falta de protección en las redes públicas
	No realizar pruebas de intrusión
	Falta de políticas para el control de acceso
Switches Dell networking N3048P (Corp - Principal)	Faltas de políticas para el mantenimiento de los dispositivos
	Inadecuada protección al equipo
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	No realizar pruebas de intrusión
	Falta de protección en las redes públicas
	Susceptibilidad de equipos a variaciones de voltaje
	Falta de evaluaciones para detectar vulnerabilidades
	No realizar pruebas de intrusión
Jefe de TI	No eliminar el acceso a los sistemas de información, al personal que no labora
	No tener una identificación visible en la organización
	No se revisa los privilegios asignados a los usuarios
	Incumplimiento del contrato
Analista de Sistemas Académicos y Gerenciales	No eliminar el acceso a los sistemas de información, al personal que no labora
	No tener una identificación visible en la organización
	No se revisa los privilegios asignados a los usuarios
Servidor Pack cable HP Proliant DL 160 GB Intel	Protección inapropiada en los almacenes
	Falta de políticas para el mantenimiento de los dispositivos
	Inadecuada protección al equipo
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Susceptibilidad de equipos a variaciones de voltaje
	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles
	No supervisar el acceso a las instalaciones a TI
Servidor HP Proliant DL 120GB 6 Intel XEON 343	Protección inapropiada en los almacenes
	Falta de políticas para el mantenimiento de los dispositivos
	Inadecuada protección al equipo
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Susceptibilidad de equipos a variaciones de voltaje
	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles
	No supervisar el acceso a las instalaciones a TI
CPU - Servidor central telefónica	Falta de Protección en las redes publicas
	Protección inapropiada en los almacenes
	Falta de políticas para el mantenimiento de los dispositivos
	Inadecuada protección al equipo
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Susceptibilidad de equipos a variaciones de voltaje
	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles
	No supervisar el acceso a las instalaciones a TI

Laptop Dell Tes. Asistente oper.	Falta de políticas para el mantenimiento de los dispositivos
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Inadecuada protección al equipo
	Susceptibilidad de equipos a variaciones de voltaje
	Falta de procedimiento de prevención frente a un ataque de software malicioso
	No tener la ultima actualización del sistema operativo
	No supervisar el acceso a las instalaciones a TI
Notebook DELL serie 3000 14" i5	Falta de políticas para el mantenimiento de los dispositivos
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Inadecuada protección al equipo
	Susceptibilidad de equipos a variaciones de voltaje
	Falta de procedimiento de prevención frente a un ataque de software malicioso
	No tener la ultima actualización del sistema operativo
	No supervisar el acceso a las instalaciones a TI
Laptop Mac Book	Falta de políticas para el mantenimiento de los dispositivos
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Inadecuada protección al equipo
	Susceptibilidad de equipos a variaciones de voltaje
	Falta de procedimiento de prevención frente a un ataque de software malicioso
	No tener la ultima actualización del sistema operativo
	No supervisar el acceso a las instalaciones a TI
Laptop Latitude 5470 - i5 8 GB 1 TB HD - 126 VZF2	Falta de políticas para el mantenimiento de los dispositivos
	lta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Inadecuada protección al equipo
	Susceptibilidad de equipos a variaciones de voltaje
	Falta de procedimiento de prevención frente a un ataque de software malicioso
	No tener la ultima actualización del sistema operativo
	No supervisar el acceso a las instalaciones a TI
2 Laptop Latitude E5470 - I7 16 GB 1 TB FHD	Falta de políticas para el mantenimiento de los dispositivos
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Inadecuada protección al equipo
	Susceptibilidad de equipos a variaciones de voltaje
	No tener la utltima actualización del antivirus
	No tener la ultima actualización del sistema operativo
	No supervisar el acceso a las instalaciones a TI
Servidores Dell Poweredge R230 - DHCP(Navegación)	Protección inapropiada en los almacenes
	Falta de políticas para el mantenimiento de los dispositivos
	Inadecuada protección al equipo
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Susceptibilidad de equipos a variaciones de voltaje
	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles
	No supervisar el acceso a las instalaciones a TI
	Falta de pruebas de intrusion
	Falta de filtrado de red en dispositivos de usuario final
Servidores Dell Poweredge R230 - WEB	Protección inapropiada en los almacenes
	Falta de políticas para el mantenimiento de los dispositivos
	Inadecuada protección al equipo
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Susceptibilidad de equipos a variaciones de voltaje
	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles
	No supervisar el acceso a las instalaciones a TI
	Falta de protección en las redes públicas
	Falta de filtrado de red en dispositivos de usuario final
Servidor Redundante - Dell poweredge Intel xeon y DELL power Intel	Protección inapropiada en los almacenes
	Falta de políticas para el mantenimiento de los dispositivos
	Inadecuada protección al equipo
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Susceptibilidad de equipos a variaciones de voltaje
	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles
	No supervisar el acceso a las instalaciones a TI
cámara de video vigilancia	Protección inapropiada en los almacenes
	No supervisar el acceso a las instalaciones de TI
Licencia de antivirus Gdata versión 2017	Perdida de recursos economicos

Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Passwords débiles
	Password sin modificarse
	Falta de evaluaciones para detectar vulnerabilidades
	Falta de políticas para el control de acceso
	Validación de usuario por perfil (Autenticación Inadecuada)
	No eliminar el acceso a los sistemas de información, al personal que no labora
	No realizar una copia de respaldo (Back - Up)
	políticas incompletas para el uso de criptografía
	Carencia de copia de respaldo (Back - Up) en la nube
	falta de Protección criptográficas
	Falta de filtrado de red en dispositivos de usuario final
	Falta de Autenticación en las aplicaciones
	falta de registros de monitoreo en los perfiles de usuario
	No se revisa los privilegios asignados a los usuarios
	No realizar pruebas de intrusión
	Carencia de validación de datos procesados
	Falta de politicas para el desarrollo seguro
	control de cambio inadecuado
	Carencia de ensayos de software
	Documentación pobre de software
Disco duro externo wster digital	Inadecuada protección al equipo
	Falta de procedimiento de prevención frente a un ataque de software malicioso
	No realizar una copia de respaldo (back-up)
Equipo de control de asistencia	No eliminar el acceso a los sistemas de información, al personal que no labora
	Carencia de validación de datos procesados
	Inadecuada protección al equipo
Accesorios de Informatica - Switches	Faltas de políticas para el mantenimiento de los dispositivos
	Inadecuada protección al equipo
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
Switch dlink DES 1210 19" para telefonía	Faltas de políticas para el mantenimiento de los dispositivos
	Inadecuada protección al equipo
	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.
	Falta de protección en las redes públicas
Manuales de Usuario	Falta de criticidad en la información
	Documentación pobre de software
	Falta de capacitación para el debido manejo(recepción y uso) de documentos especiales
	Inadecuada asignación de privilegios de accesos a los documentos sensibles
software control de asistencia premium	No eliminar el acceso a los sistemas de información, al personal que no labora
	Validación de usuario por perfil (Autenticación Inadecuada)
	Carencia de validación de datos procesados
	Falta de Autenticación en las aplicaciones
	Falta de identificación de las actividades realizadas por el usuario
Helpdesk (Servicio de soporte y mantenimiento)	Falta de políticas para el mantenimiento de los dispositivos
	Falta de evaluaciones para detectar vulnerabilidades
	Falta de conocimiento de los empleados sobre las evidencias de un incidente de seguridad
	Falta de monitorización de incidente de seguridad
Contratos	Falta de monitoreo en los contratos del personal
	Incumplimiento del contrato
	Carencia de procedimiento que asegure la entrega de activos al termino del contrato de trabajo
Estabilizador - UPS TRIPP SmathOnLine servidores	Inadecuada proteccion al equipo
	Protección inapropiada en los almacenes
Grupo Electrógeno - Transformador de aislamiento de 12 KVA flash power	Inadecuada proteccion al equipo
	Protección inapropiada en los almacenes

Anexo 17: Lista de Riesgos generales

Aspecto del análisis		Relación activos - Vulnerabilidades - Amenazas		**Código de análisis**	2017 AVA05	
Empresa de estudio		Unión Peruana del Norte		**Empresa a cargo**	System Auditors	
Área de estudio		Área de tecnologías de información (TI)		**Encargados**	Samuel Gavidia Mamani Luis Daniel Torres Torres	
Código	**Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad Ocurrencia(PO)**	**Impacto**	**Valor**
Riesgo-01	**Base de Datos**	Pérdida de datos	No eliminar el acceso a los sistemas de información, al personal que no labora	4	5	20
Riesgo-02		Pérdida de datos	Falta de evaluaciones para detectar vulnerabilidades	4	5	20
Riesgo-03		Pérdida de datos	Password sin modificarse	4	5	20
Riesgo-04		Pérdida de datos	Inadecuada protección al equipo	3	4	12
Riesgo-05	Copia de respaldo de base de datos	Virus/ Malware	No realizar una copia de respaldo (Back - Up)	4	5	20
Riesgo-06		Hacking	No realizar una copia de respaldo (Back - Up)	4	5	20
Riesgo-07		Hacking	Carencia de copia de respaldo (Back - Up) en la nube	4	5	20
Riesgo-08		Falla en la base de datos	No realizar una copia de respaldo (Back - Up)	4	5	20
Riesgo-09		Falla en la base de datos	Carencia de copia de respaldo (Back - Up) en la nube	4	5	20
Riesgo-10	Copia de respaldo de Software	Virus/ Malware	No realizar una copia de respaldo (Back - Up)	4	5	20
Riesgo-11		Hacking	Carencia de copia de respaldo (Back - Up) en la nube	4	5	20
Riesgo-12		Hacking	No realizar una copia de respaldo (Back - Up)	4	5	20
Riesgo-13		Incumplimiento en el mantenimiento del sistema de información	Carencia de ensayos de software	3	4	12
Riesgo-14		Copia fraudulenta del software	Documentación pobre de software	3	4	12
Riesgo-15	CPU - Servidor de correo	Hacking	Falta de políticas para el control de acceso	4	5	20
Riesgo-16		Hacking	No realizar pruebas de intrusión	4	5	20
Riesgo-17		Hacking	Carencia de mecanismos que aseguren el envio y recepción de mensajes	4	5	20
Riesgo-18		Hacking	Validación de usuario por perfil (Autenticación Inadecuada)	4	5	20
Riesgo-19		Fallas de red	No realizar pruebas de intrusión	4	5	20
Riesgo-20		Fallas de red	Carencia de mecanismos que aseguren el envio y recepción de mensajes	4	5	20
Riesgo-21		Fallas de servidores	Inadecuada protección al equipo	4	4	16
Riesgo-22		Fallas de servidores	Protección inapropiada en los almacenes	4	4	16
Riesgo-23		Fallas de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
Riesgo-24		Falla en el suministro de agua o de aire acondicionado	Protección inapropiada en los almacenes	4	4	16
Riesgo-25		Explosión de conexiones	Inadecuada protección al equipo	3	4	12
Riesgo-26		Explosión de conexiones	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-27		Corto circuito	Inadecuada protección al equipo	3	4	12
Riesgo-28		Corto circuito	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-29		Corto circuito	Protección inapropiada en los almacenes	3	4	12
Riesgo-30		Sabotaje por parte del personal	Falta de políticas para el mantenimiento de los dispositivos	3	4	12
Riesgo-31		Sabotaje por parte del personal	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles	3	4	12
Riesgo-32		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12
Riesgo-33		Sismos	Protección inapropiada en los almacenes	2	4	8

Riesgo-34	CPU - Centro de datos	Hacking	No realizar pruebas de intrusión	4	5	20
Riesgo-35		Hacking	Falta de políticas para el control de acceso	4	5	20
Riesgo-36		Hacking	Validación de usuario por perfil (Autenticación Inadecuada)	4	5	20
Riesgo-37		Fallas de red	No realizar pruebas de intrusión	4	4	16
Riesgo-38		Fallas de servidores	Protección inapropiada en los almacenes	4	4	16
Riesgo-39		Fallas de servidores	Inadecuada protección al equipo	4	4	16
Riesgo-40		Fallas de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
Riesgo-41		Falla en el suministro de agua o de aire acondicionado	Protección inapropiada en los almacenes	4	4	16
Riesgo-42		Explosión de conexiones	Inadecuada protección al equipo	3	4	12
Riesgo-43		Explosión de conexiones	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-44		Corto circuito	Inadecuada protección al equipo	3	4	12
Riesgo-45		Corto circuito	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-46		Corto circuito	Protección inapropiada en los almacenes	3	4	12
Riesgo-47		Sabotaje por parte del personal	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles	3	4	12
Riesgo-48		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12
Riesgo-49		Sabotaje por parte del personal	Falta de políticas para el mantenimiento de los dispositivos	3	4	12
Riesgo-50		Sismos	Protección inapropiada en los almacenes	2	4	8
Riesgo-51	Red y conectividad	Espionaje remoto	Carencia de mecanismos que aseguren el envio y recepción de mensajes	4	5	20
Riesgo-52		Fallas de red	Falta de Protección en las redes publicas	4	5	20
Riesgo-53		Fallas de red	No realizar pruebas de intrusión	4	5	20
Riesgo-54		Espionaje remoto	Falta de políticas para el control de acceso	4	5	20
Riesgo-55		Espionaje remoto	Falta de Protección en las redes publicas	4	5	20
Riesgo-56		Espionaje remoto	No realizar pruebas de intrusión	4	5	20
Riesgo-57		Virus/ Malware	Falta de Protección en las redes publicas	4	5	20
Riesgo-58		Virus/ Malware	Información no encriptada	4	5	20
Riesgo-59		Virus/ Malware	políticas incompletas para el uso de criptografía	4	5	20
Riesgo-60		Fallas de red	Falta de filtrado de red en dispositivos de usuario final	4	4	16
Riesgo-61		Espionaje remoto	Falta de filtrado de red en dispositivos de usuario final	4	4	16
Riesgo-62		Espionaje remoto	Información no encriptada	4	4	16
Riesgo-63		Espionaje remoto	políticas incompletas para el uso de criptografía	4	4	16
Riesgo-64		Explosión de conexiones	Inadecuada protección al equipo	3	4	12
Riesgo-65		Explosión de conexiones	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-66		Corto circuito	Inadecuada protección al equipo	3	4	12
Riesgo-67		Corto circuito	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-68		Sabotaje por parte del personal	No realizar pruebas de intrusión	3	4	12
Riesgo-69	Servidores Dell Poweredge R630 - Base de Datos	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
Riesgo-70		Falla de servidores	faltas de políticas para el mantenimiento de los dispositivos	4	4	16
Riesgo-71		Falla de servidores	Inadecuada protección al equipo	4	4	16
Riesgo-72		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
Riesgo-73		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
Riesgo-74		Explosión de conexiones	Inadecuada protección al equipo	3	4	12
Riesgo-75		Explosión de conexiones	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-76		Corto circuito	Inadecuada protección al equipo	3	4	12
Riesgo-77		Corto circuito	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-78		Corto circuito	Protección inapropiada en los almacenes	3	4	12
Riesgo-79		Sabotaje por parte del personal	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles	3	4	12
Riesgo-80		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12
Riesgo-81		Sismos	Protección inapropiada en los almacenes	2	4	8
Riesgo-82		Perdida de Datos	Password sin modificarse	4	5	20
Riesgo-83		Perdida de Datos	Carencia de validación de datos procesados	4	5	20

Riesgo-84	Servidores Dell Poweredge R630 - Archivos	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
Riesgo-85		Falla de servidores	faltas de políticas para el mantenimiento de los dispositivos	4	4	16
Riesgo-86		Falla de servidores	Inadecuada protección al equipo	4	4	16
Riesgo-87		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
Riesgo-88		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
Riesgo-89		Explosión de conexiones	Inadecuada protección al equipo	3	4	12
Riesgo-90		Explosión de conexiones	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-91		Corto circuito	Inadecuada protección al equipo	3	4	12
Riesgo-92		Corto circuito	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-93		Corto circuito	Protección inapropiada en los almacenes	3	4	12
Riesgo-94		Sabotaje por parte del personal	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles	3	4	12
Riesgo-95		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12
Riesgo-96		Sismos	Protección inapropiada en los almacenes	2	4	8
Riesgo-97		Perdida de Datos	No tener cifrada la información almacenada en la organización	4	5	20
Riesgo-98		Espionaje remoto	No tener cifrada la información almacenada en la organización	4	5	20
Riesgo-99	Servidores Dell Poweredge R230 - Firewall	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
Riesgo-100		Falla de servidores	faltas de políticas para el mantenimiento de los dispositivos	4	4	16
Riesgo-101		Falla de servidores	Inadecuada protección al equipo	4	4	16
Riesgo-102		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
Riesgo-103		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
Riesgo-104		Explosión de conexiones	Inadecuada protección al equipo	3	4	12
Riesgo-105		Explosión de conexiones	Susceptibilidad de equipos a variaciones de	3	4	12
Riesgo-106		Corto circuito	Inadecuada protección al equipo	3	4	12
Riesgo-107		Corto circuito	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-108		Corto circuito	Protección inapropiada en los almacenes	3	4	12
Riesgo-109		Sabotaje por parte del personal	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles	3	4	12
Riesgo-110		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12
Riesgo-111		Sismos	Protección inapropiada en los almacenes	2	4	8
Riesgo-112		Fallas de red	No realizar pruebas de intrusión	4	5	20
Riesgo-113		Fallas de red	Falta de Protección en las redes publicas	4	5	20
Riesgo-114		Hacking	Falta de Protecćon en las redes publicas	4	5	20
Riesgo-115		Hacking	Falta de politicas para el control de acceso	4	5	20
Riesgo-116	Switches Dell networking N3048P (Corp - Principal)	Fallas internas de los equipos	falta de políticas para el mantenimiento de los dispositivos	3	4	12
Riesgo-117		Fallas internas de los equipos	Inadecuada protección al equipo	4	4	16
Riesgo-118		Fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	3	4	12
Riesgo-119		Hacking	No realizar pruebas de intrusión	4	5	20
Riesgo-120		Hacking	Falta de protección en las redes públicas	4	5	20
Riesgo-121		Explosion de Conexiones	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-122		Incumplimiento en la disponibilidad del personal	Falta de evaluaciones para detectar vulnerabilidades	3	4	12
Riesgo-123		Espionaje remoto	No realizar pruebas de intrusión	4	5	20
Riesgo-124		Espionaje remoto	Falta de protección en las redes públicas	4	5	20
Riesgo-125		Fallas de red	Falta de protección en las redes públicas	4	5	20
Riesgo-126	Jefe de TI	falsificación de derechos	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
Riesgo-127		falsificación de derechos	No tener una identificación visible en la organización	4	4	16
Riesgo-128		falsificación de derechos	No se revisa los privilegios asignados a los usuarios	4	4	16
Riesgo-129		Pérdida de personal clave	Incumplimiento del contrato	4	4	16

Riesgo-130	Analista de Sistemas académicos y Gerenciales	falsificación de derechos	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
Riesgo-131		falsificación de derechos	No tener una identificación visible en la organización	4	4	16
Riesgo-132		falsificación de derechos	No se revisa los privilegios asignados a los usuarios	4	4	16
Riesgo-133	Servidor Pack cable HP Proliant DL 160 GB Intel	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
Riesgo-134		Falla de servidores	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
Riesgo-135		Falla de servidores	Inadecuada protección al equipo	4	4	16
Riesgo-136		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
Riesgo-137		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
Riesgo-138		Explosión de conexiones	Inadecuada protección al equipo	3	4	12
Riesgo-139		Explosión de conexiones	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-140		Corto circuito	Inadecuada protección al equipo	3	4	12
Riesgo-141		Corto circuito	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-142		Corto circuito	Protección inapropiada en los almacenes	3	4	12
Riesgo-143		Sabotaje por parte del personal	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles	3	4	12
Riesgo-144		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12
Riesgo-145		Sismos	Protección inapropiada en los almacenes	2	4	8
Riesgo-146	Servidor HP Proliant DL 120GB 6 Intel XEON 343	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
Riesgo-147		Falla de servidores	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
Riesgo-148		Falla de servidores	Inadecuada protección al equipo	4	4	16
Riesgo-149		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
Riesgo-150		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
Riesgo-151		Explosión de conexiones	Inadecuada protección al equipo	3	4	12
Riesgo-152		Explosión de conexiones	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-153		Corto circuito	Inadecuada protección al equipo	3	4	12
Riesgo-154		Corto circuito	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-155		Corto circuito	Protección inapropiada en los almacenes	3	4	12
Riesgo-156		Sabotaje por parte del personal	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles	3	4	12
Riesgo-157		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12
Riesgo-158		Sismos	Protección inapropiada en los almacenes	2	4	8
Riesgo-159	CPU - Servidor central telefónica	Falla en telefonía	Falta de Protección en las redes publicas	4	4	16
Riesgo-160		Fallas de red	Falta de Protección en las redes publicas	4	4	16
Riesgo-161		Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
Riesgo-162		Falla de servidores	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
Riesgo-163		Falla de servidores	Inadecuada protección al equipo	4	4	16
Riesgo-164		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
Riesgo-165		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
Riesgo-166		Explosión de conexiones	Inadecuada protección al equipo	3	4	12
Riesgo-167		Explosión de conexiones	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-168		Corto circuito	Inadecuada protección al equipo	3	4	12
Riesgo-169		Corto circuito	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-170		Corto circuito	Protección inapropiada en los almacenes	3	4	12
Riesgo-171		Sabotaje por parte del personal	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles	3	4	12
Riesgo-172		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12
Riesgo-173		Sismos	Protección inapropiada en los almacenes	2	4	8

Riesgo-174	Laptop Dell Tes. Asistente oper.	Fallas internas de los equipos	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
Riesgo-175		Fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
Riesgo-176		Virus/ Malware	Falta de procedimiento de prevención frente a un ataque de software malicioso	4	4	16
Riesgo-177		Fallas internas de los equipos	Inadecuada protección al equipo	3	4	12
Riesgo-178		Fallas internas de los equipos	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-179		Virus/ Malware	No tener la ultima actualización del sistema operativo	3	4	12
Riesgo-180		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12
Riesgo-181	Notebook DELL serie 3000 14" i5	Fallas internas de los equipos	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
Riesgo-182		Fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
Riesgo-183		Virus/ Malware	Falta de procedimiento de prevención frente a un ataque de software malicioso	4	4	16
Riesgo-184		Fallas internas de los equipos	Inadecuada protección al equipo	3	4	12
Riesgo-185		Fallas internas de los equipos	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-186		Virus/ Malware	No tener la ultima actualización del sistema operativo	3	4	12
Riesgo-187		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12
Riesgo-188	Laptop Mac Book	fallas internas de los equipos	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
Riesgo-189		fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
Riesgo-190		Virus/ Malware	Falta de procedimiento de prevención frente a un ataque de software malicioso	4	4	16
Riesgo-191		fallas internas de los equipos	Inadecuada protección al equipo	3	4	12
Riesgo-192		fallas internas de los equipos	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-193		Virus/ Malware	No tener la ultima actualización del sistema operativo	3	4	12
Riesgo-194		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12
Riesgo-195	Laptop Latitude 5470 - i5 8 GB 1 TB HD - 126 VZF2	Fallas internas de los equipos	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
Riesgo-196		Fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
Riesgo-197		Virus/ Malware	Falta de procedimiento de prevención frente a un ataque de software malicioso	4	4	16
Riesgo-198		Fallas internas de los equipos	Inadecuada protección al equipo	3	4	12
Riesgo-199		Fallas internas de los equipos	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-200		Virus/ Malware	No tener la ultima actualización del sistema operativo	3	4	12
Riesgo-201		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12
Riesgo-202	2 Laptop Latitude E5470 - I7 16 GB 1 TB FHD	fallas internas de los equipos	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
Riesgo-203		fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
Riesgo-204		Virus/ Malware	Inadecuada protección al equipo	4	4	16
Riesgo-205		fallas internas de los equipos	Inadecuada protección al equipo	3	4	12
Riesgo-206		fallas internas de los equipos	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-207		Virus/ Malware	No tener la ultima actualización del sistema operativo	3	4	12
Riesgo-208		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12

Riesgo-209	Servidores Dell Poweredge R230 - DHCP(Puerto)	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
Riesgo-210		Falla de servidores	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
Riesgo-211		Falla de servidores	Inadecuada protección al equipo	4	4	16
Riesgo-212		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
Riesgo-213		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
Riesgo-214		Explosión de conexiones	Inadecuada protección al equipo	3	4	12
Riesgo-215		Explosión de conexiones	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-216		Corto circuito	Inadecuada protección al equipo	3	4	12
Riesgo-217		Corto circuito	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-218		Corto circuito	Protección inapropiada en los almacenes	3	4	12
Riesgo-219		Sabotaje por parte del personal	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles	3	4	12
Riesgo-220		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12
Riesgo-221		Sismos	Protección inapropiada en los almacenes	2	4	8
Riesgo-222		Espionaje remoto	Falta de pruebas de intrusion	4	5	20
Riesgo-223		Espionaje remoto	Falta de filtrado de red en dispositivos de usuario fi	4	5	20
Riesgo-224		Fallas de red	Falta de pruebas de intrusion	4	5	20
Riesgo-225	Servidores Dell Poweredge R230 - WEB	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
Riesgo-226		Falla de servidores	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
Riesgo-227		Falla de servidores	Inadecuada protección al equipo	4	4	16
Riesgo-228		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
Riesgo-229		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
Riesgo-230		Explosión de conexiones	Inadecuada protección al equipo	3	4	12
Riesgo-231		Explosión de conexiones	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-232		Corto circuito	Inadecuada protección al equipo	3	4	12
Riesgo-233		Corto circuito	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-234		Corto circuito	Protección inapropiada en los almacenes	3	4	12
Riesgo-235		Sabotaje por parte del personal	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles	3	4	12
Riesgo-236		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12
Riesgo-237		Sismos	Protección inapropiada en los almacenes	2	4	8
Riesgo-238		Hacking	Falta de protección en las redes públicas	4	5	20
Riesgo-239		Espionaje remoto	Falta de filtrado de red en dispositivos de usuario fi	4	5	20
Riesgo-240	Servidor Redundante - Dell poweredge Intel xeon y DELL power Intel	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
Riesgo-241		Falla de servidores	faltas de políticas para el mantenimiento de los dispositivos	4	4	16
Riesgo-242		Falla de servidores	Inadecuada protección al equipo	4	4	16
Riesgo-243		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
Riesgo-244		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
Riesgo-245		Explosión de conexiones	Inadecuada protección al equipo	3	4	12
Riesgo-246		Explosión de conexiones	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-247		Corto circuito	Inadecuada protección al equipo	3	4	12
Riesgo-248		Corto circuito	Susceptibilidad de equipos a variaciones de voltaje	3	4	12
Riesgo-249		Corto circuito	Protección inapropiada en los almacenes	3	4	12
Riesgo-250		Sabotaje por parte del personal	Falta de restricciones en el perímetro que permite el libre acceso a ubicaciones de TI sensibles	3	4	12
Riesgo-251		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12
Riesgo-252		Sismos	Protección inapropiada en los almacenes	2	4	8
Riesgo-253	Caramas de video vigilancia	Fallas internas de los equipos	Protección inapropiada en los almacenes	4	4	16
Riesgo-254		Sabotaje por parte del personal	No supervisar el acceso a las instalaciones a TI	3	4	12
Riesgo-255	Antivirus Gdata versión 2017	Crisis Financiera (presupuesto)	Perdida de recursos economicos	4	4	16

Riesgo-256	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Virus/ Malware	Passwords débiles	4	4	16
Riesgo-257		Virus/ Malware	Password sin modificarse	4	4	16
Riesgo-258		Virus/ Malware	Falta de evaluaciones para detectar vulnerabilidades	4	4	16
Riesgo-259		Hacking	Passwords débiles	4	4	16
Riesgo-260		Hacking	Password sin modificarse	4	4	16
Riesgo-261		Hacking	Falta de políticas para el control de acceso	4	4	16
Riesgo-262		Hacking	Validación de usuario por perfil (Autenticación Inadecuada)	4	4	16
Riesgo-263		Hacking	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
Riesgo-264		Hacking	Falta de evaluaciones para detectar vulnerabilidades	4	4	16
Riesgo-265		Hacking	No realizar una copia de respaldo (Back - Up)	4	4	16
Riesgo-266		Hacking	políticas incompletas para el uso de criptografía	4	4	16
Riesgo-267		Hacking	Carencia de copia de respaldo (Back - Up) en la nube	4	4	16
Riesgo-268		Hacking	falta de Protección criptográficas	4	4	16
Riesgo-269		Hacking	Falta de filtrado de red en dispositivos de usuario final	4	4	16
Riesgo-270		Hacking	Falta de Autenticación en las aplicaciones	4	4	16
Riesgo-271		Hacking	falta de registros de monitoreo en los perfiles de usuario	4	4	16
Riesgo-272		Hacking	No se revisa los privilegios asignados a los usuarios	4	4	16
Riesgo-273		Hacking	No realizar pruebas de intrusión	4	4	16
Riesgo-274		Fallas de red	Validación de usuario por perfil (Autenticación Inadecuada)	4	4	16
Riesgo-275		Fallas de red	Falta de filtrado de red en dispositivos de usuario final	4	4	16
Riesgo-276		Fallas de servidores	Validación de usuario por perfil (Autenticación Inadecuada)	4	4	16
Riesgo-277		Fallas de servidores	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
Riesgo-278		Falla en las aplicaciones	Validación de usuario por perfil (Autenticación Inadecuada)	4	4	16
Riesgo-279		Falla en las aplicaciones	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
Riesgo-280		Falla en las aplicaciones	Carencia de validación de datos procesados	4	4	16
Riesgo-281		Falla en las aplicaciones	Falta de politicas para el desarrollo seguro	4	4	16
Riesgo-282		Falla en las aplicaciones	Falta de filtrado de red en dispositivos de usuario final	4	4	16
Riesgo-283		Falla en las aplicaciones	Falta de Autenticación en las aplicaciones	4	4	16
Riesgo-284		Falla en las aplicaciones	falta de registros de monitoreo en los perfiles de usuario	4	4	16
Riesgo-285		Falla en las aplicaciones	No se revisa los privilegios asignados a los usuarios	4	4	16
Riesgo-286		Falla en las aplicaciones	control de cambio inadecuado	4	4	16
Riesgo-287		Falla en las aplicaciones	No realizar pruebas de intrusión	4	4	16
Riesgo-288		Incumplimiento en el mantenimiento del sistema de información	Carencia de ensayos de software	4	4	16
Riesgo-289		Copia fraudulenta del software	Documentación pobre de software	4	4	16
Riesgo-290		Fallas de servidores	Carencia de validación de datos procesados	3	4	12
Riesgo-291		Fallas de servidores	Falta de Autenticación en las aplicaciones	3	4	12
Riesgo-292		Fallas de servidores	Falta de registro de monitoreo en los perfiles de usuario	3	4	12
Riesgo-293		Fallas de servidores	No se revisa los privilegios asignados a los usuarios	3	4	12
Riesgo-294		Fallas de servidores	No realizar pruebas de intrusión	3	4	12
Riesgo-295		Falla en la base de datos	Validación de usuario por perfil (Autenticación Inadecuada)	3	4	12
Riesgo-296		Falla en la base de datos	No eliminar el acceso a los sistemas de información, al personal que no labora	3	4	12
Riesgo-297		Falla en la base de datos	Carencia de validación de datos procesados	3	4	12
Riesgo-298		Falla en la base de datos	Falta de Autenticación en las aplicaciones	3	4	12
Riesgo-299		Falla en la base de datos	falta de registros de monitoreo en los perfiles de usuario	3	4	12
Riesgo-300		Falla en la base de datos	No se revisa los privilegios asignados a los usuarios	3	4	12
Riesgo-301		Sabotaje por parte del personal	Validación de usuario por perfil (Autenticación Inadecuada)	3	4	12
Riesgo-302		Sabotaje por parte del personal	No realizar una copia de respaldo (Back - Up)	3	4	12
Riesgo-303		Sabotaje por parte del personal	Carencia de copia de respaldo (Back - Up) en la nube	3	4	12
Riesgo-304		Sabotaje por parte del personal	Falta de filtrado de red en dispositivos de usuario final	3	4	12
Riesgo-305		Sabotaje por parte del personal	Falta de Autenticación en las aplicaciones	3	4	12
Riesgo-306		Sabotaje por parte del personal	Falta de registro de monitoreo en los perfiles de usuario	3	4	12
Riesgo-307		Sabotaje por parte del personal	No se revisa los privilegios asignados a los usuarios	3	4	12
Riesgo-308		Copia fraudulenta del software	control de cambio inadecuado	3	4	12

Riesgo-309	Disco duro externo wster digital	Virus/ Malware	Falta de procedimiento de prevención frente a un ataque de software malicioso	4	5	20
Riesgo-310		Fallas internas de los equipos	Inadecuada protección al equipo	4	4	16
Riesgo-311		Sabotaje por parte del personal	No realizar una copia de respaldo (Back - Up)	3	4	12
Riesgo-312	Equipo de control de asistencia	falsificación de derechos	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
Riesgo-313		Uso no autorizado del equipo	Carencia de validación de datos procesados	3	4	12
Riesgo-314		fallas internas de los equipos	Inadecuada protección al equipo	3	3	9
Riesgo-315	Accesorios de Informatica - Switches	Fallas internas de los equipos	falta de políticas para el mantenimiento de los dispositivos	3	4	12
Riesgo-316		Fallas internas de los equipos	Inadecuada protección al equipo	4	4	16
Riesgo-317		Fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	3	4	12
Riesgo-318	Switch dlink DES 1210 19" para telefonía	Fallas internas de los equipos	falta de políticas para el mantenimiento de los dispositivos	3	4	12
Riesgo-319		Fallas internas de los equipos	Inadecuada protección al equipo	4	4	16
Riesgo-320		Fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	3	4	12
Riesgo-321		Falla en telefonía	Falta de protección en las redes públicas	4	4	16
Riesgo-322	Manuales de usuario	Copia fraudulenta del software	Falta de criticidad en la información	4	3	12
Riesgo-323		Copia fraudulenta del software	Documentación pobre de software	4	3	12
Riesgo-324		Hurto de medios o documentos	Inadecuada asignación de privilegios de accesos a los documentos sensibles	3	3	9
Riesgo-325		Incumplimiento en la disponibilidad del personal	Falta de capacitación para el debido manejo (recepción y uso) de documentos especiales	3	3	9
Riesgo-326	Software control de asistencia Premium	Fallas de servidores	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
Riesgo-327		Fallas en las aplicaciones	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
Riesgo-328		Falla en la base de datos	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
Riesgo-329		Fallas de servidores	Validación de usuario por perfil (Autenticación Inadecuada)	3	4	12
Riesgo-330		Fallas de servidores	Carencia de validación de datos procesados	3	4	12
Riesgo-331		Fallas en las aplicaciones	Validación de usuario por perfil (Autenticación Inadecuada)	3	4	12
Riesgo-332		Fallas en las aplicaciones	Carencia de validación de datos procesados	3	4	12
Riesgo-333		Fallas en las aplicaciones	Falta de Autenticación en las aplicaciones	3	4	12
Riesgo-334		Falla en la base de datos	Validación de usuario por perfil (Autenticación Inadecuada)	3	4	12
Riesgo-335		Falla en la base de datos	Falta de Autenticación en las aplicaciones	3	4	12
Riesgo-336		falsificación de derechos	Falta de identificación de las actividades realizadas por el usuario	3	4	12

Riesgo-337	Helpdesk (Servicio de soporte y mantenimiento)	Uso no autorizado del equipo	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
Riesgo-338		Incumplimiento en la disponibilidad del personal	Falta de evaluaciones para detectar vulnerabilidades	3	3	9
Riesgo-339		Incumplimiento en la disponibilidad del personal	Falta de conocimiento de los empleados sobre las evidencias de un incidente de seguridad	3	3	9
Riesgo-340		Incumplimiento en la disponibilidad del personal	Falta de monitorización de incidente de seguridad	3	3	9
Riesgo-341	Contratos	Crisis financiera (presupuesto)	Incumplimiento del contrato	3	3	9
Riesgo-342		Perdida de personal clave	Incumplimiento del contrato	3	3	9
Riesgo-343		Perdida de personal clave	Falta de monitoreo en los contratos del personal	2	3	6
Riesgo-344		Perdida de personal clave	Carencia de procedimiento que asegure la entrega de activos al termino del contrato de trabajo	2	3	6
Riesgo-345	Estabilizador - UPS TRIPP SmathOnLine servidores	Falla en el suministro de agua o de aire acondicionado	Inadecuada protección al equipo	4	4	16
Riesgo-346		Sismos	Protección inapropiada en los almacenes	3	4	12
Riesgo-347	Grupo Electrógeno - Transformador de aislamiento de 12 KVA flash power	Falla en el suministro de agua o de aire acondicionado	Iandecuada protección al equipo	4	4	16
Riesgo-348		Sismos	Protección inapropiada en los almacenes	3	4	12

Anexo 18: Lista de riesgos priorizados

Aspecto del análisis			Relación activos - Vulnerabilidades - Amenazas		Código de análisis	2017 AVA06	
Empresa de estudio			Unión Peruana del Norte		Empresa a cargo	System Auditors	
Área de estudio			Área de tecnologías de información (TI)		Encargados	Samuel Gavidia Mamani Luis Daniel Torres Torres	
Código Riesgo Priorizado	Código Riesgo	Activo	Amenaza	Vulnerabilidad	Probabilidad Ocurrencia(PO)	Impacto	Valor
RP-01	Riesgo-01	Base de Datos	Pérdida de datos	No eliminar el acceso a los sistemas de información, al personal que no labora	4	5	20
RP-02	Riesgo-02		Pérdida de datos	Falta de evaluaciones para detectar vulnerabilidades	4	5	20
RP-03	Riesgo-03		Pérdida de datos	Password sin modificarse	4	5	20
RP-04	Riesgo-05	Copia de respaldo de base de datos	Virus/ Malware	No realizar una copia de respaldo (Back - Up)	4	5	20
RP-05	Riesgo-06		Hacking	No realizar una copia de respaldo (Back - Up)	4	5	20
RP-06	Riesgo-07		Hacking	Carencia de copia de respaldo (Back - Up) en la nube	4	5	20
RP-07	Riesgo-08		Falla en la base de datos	No realizar una copia de respaldo (Back - Up)	4	5	20
RP-08	Riesgo-09		Falla en la base de datos	Carencia de copia de respaldo (Back - Up) en la nube	4	5	20
RP-09	Riesgo-10	Copia de respaldo de Software	Virus/ Malware	No realizar una copia de respaldo (Back - Up)	4	5	20
RP-10	Riesgo-11		Hacking	Carencia de copia de respaldo (Back - Up) en la nube	4	5	20
RP-11	Riesgo-12		Hacking	No realizar una copia de respaldo (Back - Up)	4	5	20
RP-12	Riesgo-15	CPU - Servidor de correo	Hacking	Falta de políticas para el control de acceso	4	5	20
RP-13	Riesgo-16		Hacking	No realizar pruebas de intrusión	4	5	20
RP-14	Riesgo-17		Hacking	Carencia de mecanismos que aseguren el envio y recepción de mensajes	4	5	20
RP-15	Riesgo-18		Hacking	Validación de usuario por perfil (Autenticación Inadecuada)	4	5	20
RP-16	Riesgo-19		Fallas de red	No realizar pruebas de intrusión	4	5	20
RP-17	Riesgo-20		Fallas de red	Carencia de mecanismos que aseguren el envio y recepción de mensajes	4	5	20
RP-18	Riesgo-21		Fallas de servidores	Inadecuada protección al equipo	4	4	16
RP-19	Riesgo-22		Fallas de servidores	Protección inapropiada en los almacenes	4	4	16
RP-20	Riesgo-23		Fallas de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
RP-21	Riesgo-24		Falla en el suministro de agua o de aire acondicionado	Protección inapropiada en los almacenes	4	4	16
RP-22	Riesgo-34	CPU - Centro de datos	Hacking	No realizar pruebas de intrusión	4	5	20
RP-23	Riesgo-35		Hacking	Falta de políticas para el control de acceso	4	5	20
RP-24	Riesgo-36		Hacking	Validación de usuario por perfil (Autenticación Inadecuada)	4	5	20
RP-25	Riesgo-37		Fallas de red	No realizar pruebas de intrusión	4	4	16
RP-26	Riesgo-38		Fallas de servidores	Protección inapropiada en los almacenes	4	4	16
RP-27	Riesgo-39		Fallas de servidores	Inadecuada protección al equipo	4	4	16
RP-28	Riesgo-40		Fallas de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
RP-29	Riesgo-41		Falla en el suministro de agua o de aire acondicionado	Protección inapropiada en los almacenes	4	4	16
RP-30	Riesgo-51	Red y conectividad	Espionaje remoto	Carencia de mecanismos que aseguren el envio y recepción de mensajes	4	5	20
RP-31	Riesgo-52		Fallas de red	Falta de Protección en las redes publicas	4	5	20
RP-32	Riesgo-53		Fallas de red	No realizar pruebas de intrusión	4	5	20
RP-33	Riesgo-54		Espionaje remoto	Falta de políticas para el control de acceso	4	5	20
RP-34	Riesgo-55		Espionaje remoto	Falta de Protección en las redes publicas	4	5	20
RP-35	Riesgo-56		Espionaje remoto	No realizar pruebas de intrusión	4	5	20
RP-36	Riesgo-57		Virus/ Malware	Falta de Protección en las redes publicas	4	5	20
RP-37	Riesgo-58		Virus/ Malware	Información no encriptada	4	5	20
RP-38	Riesgo-59		Virus/ Malware	políticas incompletas para el uso de criptografía	4	5	20
RP-39	Riesgo-60		Fallas de red	Falta de filtrado de red en dispositivos de usuario final	4	4	16
RP-40	Riesgo-61		Espionaje remoto	Falta de filtrado de red en dispositivos de usuario final	4	4	16
RP-41	Riesgo-62		Espionaje remoto	Información no encriptada	4	4	16
RP-42	Riesgo-63		Espionaje remoto	políticas incompletas para el uso de criptografía	4	4	16

RP-43	Riesgo-82	Servidores Dell Poweredge R630 - Base de Datos	Perdida de Datos	Password sin modificarse	4	5	20
RP-44	Riesgo-83		Perdida de Datos	Carencia de validación de datos procesados	4	5	20
RP-45	Riesgo-69		Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
RP-46	Riesgo-70		Falla de servidores	faltas de políticas para el mantenimiento de los dispositivos	4	4	16
RP-47	Riesgo-71		Falla de servidores	Inadecuada protección al equipo	4	4	16
RP-48	Riesgo-72		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
RP-49	Riesgo-73		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
RP-50	Riesgo-97	Servidores Dell Poweredge R630 - Archivos	Perdida de Datos	No tener cifrada la información almacenada en la organización	4	5	20
RP-51	Riesgo-98		Espionaje remoto	No tener cifrada la información almacenada en la organización	4	5	20
RP-52	Riesgo-84		Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
RP-53	Riesgo-85		Falla de servidores	faltas de políticas para el mantenimiento de los dispositivos	4	4	16
RP-54	Riesgo-86		Falla de servidores	Inadecuada protección al equipo	4	4	16
RP-55	Riesgo-87		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
RP-56	Riesgo-88		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
RP-57	Riesgo-112	Servidores Dell Poweredge R230 - Firewall	Fallas de red	No realizar pruebas de intrusión	4	5	20
RP-58	Riesgo-113		Fallas de red	Falta de Protección en las redes publicas	4	5	20
RP-59	Riesgo-114		Hacking	Falta de Protecón en las redes publicas	4	5	20
RP-60	Riesgo-115		Hacking	Falta de politicas para el control de acceso	4	5	20
RP-61	Riesgo-99		Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
RP-62	Riesgo-100		Falla de servidores	faltas de políticas para el mantenimiento de los dispositivos	4	4	16
RP-63	Riesgo-101		Falla de servidores	Inadecuada protección al equipo	4	4	16
RP-64	Riesgo-102		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
RP-65	Riesgo-103		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
RP-66	Riesgo-119	Switches Dell networking N3048P (Corp - Principal)	Hacking	No realizar pruebas de intrusión	4	5	20
RP-67	Riesgo-120		Hacking	Falta de protección en las redes públicas	4	5	20
RP-68	Riesgo-123		Espionaje remoto	No realizar pruebas de intrusión	4	5	20
RP-69	Riesgo-124		Espionaje remoto	Falta de protección en las redes públicas	4	5	20
RP-70	Riesgo-125		Fallas de red	Falta de protección en las redes públicas	4	5	20
RP-71	Riesgo-117		Fallas internas de los equipos	Inadecuada protección al equipo	4	4	16
RP-72	Riesgo-126	Jefe de TI	falsificación de derechos	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
RP-73	Riesgo-127		falsificación de derechos	No tener una identificación visible en la organización	4	4	16
RP-74	Riesgo-128		falsificación de derechos	No se revisa los privilegios asignados a los usuarios	4	4	16
RP-75	Riesgo-129		Pérdida de personal clave	Incumplimiento del contrato	4	4	16
RP-76	Riesgo-130	Analista de Sistemas académicos y Gerenciales	falsificación de derechos	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
RP-77	Riesgo-131		falsificación de derechos	No tener una identificación visible en la organización	4	4	16
RP-78	Riesgo-132		falsificación de derechos	No se revisa los privilegios asignados a los usuarios	4	4	16
RP-79	Riesgo-133	Servidor Pack cable HP Proliant DL 160 GB Intel	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
RP-80	Riesgo-134		Falla de servidores	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
RP-81	Riesgo-135		Falla de servidores	Inadecuada protección al equipo	4	4	16
RP-82	Riesgo-136		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
RP-83	Riesgo-137		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
RP-84	Riesgo-146	Servidor HP Proliant DL 120GB 6 Intel XEON 343	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
RP-85	Riesgo-147		Falla de servidores	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
RP-86	Riesgo-148		Falla de servidores	Inadecuada protección al equipo	4	4	16
RP-87	Riesgo-149		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
RP-88	Riesgo-150		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
RP-89	Riesgo-159	CPU - Servidor central telefónica	Falla en telefonía	Falta de Protección en las redes publicas	4	4	16
RP-90	Riesgo-160		Fallas de red	Falta de Protección en las redes publicas	4	4	16
RP-91	Riesgo-161		Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
RP-92	Riesgo-162		Falla de servidores	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
RP-93	Riesgo-163		Falla de servidores	Inadecuada protección al equipo	4	4	16
RP-94	Riesgo-164		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
RP-95	Riesgo-165		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16

RP-96	Riesgo-174	Laptop Dell Tes. Asistente oper.	Fallas internas de los equipos	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
RP-97	Riesgo-175		Fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
RP-98	Riesgo-176		Virus/ Malware	Falta de procedimiento de prevención frente a un ataque de software malicioso	4	4	16
RP-99	Riesgo-181	Notebook DELL serie 3000 14" i5	Fallas internas de los equipos	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
RP-100	Riesgo-182		Fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
RP-101	Riesgo-183		Virus/ Malware	Falta de procedimiento de prevención frente a un ataque de software malicioso	4	4	16
RP-102	Riesgo-188	Laptop Mac Book	fallas internas de los equipos	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
RP-103	Riesgo-189		fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
RP-104	Riesgo-190		Virus/ Malware	Falta de procedimiento de prevención frente a un ataque de software malicioso	4	4	16
RP-105	Riesgo-195	Laptop Latitude 5470 - i5 8 GB 1 TB HD - 126 VZF2	Fallas internas de los equipos	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
RP-106	Riesgo-196		Fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
RP-107	Riesgo-197		Virus/ Malware	No tener la ultima actualización de antivirus	4	4	16
RP-108	Riesgo-202	2 Laptop Latitude E5470 - I7 16 GB 1 TB FHD	fallas internas de los equipos	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
RP-109	Riesgo-203		fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
RP-110	Riesgo-204		Virus/ Malware	Inadecuada protección al equipo	4	4	16
RP-111	Riesgo-222	Servidores Dell Poweredge R230 - DHCP(Navegación)	Espionaje remoto	Falta de pruebas de intrusion	4	5	20
RP-112	Riesgo-223		Espionaje remoto	Falta de filtrado de red en dispositivos de usuario final	4	5	20
RP-113	Riesgo-224		Fallas de red	Falta de pruebas de intrusion	4	5	20
RP-114	Riesgo-209		Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
RP-115	Riesgo-210		Falla de servidores	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
RP-116	Riesgo-211		Falla de servidores	Inadecuada protección al equipo	4	4	16
RP-117	Riesgo-212		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
RP-118	Riesgo-213		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
RP-119	Riesgo-238	Servidores Dell Poweredge R230 - WEB	Hacking	Falta de protección en las redes públicas	4	5	20
RP-120	Riesgo-239		Espionaje remoto	Falta de filtrado de red en dispositivos de usuario final	4	5	20
RP-121	Riesgo-225		Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
RP-122	Riesgo-226		Falla de servidores	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
RP-123	Riesgo-227		Falla de servidores	Inadecuada protección al equipo	4	4	16
RP-124	Riesgo-228		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
RP-125	Riesgo-229		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
RP-126	Riesgo-240	Servidor Redundante - Dell poweredge Intel xeon y DELL power Intel	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16
RP-127	Riesgo-241		Falla de servidores	faltas de políticas para el mantenimiento de los dispositivos	4	4	16
RP-128	Riesgo-242		Falla de servidores	Inadecuada protección al equipo	4	4	16
RP-129	Riesgo-243		Falla de servidores	Protección inapropiada en los almacenes	4	4	16
RP-130	Riesgo-244		Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16
RP-131	Riesgo-253	Caramas de video vigilancia	Fallas internas de los equipos	Protección inapropiada en los almacenes	4	4	16
RP-132	Riesgo-255	Licencia de Antivirus Gdata versión 2017	Crisis Financiera (presupuesto)	Perdida de recursos economicos	4	4	16

RP-133	Riesgo-256	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Virus/ Malware	Passwords débiles	4	4	16
RP-134	Riesgo-257		Virus/ Malware	Password sin modificarse	4	4	16
RP-135	Riesgo-258		Virus/ Malware	Falta de evaluaciones para detectar vulnerabilidades	4	4	16
RP-136	Riesgo-259		Hacking	Passwords débiles	4	4	16
RP-137	Riesgo-260		Hacking	Password sin modificarse	4	4	16
RP-138	Riesgo-261		Hacking	Falta de políticas para el control de acceso	4	4	16
RP-139	Riesgo-262		Hacking	Validación de usuario por perfil (Autenticación Inadecuada)	4	4	16
RP-140	Riesgo-263		Hacking	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
RP-141	Riesgo-264		Hacking	Falta de evaluaciones para detectar vulnerabilidades	4	4	16
RP-142	Riesgo-265		Hacking	No realizar una copia de respaldo (Back - Up)	4	4	16
RP-143	Riesgo-266		Hacking	políticas incompletas para el uso de criptografía	4	4	16
RP-144	Riesgo-267		Hacking	Carencia de copia de respaldo (Back - Up) en la nube	4	4	16
RP-145	Riesgo-268		Hacking	falta de Protección criptográficas	4	4	16
RP-146	Riesgo-269		Hacking	Falta de filtrado de red en dispositivos de usuario final	4	4	16
RP-147	Riesgo-270		Hacking	Falta de Autenticación en las aplicaciones	4	4	16
RP-148	Riesgo-271		Hacking	falta de registros de monitoreo en los perfiles de usuario	4	4	16
RP-149	Riesgo-272		Hacking	No se revisa los privilegios asignados a los usuarios	4	4	16
RP-150	Riesgo-273		Hacking	No realizar pruebas de intrusión	4	4	16
RP-151	Riesgo-274		Fallas de red	Validación de usuario por perfil (Autenticación Inadecuada)	4	4	16
RP-152	Riesgo-275		Fallas de red	Falta de filtrado de red en dispositivos de usuario final	4	4	16
RP-153	Riesgo-276		Fallas de servidores	Validación de usuario por perfil (Autenticación Inadecuada)	4	4	16
RP-154	Riesgo-277		Fallas de servidores	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
RP-155	Riesgo-278		Falla en las aplicaciones	Validación de usuario por perfil (Autenticación Inadecuada)	4	4	16
RP-156	Riesgo-279		Falla en las aplicaciones	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
RP-157	Riesgo-280		Falla en las aplicaciones	Carencia de validación de datos procesados	4	4	16
RP-158	Riesgo-281		Falla en las aplicaciones	Falta de politicas para el desarrollo seguro	4	4	16
RP-159	Riesgo-282		Falla en las aplicaciones	Falta de filtrado de red en dispositivos de usuario final	4	4	16
RP-160	Riesgo-283		Falla en las aplicaciones	Falta de Autenticación en las aplicaciones	4	4	16
RP-161	Riesgo-284		Falla en las aplicaciones	falta de registros de monitoreo en los perfiles de usuario	4	4	16
RP-162	Riesgo-285		Falla en las aplicaciones	No se revisa los privilegios asignados a los usuarios	4	4	16
RP-163	Riesgo-286		Falla en las aplicaciones	control de cambio inadecuado	4	4	16
RP-164	Riesgo-287		Falla en las aplicaciones	No realizar pruebas de intrusión	4	4	16
RP-165	Riesgo-288		Incumplimiento en el mantenimiento del sistema de información	Carencia de ensayos de software	4	4	16
RP-166	Riesgo-289		Copia fraudulenta del software	Documentación pobre de software	4	4	16
RP-167	Riesgo-309	Disco duro externo wster digital	Virus/ Malware	Falta de procedimiento de prevención frente a un ataque de software malicioso	4	5	20
RP-168	Riesgo-310		Fallas internas de los equipos	Inadecuada protección al equipo	4	4	16
RP-169	Riesgo-312	Equipo de control de asistencia	falsificación de derechos	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
RP-170	Riesgo-316	Accesorios de Informatica - Switches	Fallas internas de los equipos	Inadecuada protección al equipo	4	4	16
RP-171	Riesgo-319	Switch dlink DES 1210 19" para telefonía	Fallas internas de los equipos	Inadeacuada protección al equipo	4	4	16
RP-172	Riesgo-321		Falla en telefonía	Falta de protección en las redes públicas	4	4	16
RP-173	Riesgo-326	Software control de asistencia Premium	Fallas de servidores	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
RP-174	Riesgo-327		Fallas en las aplicaciones	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
RP-175	Riesgo-328		Falla en la base de datos	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16
RP-176	Riesgo-337	Helpdesk (Servicio de soporte y mantenimiento)	Uso no autorizado del equipo	Falta de políticas para el mantenimiento de los dispositivos	4	4	16
RP-177	Riesgo-345	Estabilizador - UPS TRIPP SmathOnLine servidores	Falla en el suministro de agua o de aire acondicionado	Inadecuada protección en los equipos	4	4	16
RP-178	Riesgo-347	Grupo Electrógeno - Transformador de aislamiento de 12 KVA flash power	Falla en el suministro de agua o de aire acondicionado	Iandecuada protección en los equipos	4	4	16

Anexo 19: Estrategias de Riesgo y Controles definidos

Aspecto de analisis				Plan de tratamiento de riesgo con la norma ISO 27002:2013				Código de análisis		2017PTR01	
Empresa de estudio				Unión Peruana del Norte				Empresa a Cargo		System Auditors	
Area de estudio				Área de tecnología de información (TI)				Encargado		Samuel Gavidia Mamani Luis Daniel Torres Torres	
Codigo plan	Código Riesgo	Activo	Amenaza	Vulnerabilidad	Probabilidad Ocurrencia (PO)	Impacto	Valor	Tipo de seguridad (S.F y S.I)	Dominio de la Iso 27002	Estrategia del Riesgo (Transferir, Evadir, Reducir y Aceptar)	Controles del dominio de la iso 27002
PTR-01	Riesgo-51	Red y conectividad	Espionaje remoto	Carencia de mecanismos que aseguren el envio y recepción de mensajes	4	5	20	SL		Aceptar	
PTR-02	Riesgo-01	Base de Datos	Pérdida de datos	No eliminar el acceso a los sistemas de información, al personal que no labora	4	5	20	SL	9	Reducir	9.2.2
PTR-03	Riesgo-02	Base de Datos	Pérdida de datos	Falta de evaluaciones para detectar vulnerabilidades	4	5	20	SL	12	Reducir	12.6.1
PTR-04	Riesgo-03	Base de Datos	Pérdida de datos	Password sin modificarse	4	5	20	SL	9	Reducir	9.4.3
PTR-05	Riesgo-05	Copia de respaldo de base de datos	Virus/ Malware	No realizar una copia de respaldo (Back - Up)	4	5	20	SL	12	Reducir	12.3.1
PTR-06	Riesgo-06	Copia de respaldo de base de datos	Hacking	No realizar una copia de respaldo (Back - Up)	4	5	20	SL	12	Reducir	12.3.1
PTR-07	Riesgo-07	Copia de respaldo de base de datos	Hacking	Carencia de copia de respaldo (Back - Up) en la nube	4	5	20	SL	12	Reducir	12.3.1
PTR-08	Riesgo-10	Copia de respaldo de Software	Virus/ Malware	No realizar una copia de respaldo (Back - Up)	4	5	20	SL	12	Reducir	12.3.1
PTR-09	Riesgo-11	Copia de respaldo de Software	Hacking	Carencia de copia de respaldo (Back - Up) en la nube	4	5	20	SL	12	Reducir	12.3.1
PTR-10	Riesgo-12	Copia de respaldo de Software	Hacking	No realizar una copia de respaldo (Back - Up)	4	5	20	SL	12	Reducir	12.3.1
PTR-11	Riesgo-15	CPU - Servidor de correo	Hacking	Falta de políticas para el control de acceso	4	5	20	SL	9	Reducir	9.1.1
PTR-12	Riesgo-16	CPU - Servidor de correo	Hacking	No realizar pruebas de intrusión	4	5	20	SL		Aceptar	
PTR-13	Riesgo-17	CPU - Servidor de correo	Hacking	Carencia de mecanismos que aseguren el envio y recepción de mensajes	4	5	20	SL		Aceptar	
PTR-14	Riesgo-18	CPU - Servidor de correo	Hacking	Validación de usuario por perfil (Autenticación Inadecuada)	4	5	20	SL	9	Reducir	9.4.2
PTR-15	Riesgo-19	CPU - Servidor de correo	Fallas de red	No realizar pruebas de intrusión	4	5	20	SL		Aceptar	
PTR-16	Riesgo-20	CPU - Servidor de correo	Fallas de red	Carencia de mecanismos que aseguren el envio y recepción de mensajes	4	5	20	SL		Aceptar	
PTR-17	Riesgo-34	CPU - Centro de datos	Hacking	No realizar pruebas de intrusión	4	5	20	SL		Aceptar	
PTR-18	Riesgo-35	CPU - Centro de datos	Hacking	Falta de políticas para el control de acceso logico	4	5	20	SL	9	Reducir	9.1.1
PTR-19	Riesgo-36	CPU - Centro de datos	Hacking	Validación de usuario por perfil (Autenticación Inadecuada)	4	5	20	SL	9	Reducir	9.4.2
PTR-20	Riesgo-52	Red y conectividad	Fallas de red	Falta de Protección en las redes publicas	4	5	20	SL		Aceptar	
PTR-21	Riesgo-53	Red y conectividad	Fallas de red	No realizar pruebas de intrusión	4	5	20	SL		Aceptar	
PTR-22	Riesgo-54	Red y conectividad	Espionaje remoto	Falta de políticas para el control de acceso	4	5	20	SL	9	Reducir	9.1.1
PTR-23	Riesgo-55	Red y conectividad	Espionaje remoto	Falta de Protección en las redes publicas	4	5	20	SL		Aceptar	
PTR-24	Riesgo-56	Red y conectividad	Espionaje remoto	No realizar pruebas de intrusión	4	5	20	SL		Aceptar	
PTR-25	Riesgo-57	Red y conectividad	Virus/ Malware	Falta de Protección en las redes publicas	4	5	20	SL		Aceptar	
PTR-26	Riesgo-58	Red y conectividad	Virus/ Malware	Información no encriptada	4	5	20	SL		Transferir	
PTR-27	Riesgo-59	Red y conectividad	Virus/ Malware	políticas incompletas para el uso de criptografía	4	5	20	SL		Transferir	
PTR-28	Riesgo-309	Disco duro externo wster digital	Virus/ Malware	Falta de procedimiento de prevención frente a un ataque de software malicioso	4	5	20	SL	12	Reducir	12.2.1
PTR-29	Riesgo-08	Copia de respaldo de base de datos	Falla en la base de datos	No realizar una copia de respaldo (Back - Up)	4	5	20	SL	12	Reducir	12.3.1
PTR-30	Riesgo-09	Copia de respaldo de base de datos	Falla en la base de datos	Carencia de copia de respaldo (Back - Up) en la nube	4	5	20	SL	12	Reducir	12.3.1
PTR-31	Riesgo-82	Servidores Dell Poweredge R630 - Base de Datos	Perdida de Datos	Password sin modificarse	4	5	20	SL	9	Reducir	9.4.3
PTR-32	Riesgo-83	Servidores Dell Poweredge R630 - Base de Datos	Perdida de Datos	Carencia de validación de datos procesados	4	5	20	SL	12	Reducir	12.7.1
PTR-33	Riesgo-97	Servidores Dell Poweredge R630 - Archivos	Perdida de Datos	No tener cifrada la información almacenada en la organización	4	5	20	SL		Transferir	
PTR-34	Riesgo-98	Servidores Dell Poweredge R630 - Archivos	Espionaje remoto	No tener cifrada la información almacenada en la organización	4	5	20	SL		Transferir	
PTR-35	Riesgo-112	Servidores Dell Poweredge R230 - Firewall	Fallas de red	No realizar pruebas de intrusión	4	5	20	SL		Aceptar	
PTR-36	Riesgo-113	Servidores Dell Poweredge R230 - Firewall	Fallas de red	Falta de Protección en las redes publicas	4	5	20	SL		Aceptar	
PTR-37	Riesgo-114	Servidores Dell Poweredge R230 - Firewall	Hacking	Falta de Protecćon en las redes publicas	4	5	20	SL		Aceptar	
PTR-38	Riesgo-115	Servidores Dell Poweredge R230 - Firewall	Hacking	Falta de politicas para el control de acceso	4	5	20	SL	9	Reducir	9.1.1

PTR-39	Riesgo-119	Switches Dell networking N3048P (Corp - Principal)	Hacking	No realizar pruebas de intrusión	4	5	20	SL		Aceptar	
PTR-40	Riesgo-120	Switches Dell networking N3048P (Corp - Principal)	Hacking	Falta de protección en las redes públicas	4	5	20	SL		Aceptar	
PTR-41	Riesgo-123	Switches Dell networking N3048P (Corp - Principal)	Espionaje remoto	No realizar pruebas de intrusión	4	5	20	SL		Aceptar	
PTR-42	Riesgo-124	Switches Dell networking N3048P (Corp - Principal)	Espionaje remoto	Falta de protección en las redes públicas	4	5	20	SL		Aceptar	
PTR-43	Riesgo-125	Switches Dell networking N3048P (Corp - Principal)	Fallas de red	Falta de protección en las redes públicas	4	5	20	SL		Aceptar	
PTR-44	Riesgo-222	Servidores Dell Poweredge R230 - DHCP(Navegación)	Espionaje remoto	Falta de pruebas de intrusion	4	5	20	SL		Aceptar	
PTR-45	Riesgo-223	Servidores Dell Poweredge R230 - DHCP(Navegación)	Espionaje remoto	Falta de filtrado de red en dispositivos de usuario final	4	5	20	SL		Aceptar	
PTR-46	Riesgo-224	Servidores Dell Poweredge R230 - DHCP(Navegación)	Fallas de red	Falta de pruebas de intrusion	4	5	20	SL		Aceptar	
PTR-47	Riesgo-238	Servidores Dell Poweredge R230 - WEB	Hacking	Falta de protección en las redes públicas	4	5	20	SL		Aceptar	
PTR-48	Riesgo-239	Servidores Dell Poweredge R230 - WEB	Espionaje remoto	Falta de filtrado de red en dispositivos de usuario final	4	5	20	SL		Aceptar	
PTR-49	Riesgo-21	CPU - Servidor de correo	Fallas de servidores	Inadecuada protección al equipo	4	4	16	SF	11	Reducir	11.2.1
PTR-50	Riesgo-22	CPU - Servidor de correo	Fallas de servidores	Protección inapropiada en los almacenes	4	4	16	SF		Evadir	
PTR-51	Riesgo-23	CPU - Servidor de correo	Fallas de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16	SF	11	Reducir	11.1.2
PTR-52	Riesgo-24	CPU - Servidor de correo	Falla en el suministro de agua o de aire acondicionado	Protección inapropiada en los almacenes	4	4	16	SF		Transferir	
PTR-53	Riesgo-37	CPU - Centro de datos	Fallas de red	No realizar pruebas de intrusión	4	4	16	SL		Aceptar	
PTR-54	Riesgo-38	CPU - Centro de datos	Fallas de servidores	Protección inapropiada en los almacenes	4	4	16	SF		Evadir	
PTR-55	Riesgo-39	CPU - Centro de datos	Fallas de servidores	Inadecuada protección al equipo	4	4	16	SF	11	Reducir	11.2.1
PTR-56	Riesgo-40	CPU - Centro de datos	Fallas de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16	SF	11	Reducir	11.1.2
PTR-57	Riesgo-41	CPU - Centro de datos	Falla en el suministro de agua o de aire acondicionado	Protección inapropiada en los almacenes	4	4	16	SF		Transferir	
PTR-58	Riesgo-60	Red y conectividad	Fallas de red	Falta de filtrado de red en dispositivos de usuario final	4	4	16	SL		Aceptar	
PTR-59	Riesgo-61	Red y conectividad	Espionaje remoto	Falta de filtrado de red en dispositivos de usuario final	4	4	16	SL		Aceptar	
PTR-60	Riesgo-62	Red y conectividad	Espionaje remoto	Información no encriptada	4	4	16	SL		Transferir	
PTR-61	Riesgo-63	Red y conectividad	Espionaje remoto	políticas incompletas para el uso de criptografía	4	4	16	SL		Transferir	
PTR-62	Riesgo-126	Jefe de TI	falsificación de derechos	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16	SL	9	Reducir	9.2.2
PTR-63	Riesgo-127	Jefe de TI	falsificación de derechos	No tener una identificación visible en la organización	4	4	16	SF	11	Reducir	11.1.2
PTR-64	Riesgo-128	Jefe de TI	falsificación de derechos	No se revisa los privilegios asignados a los usuarios	4	4	16	SL	9	Reducir	9.2.5
PTR-65	Riesgo-129	Jefe de TI	Pérdida de personal clave	Incumplimiento del contrato	4	4	16	SF		Evadir	
PTR-66	Riesgo-130	Analista de Sistemas académicos y Gerenciales	falsificación de derechos	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16	SL	9	Reducir	9.2.2
PTR-67	Riesgo-131	Analista de Sistemas académicos y Gerenciales	falsificación de derechos	No tener una identificación visible en la organización	4	4	16	SF	11	Reducir	11.1.2
PTR-68	Riesgo-132	Analista de Sistemas académicos y Gerenciales	falsificación de derechos	No se revisa los privilegios asignados a los usuarios	4	4	16	SL	9	Reducir	9.2.5
PTR-69	Riesgo-133	Servidor Pack cable HP Proliant DL 160 GB Intel	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16	SF		Transferir	

PTR-70	Riesgo-134	Servidor Pack cable HP Proliant DL 160 GB Intel	Falla de servidores	Falta de políticas para el mantenimiento de los dispositivos	4	4	16	SF	11	Reducir	11.2.4
PTR-71	Riesgo-135	Servidor Pack cable HP Proliant DL 160 GB Intel	Falla de servidores	Inadecuada protección al equipo	4	4	16	SF	11	Reducir	11.2.1
PTR-72	Riesgo-136	Servidor Pack cable HP Proliant DL 160 GB Intel	Falla de servidores	Protección inapropiada en los almacenes	4	4	16	SF		Evadir	
PTR-73	Riesgo-137	Servidor Pack cable HP Proliant DL 160 GB Intel	Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16	SF	11	Reducir	11.1.2
PTR-74	Riesgo-146	Servidor HP Proliant DL 120GB 6 Intel XEON 343	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16	SF		Transferir	
PTR-75	Riesgo-147	Servidor HP Proliant DL 120GB 6 Intel XEON 344	Falla de servidores	Falta de políticas para el mantenimiento de los dispositivos	4	4	16	SF	11	Reducir	11.2.4
PTR-76	Riesgo-148	Servidor HP Proliant DL 120GB 6 Intel XEON 345	Falla de servidores	Inadecuada protección al equipo	4	4	16	SF	11	Reducir	11.2.1
PTR-77	Riesgo-149	Servidor HP Proliant DL 120GB 6 Intel XEON 346	Falla de servidores	Protección inapropiada en los almacenes	4	4	16	SF		Evadir	
PTR-78	Riesgo-150	Servidor HP Proliant DL 120GB 6 Intel XEON 347	Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16	SF	11	Reducir	11.1.2
PTR-79	Riesgo-159	CPU - Servidor central telefónica	Falla en telefonía	Falta de Protección en las redes publicas	4	4	16	SL		Aceptar	
PTR-80	Riesgo-160	CPU - Servidor central telefónica	Fallas de red	Falta de Protección en las redes publicas	4	4	16	SL		Aceptar	
PTR-81	Riesgo-161	CPU - Servidor central telefónica	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16	SF		Transferir	
PTR-82	Riesgo-162	CPU - Servidor central telefónica	Falla de servidores	Falta de políticas para el mantenimiento de los dispositivos	4	4	16	SF	11	Reducir	11.2.4
PTR-83	Riesgo-163	CPU - Servidor central telefónica	Falla de servidores	Inadecuada protección al equipo	4	4	16	SF	11	Reducir	11.2.1
PTR-84	Riesgo-164	CPU - Servidor central telefónica	Falla de servidores	Protección inapropiada en los almacenes	4	4	16	SF		Evadir	
PTR-85	Riesgo-165	CPU - Servidor central telefónica	Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16	SF	11	Reducir	11.1.2
PTR-86	Riesgo-174	Laptop Dell Tes. Asistente oper.	Fallas internas de los equipos	Falta de políticas para el mantenimiento de los dispositivos	4	4	16	SF	11	Reducir	11.2.4
PTR-87	Riesgo-175	Laptop Dell Tes. Asistente oper.	Fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16	SF	11	Reducir	11.1.2
PTR-88	Riesgo-176	Laptop Dell Tes. Asistente oper.	Virus/ Malware	Falta de procedimiento de prevención frente a un ataque de software malicioso	4	4	16	SL	12	Reducir	12.2.1
PTR-89	Riesgo-181	Notebook DELL serie 3000 14" i5	Fallas internas de los equipos	Falta de políticas para el mantenimiento de los dispositivos	4	4	16	SF	11	Reducir	11.2.4
PTR-90	Riesgo-182	Notebook DELL serie 3000 14" i6	Fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16	SF	11	Reducir	11.1.2
PTR-91	Riesgo-183	Notebook DELL serie 3000 14" i7	Virus/ Malware	Falta de procedimiento de prevención frente a un ataque de software malicioso	4	4	16	SL	12	Reducir	12.2.1
PTR-92	Riesgo-188	Laptop Mac Book	fallas internas de los equipos	Falta de políticas para el mantenimiento de los dispositivos	4	4	16	SF	11	Reducir	11.2.4
PTR-93	Riesgo-189	Laptop Mac Book	fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16	SF	11	Reducir	11.1.2
PTR-94	Riesgo-190	Laptop Mac Book	Virus/ Malware	Falta de procedimiento de prevención frente a un ataque de software malicioso	4	4	16	SL	12	Reducir	12.2.1
PTR-95	Riesgo-195	Laptop Latitude 5470 - i5 8 GB 1 TB HD - 126 VZF2	Fallas internas de los equipos	Falta de políticas para el mantenimiento de los dispositivos	4	4	16	SF	11	Reducir	11.2.4
PTR-96	Riesgo-196	Laptop Latitude 5470 - i5 8 GB 1 TB HD - 126 VZF3	Fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16	SF	11	Reducir	11.1.2
PTR-97	Riesgo-197	Laptop Latitude 5470 - i5 8 GB 1 TB HD - 126 VZF4	Virus/ Malware	Falta de procedimiento de prevención frente a un ataque de software malicioso	4	4	16	SL	12	Reducir	12.2.1
PTR-98	Riesgo-202	2 Laptop Latitude E5470 - I7 16 GB 1 TB FHD	fallas internas de los equipos	Falta de políticas para el mantenimiento de los dispositivos	4	4	16	SF	11	Reducir	11.2.4
PTR-99	Riesgo-203	2 Laptop Latitude E5470 - I7 16 GB 1 TB FHD	fallas internas de los equipos	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16	SF	11	Reducir	11.1.2
PTR-100	Riesgo-204	2 Laptop Latitude E5470 - I7 16 GB 1 TB FHD	Virus/ Malware	Falta de procedimiento de prevención frente a un ataque de software malicioso	4	4	16	SL	12	Reducir	12.2.1

PTR-101	Riesgo-69	Servidores Dell Poweredge R630 - Base de Datos	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16	SF		Transferir	
PTR-102	Riesgo-70	Servidores Dell Poweredge R630 - Base de Datos	Falla de servidores	faltas de políticas para el mantenimiento de los dispositivos	4	4	16	SF	11	Reducir	11.2.4
PTR-103	Riesgo-71	Servidores Dell Poweredge R630 - Base de Datos	Falla de servidores	Inadecuada protección al equipo	4	4	16	SF	11	Reducir	11.2.1
PTR-104	Riesgo-72	Servidores Dell Poweredge R630 - Base de Datos	Falla de servidores	Protección inapropiada en los almacenes	4	4	16	SF		Evadir	
PTR-105	Riesgo-73	Servidores Dell Poweredge R630 - Base de Datos	Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16	SF	11	Reducir	11.1.2
PTR-106	Riesgo-84	Servidores Dell Poweredge R630 - Archivos	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16	SF		Transferir	
PTR-107	Riesgo-85	Servidores Dell Poweredge R630 - Archivos	Falla de servidores	faltas de políticas para el mantenimiento de los dispositivos	4	4	16	SF	11	Reducir	11.2.4
PTR-108	Riesgo-86	Servidores Dell Poweredge R630 - Archivos	Falla de servidores	Inadecuada protección al equipo	4	4	16	SF	11	Reducir	11.2.1
PTR-109	Riesgo-87	Servidores Dell Poweredge R630 - Archivos	Falla de servidores	Protección inapropiada en los almacenes	4	4	16	SF		Evadir	
PTR-110	Riesgo-88	Servidores Dell Poweredge R630 - Archivos	Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16	SF	11	Reducir	11.1.2
PTR-111	Riesgo-99	Servidores Dell Poweredge R230 - Firewall	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16	SF		Transferir	
PTR-112	Riesgo-100	Servidores Dell Poweredge R230 - Firewall	Falla de servidores	faltas de políticas para el mantenimiento de los dispositivos	4	4	16	SF	11	Reducir	11.2.4
PTR-113	Riesgo-101	Servidores Dell Poweredge R230 - Firewall	Falla de servidores	Inadecuada protección al equipo	4	4	16	SF	11	Reducir	11.2.1
PTR-114	Riesgo-102	Servidores Dell Poweredge R230 - Firewall	Falla de servidores	Protección inapropiada en los almacenes	4	4	16	SF		Evadir	
PTR-115	Riesgo-103	Servidores Dell Poweredge R230 - Firewall	Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16	SF	11	Reducir	11.1.2
PTR-116	Riesgo-209	Servidores Dell Poweredge R230 - DHCP(Navegación)	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16	SF		Transferir	
PTR-117	Riesgo-210	Servidores Dell Poweredge R230 - DHCP(Navegación)	Falla de servidores	faltas de políticas para el mantenimiento de los dispositivos	4	4	16	SF	11	Reducir	11.2.4
PTR-118	Riesgo-211	Servidores Dell Poweredge R230 - DHCP(Navegación)	Falla de servidores	Inadecuada protección al equipo	4	4	16	SF	11	Reducir	11.2.1
PTR-119	Riesgo-212	Servidores Dell Poweredge R230 - DHCP(Navegación)	Falla de servidores	Protección inapropiada en los almacenes	4	4	16	SF		Evadir	
PTR-120	Riesgo-213	Servidores Dell Poweredge R230 - DHCP(Navegación)	Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16	SF	11	Reducir	11.1.2
PTR-121	Riesgo-225	Servidores Dell Poweredge R230 - WEB	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16	SF		Transferir	
PTR-122	Riesgo-226	Servidores Dell Poweredge R230 - WEB	Falla de servidores	Falta de políticas para el mantenimiento de los dispositivos	4	4	16	SF	11	Reducir	11.2.4
PTR-123	Riesgo-227	Servidores Dell Poweredge R230 - WEB	Falla de servidores	Inadecuada protección al equipo	4	4	16	SF	11	Reducir	11.2.1
PTR-124	Riesgo-228	Servidores Dell Poweredge R230 - WEB	Falla de servidores	Protección inapropiada en los almacenes	4	4	16	SF		Evadir	
PTR-125	Riesgo-229	Servidores Dell Poweredge R230 - WEB	Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16	SF	11	Reducir	11.1.2
PTR-126	Riesgo-253	Caramas de video vigilancia	Fallas internas de los equipos	Protección inapropiada en los almacenes	4	4	16	SF		Evadir	
PTR-127	Riesgo-240	Servidor Redundante - Dell poweredge Intel xeon y DELL power Intel	Falla en el sistema de suministros de agua o aire acondicionado	Protección inapropiada en los almacenes	4	4	16	SF		Transferir	
PTR-128	Riesgo-241	Servidor Redundante - Dell poweredge Intel xeon y DELL power Intel	Falla de servidores	faltas de políticas para el mantenimiento de los dispositivos	4	4	16	SF	11	Reducir	11.2.4
PTR-129	Riesgo-242	Servidor Redundante - Dell poweredge Intel xeon y DELL power Intel	Falla de servidores	Inadecuada protección al equipo	4	4	16	SF	11	Reducir	11.2.1
PTR-130	Riesgo-243	Servidor Redundante - Dell poweredge Intel xeon y DELL power Intel	Falla de servidores	Protección inapropiada en los almacenes	4	4	16	SF		Evadir	
PTR-131	Riesgo-244	Servidor Redundante - Dell poweredge Intel xeon y DELL power Intel	Falla de servidores	Falta de controles de acceso físico a las áreas de la organización para la seguridad de la información.	4	4	16	SF	11	Reducir	11.1.2
PTR-132	Riesgo-255	Licencia de Antivirus Gdata versión 2017	Crisis Financiera (presupuesto)	Falta de recursos económicos	4	4	16	SF		Aceptar	

PTR-133	Riesgo-256	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Virus/ Malware	Passwords débiles	4	4	16	SL	9	Reducir	9.4.3
PTR-134	Riesgo-257	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Virus/ Malware	Password sin modificarse	4	4	16	SL	9	Reducir	9.4.3
PTR-135	Riesgo-258	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Virus/ Malware	Falta de evaluaciones para detectar vulnerabilidades	4	4	16	SL	12	Reducir	12.6.1
PTR-136	Riesgo-259	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Hacking	Passwords débiles	4	4	16	SL	9	Reducir	9.4.3
PTR-137	Riesgo-260	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Hacking	password sin modificarse	4	4	16	SL	9	Reducir	9.4.3
PTR-138	Riesgo-261	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Hacking	Falta de políticas para el control de acceso	4	4	16	SL	9	Reducir	9.1.1
PTR-139	Riesgo-262	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Hacking	Validación de usuario por perfil (Autenticación Inadecuada)	4	4	16	SL	9	Reducir	9.4.2
PTR-140	Riesgo-263	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Hacking	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16	SL	9	Reducir	9.2.2
PTR-141	Riesgo-264	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Hacking	Falta de evaluaciones para detectar vulnerabilidades	4	4	16	SL	12	Reducir	12.6.1
PTR-142	Riesgo-265	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Hacking	No realizar una copia de respaldo (Back - Up)	4	4	16	SL	12	Reducir	12.3.1
PTR-143	Riesgo-266	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Hacking	políticas incompletas para el uso de criptografía	4	4	16	SL		Transferir	
PTR-144	Riesgo-267	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Hacking	Carencia de copia de respaldo (Back - Up) en la nube	4	4	16	SL	12	Reducir	12.3.1
PTR-145	Riesgo-268	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Hacking	falta de Protección criptográficas	4	4	16	SL		Transferir	
PTR-146	Riesgo-269	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Hacking	Falta de filtrado de red en dispositivos de usuario final	4	4	16	SL		Aceptar	
PTR-147	Riesgo-270	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Hacking	Falta de Autenticación en las aplicaciones	4	4	16	SL	9	Reducir	9.4.2
PTR-148	Riesgo-271	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Hacking	falta de registros de monitoreo en los perfiles de usuario	4	4	16	SL	9	Reducir	9.2.5
PTR-149	Riesgo-272	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Hacking	No se revisa los privilegios asignados a los usuarios	4	4	16	SL	9	Reducir	9.2.5
PTR-150	Riesgo-273	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Hacking	No realizar pruebas de intrusión	4	4	16	SL		Aceptar	
PTR-151	Riesgo-274	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Fallas de red	Validación de usuario por perfil (Autenticación Inadecuada)	4	4	16	SL	9	Reducir	9.4.2
PTR-152	Riesgo-275	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Fallas de red	Falta de filtrado de red en dispositivos de usuario final	4	4	16	SL		Aceptar	
PTR-153	Riesgo-276	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Fallas de servidores	Validación de usuario por perfil (Autenticación Inadecuada)	4	4	16	SL	9	Reducir	9.4.2
PTR-154	Riesgo-277	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Fallas de servidores	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16	SL	9	Reducir	9.2.2
PTR-155	Riesgo-278	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Falla en las aplicaciones	Validación de usuario por perfil (Autenticación Inadecuada)	4	4	16	SL	9	Reducir	9.4.2
PTR-156	Riesgo-279	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Falla en las aplicaciones	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16	SL	9	Reducir	9.2.2
PTR-157	Riesgo-280	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Falla en las aplicaciones	Carencia de validación de datos procesados	4	4	16	SL	12	Reducir	12.7.1
PTR-158	Riesgo-281	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Falla en las aplicaciones	Falta de politicas para el desarrollo seguro	4	4	16	SL	14	Reducir	14.2.1
PTR-159	Riesgo-282	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Falla en las aplicaciones	Falta de filtrado de red en dispositivos de usuario final	4	4	16	SL		Aceptar	

PTR-160	Riesgo-283	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Falla en las aplicaciones	Falta de Autenticación en las aplicaciones	4	4	16	SL	9	Reducir	9.4.2
PTR-161	Riesgo-284	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Falla en las aplicaciones	falta de registros de monitoreo en los perfiles de usuario	4	4	16	SL	9	Reducir	9.2.5
PTR-162	Riesgo-285	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Falla en las aplicaciones	No se revisa los privilegios asignados a los usuarios	4	4	16	SL	9	Reducir	9.2.5
PTR-163	Riesgo-286	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Falla en las aplicaciones	control de cambio inadecuado	4	4	16	SL	14	Reducir	14.2.2
PTR-164	Riesgo-287	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Falla en las aplicaciones	No realizar pruebas de intrusión	4	4	16	SL		Aceptar	
PTR-165	Riesgo-288	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Incumplimiento en el mantenimiento del sistema de información	Carencia de ensayos de software	4	4	16	SL	14	Reducir	14.2.8
PTR-166	Riesgo-289	Sistema DSA, Gerencial y Academico - Unión Peruana del Norte(UPN)	Copia fraudulenta del software	Documentación pobre de software	4	4	16	SL	14	Reducir	14.2.2
PTR-167	Riesgo-310	Disco duro externo wster digital	Fallas internas de los equipos	Inadecuada protección al equipo	4	4	16	SF	11	Reducir	11.2.1
PTR-168	Riesgo-312	Equipo de control de asistencia	falsificación de derechos	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16	SL	9	Reducir	9.2.2
PTR-169	Riesgo-316	Accesorios de Informatica - Switches	Fallas internas de los equipos	Inadecuada protección al equipo	4	4	16	SF	11	Reducir	11.2.1
PTR-170	Riesgo-319	Switch dlink DES 1210 19" para telefonía	Fallas internas de los equipos	Inadecuada protección al equipo	4	4	16	SF	11	Reducir	11.2.1
PTR-171	Riesgo-321	Switch dlink DES 1210 19" para telefonía	Falla en telefonía	Falta de protección en las redes públicas	4	4	16	SL		Aceptar	
PTR-172	Riesgo-117	Switches Dell networking N3048P (Corp - Principal)	Fallas internas de los equipos	Inadecuada protección al equipo	4	4	16	SF	11	Reducir	11.2.1
PTR-173	Riesgo-326	Software control de asistencia Premium	Fallas de servidores	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16	SL	9	Reducir	9.2.2
PTR-174	Riesgo-327	Software control de asistencia Premium	Fallas en las aplicaciones	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16	SL	9	Reducir	9.2.2
PTR-175	Riesgo-328	Software control de asistencia Premium	Falla en la base de datos	No eliminar el acceso a los sistemas de información, al personal que no labora	4	4	16	SL	9	Reducir	9.2.2
PTR-176	Riesgo-337	Helpdesk (Servicio de soporte y mantenimiento)	Uso no autorizado del equipo	Falta de políticas para el mantenimiento de los dispositivos	4	4	16	SF	11	Reducir	11.2.4
PTR-177	Riesgo-345	Estabilizador - UPS TRIPP SmathOnLine servidores	Falla en el suministro de agua o de aire acondicionado	Inadecuada protección en los equipos	4	4	16	SF		Transferir	
PTR-178	Riesgo-347	Grupo Electrógeno - Transformador de aislamiento de 12 KVA flash power	Falla en el suministro de agua o de aire acondicionado	Inadecuada protección en los equipos	4	4	16	SF		Transferir	

Anexo 20: Documento relacionado a la estrategia de riesgo Transferir, en conjunto con las políticas de criptografía

ESTRATEGIA DE RIESGO TRANSFERIR -

Manual de Políticas de Criptografía

Lugar:

Área de TI

Versión de Documento:

Primera Versión

2017

1. **Introducción**

La implementación de controles de la norma ISO/IEC 27002 permite cumplir con los servicios de seguridad lógica y física, entre ellos la Criptografía que genera el área de TI dentro de la organización.
Al tener la información cifrada puede, se genera que la información este vulnerable a cualquier tipo de amenaza, como por ejemplo hacking de la información y las fallas en los equipos tecnológicos, estas políticas ayuda a dar soporte y un mejor control para la transmisión y recepción de los mensajes en los sistemas de información.

2. **Objetivo**

El área de TI, es el responsable de los sistemas de información, servidores y la red y conectividad, que maneja actualmente en la organización, ellos deben proteger la integridad, confidencialidad y disponibilidad de la información, salvaguardando a través de llaves y/o claves criptográficas que protejan la información, ante cualquier evento de amenaza.

3. **Alcance**

Este documento estará alineado con las políticas de seguridad de la información general, además detalla las restricciones de acceso lógico para los sistemas de información.

La política se destina a todos los accesos locales que contenga el área de TI de la Unión Peruana del Norte, teniendo como destino a todos los trabajadores

4. **Estrategia de Riesgo establecida**

La estrategia establecida en este documento es Transferir, que requiere que las acciones escritas, analizadas e implementadas tenga la certificación para desarrollar claves o llaves criptográficas.
Este proceso requiere de desarrolladores capacitados y certificados que promuevan la seguridad encriptado en la información, generando que el área de TI pueda cumplir con los controles requeridos por la norma.
El área de TI supervisa y monitorea la implementación de llaves y/o claves criptográficas, permitiendo la eficacia de ello, logrando cumplir con la seguridad de la Confidencialidad, Integridad y Disponibilidad
El área tiene en cuenta que a pesar de que se implementó la mejora de estos controles, puede que aun ocasione alguna amenaza, a ello se le conoce como riesgos residuales, que se manifiesta cuando se redujo el riesgo en cierto periodo de tiempo y luego de ese periodo vuelve a surgir tales riesgos o más riesgos que perjudiquen la información de la Unión Peruana del Norte.
El costo o presupuesto que se estimó en la estrategia de riesgo Aceptar cubre en gran parte con lo que se requiere en este apartado, del cual sería muy beneficioso para el área de TI poder contar con ello, esto con el fin de tener una seguridad robusta y segura en todas sus dimensiones.

5. **Política de Criptografía**

El área de TI supervisa y monitorea que los desarrolladores capacitados y certificados en la encriptación, constaten que la información clasificada dentro de la organización se encuentre cifrada al momento de almacenarse o transmitirse para cualquier medio perteneciente a la Unión Peruana del Norte.

5.1. Política para el debido manejo de la información en la Red y Conectividad, Sistemas de Información (Sistemas UPN y DSA) y Servidores

- ✧ El área de TI supervisa y monitorea que los desarrolladores capacitados y certificados en la encriptación, cifren la información según su clasificación para el transito seguro en la red (Red y Conectividad), con la consigna de proteger la integridad y confidencialidad de la Unión Peruana del Norte.

- ✧ Los desarrolladores capacitados y certificados en la encriptación, supervisan que cada sistema información (Sistemas DSA y UPN) tenga los mecanismos adecuados para el cifrado.
- ✧ El área de TI supervisa y monitorea que los desarrolladores capacitados y certificados en la encriptación, cifren la información clasificada y almacenada, que cercioré la confiabilidad de los medios de almacenamiento (Sistemas UPN y DSA, Servidores).
- ✧ El área de TI supervisa y monitorea que los desarrolladores capacitados y certificados en la encriptación, implementen el cifrado para salvaguardar la información sensible que se transporta a través de los dispositivos extraíbles o móviles, tomando en cuenta la fortaleza, el tipo y la calidad del algoritmo de cifrado requerido.
- ✧ El área de TI supervisa y monitorea que los desarrolladores capacitados y certificados en la encriptación, cifren la información restringida o reservada y autentiquen la confiabilidad de los sistemas de almacenamiento (Sistemas UPN y DSA) de dicha información.
- ✧ El área de TI supervisa y monitorea que los desarrolladores capacitados y certificados en la encriptación, se cercioren que los controles criptográficos de los sistemas de información desarrollados (Sistemas UPN y DSA) se efectúen de acuerdo a los estándares establecidos por el área de TI.
- ✧ El área de TI supervisa y monitorea que los desarrolladores capacitados y certificados en la encriptación, incluyan los requisitos de gestión de las claves criptográficas durante todo su ciclo de vida abarcando el almacenamiento, generación, recuperación, retirada, distribución y destrucción de las mismas.
- ✧ El área de TI supervisa y monitorea que los desarrolladores capacitados y certificados en la encriptación, generen claves criptográficas para las diferentes aplicaciones.
- ✧ El área de TI supervisa y monitorea que los desarrolladores capacitados y certificados en la encriptación, revoquen las claves, incluyendo como deben desactivarse o revocarse cuando un usuario deja la Unión Peruana del Norte o cuando estas fueron comprometidas, en estos casos las claves son archivadas.

Anexo 21: Documento relacionado a la estrategia de riesgo aceptar, en conjunto con las políticas de Seguridad de las comunicaciones.

ESTRATEGIA DE RIESGO ACEPTAR - Manual de Políticas de Seguridad de las Comunicaciones

UNIÓN PERUANA DEL NORTE

Lugar:

Área de TI

Versión de Documento:

Primera Versión

2017

1. Introducción

La implementación de controles de la norma ISO/IEC 27002 permite cumplir con los servicios de seguridad lógica y física, entre ellos los servicios de seguridad en las comunicaciones dentro de la organización.
La gestión de la seguridad ayuda a garantizar la seguridad de la información en las redes y protección de servicios de los servicios que se encuentran conectados frente a accesos no autorizados.
El establecimiento de estas políticas protege el intercambio de información mediante el uso de todo tipo de recursos de comunicación, además de garantizar la protección en los servicios de comunicación y que redes que se transportan en los equipos y sistemas de información, esto para su eficaz resguardo y aseguramiento de la información.

2. Objetivo

El área de TI, es el responsable de los sistemas de información, servidores y la red y conectividad, que maneja actualmente en la organización, ellos deben proteger la integridad, confidencialidad y disponibilidad de la información, salvaguardando la información por medio de la gestión de seguridad en las comunicaciones, que permiten brindar una protección eficiente en las redes y en los recursos de tratamiento de la información.

3. Alcance

Este documento detalla las acciones a tomarse en cuenta para el debido manejo de la seguridad en las comunicaciones en los sistemas de información.
La política se destina a todos los accesos locales que contenga el área de TI de la Unión Peruana del Norte, teniendo como destino a todos los trabajadores

4. Estrategia de Riesgo establecida

La estrategia establecida en este documento es Aceptar, puesto que el área de TI no cuenta con un presupuesto para poder implementar los controles relacionados con la seguridad en las comunicaciones, además de que el personal no tiene conocimiento amplio en algunos temas relacionados a estos, tales como: el filtrado de red en los dispositivos de usuarios final y la falta y no realización de pruebas de intrusión. Estos son los factores los cuales el área de TI opto por tomar esta estrategia de riesgo.
Se estima un presupuesto de $/.126.851 hasta $/.531.767 para la adquisición de equipos en redes, que ayudan a realizar lo anterior dicho como el filtrado de red, pruebas de intrusión, encriptación, etc. El monto mostrado es un estimado, puesto que de manera específica no es viable obtener precios precisos. Por un lado Cisco, que es un proveedor de estos equipos no vende equipos concisamente a los particulares ni igualmente brinda un listado de precios en su página web, ya que éste vende a través de partners, abarcando y/o incluyendo al proveedor de servicios Telefónica. Por otra parte, Telefónica brinda la posibilidad de comprar o alquilar cada equipo junto con sus líneas que se gestionan a través de un comercial.
Cada cliente puede obtener precios distintos ya que hay que negociar con Telefónica sus propios descuentos. Por lo que los precios que se muestran podrían ser menores a ellos como mayores, esto dependiendo del acuerdo en que lleguen ambas partes.
Los criterios de aceptación se describen en forma de definición de políticas relacionada en las comunicaciones, las cuales ayudaran en un futuro a que el área pueda establecer y manejar de manera eficiente la información que se transmite por medio de las redes.

5. Políticas de seguridad en las comunicaciones

5.1. Políticas de Gestión de la seguridad de las redes

El área de TI certifica el resguardo de la información en los recursos de tratamiento de información y la información en las redes.

5.1.1. Norma de gestión y aseguramiento de las redes de datos

Norma dirigida a: Área de TI

- ✧ El área de TI establece parámetros para proteger la seguridad de la información en las redes y en la protección de servicios de red frente accesos no autorizados.

- El área de TI instaura controles especiales para salvaguardar la integridad y confidencialidad de los datos que pasan por medio de redes públicas y/o inalámbricas.
- El área de TI implanta procedimientos y responsabilidades para la administración de los equipos de red.
- El área de TI efectúa un registro apropiado de eventos y monitorización, para permitir el registro y detección de acciones, que pueda afligir, o ser relevante para la seguridad en la información.
- El área de TI determina los niveles de servicio de red solicitados, y estos son añadidos en los arreglos de servicio de red cuando son contratados externamente.
- El área de TI autentica los sistemas de la red y restringe las conexiones de los sistemas a la red.
- El área de TI custodia todas redes de datos que son segmentadas por dominios, grupos de usuarios y servicios, ubicaciones geográficas u otra caracterización que sea beneficioso para el área.
- El área de TI vale por la confidencialidad de la información del enrutamiento y direccionamiento de las redes de datos de la UPN.
- El área de TI realiza el filtrado de red en los dispositivos de usuarios final para el buen resguardo y/o protección de la información contenidos en los servidores, sistemas de información (Sistemas UPN, Sistema DSA) y en la red y conectividad.
- El área de TI controla el trafico entrante y saliente de la información mediante la red para los dispositivos autorizados de la Unión Peruana de Norte
- El área de TI realiza pruebas de intrusión en los equipos que procesan información tales como: servidores y centro de datos, además del Switch principal de la Organización, incluyendo a esto los sistemas de información (Sistemas UPN, Sistema DSA) y red y conectividad, esto para el buen resguardo de ellos.

5.2. Políticas de Intercambio de Información

El área de TI protege la seguridad en la información que se transfiere en la UPN y con cualquier entidad ajena a ella.

5.2.1. Normas de intercambio de información

Norma dirigida a: Propietarios de los activos de información

- Los propietarios de los activos de información están en la obligación de cerciorarse que el cambio de información de manera digital, únicamente se efectúe, si se hallase acreditada y cumpliendo con las políticas de administración de redes, de acceso lógico y de resguardo de datos confidenciales de la organización, así como del proceso de intercambio de información.
- Los propietarios de los activos de información están en la obligación de evidenciar que el intercambio de información con personas externas a la organización deje un informe del tipo de información intercambiada, el receptor y emisor de la misma, junto con la fecha de entrega y recepción.
- Los propietarios de los activos de información se aseguran que la información de la UPN o demás usuarios que laboran en la organización, son salvaguardadas de publicaciones no autorizada por parte de personas externas a la organización a quienes se les hace llegar esta información, evidenciando la realización de las cláusulas vinculadas en los contratos, los compromisos de confidencialidad e intercambios establecidos.

Norma dirigida a: Todos los usuarios

- Todos los usuarios no manejan el correo electrónico de la organización como un medio para recibir o enviar información relevante para la UPN o para sus beneficiarios.
- No se permite el intercambio de información confidencial y relevante de la organización y sus áreas por vía móvil u otro medio.

Norma dirigida a: Dirección de Tecnología de Información

El director de tecnología de información de la UPN ofrece y garantiza servicios y herramientas de intercambio de información óptimos, igualmente el de acoger medidas como el cifrado de información, que admitan la realización del proceso para el intercambio de información, esto con el fin de salvaguardar dicha información contra modificaciones no autorizadas o divulgación de la información.

Anexo 22: Documento de Plan de Tratamiento de riesgo con la norma ISO/IEC 27002

Plan de Tratamiento de Riesgo con la norma ISO/IEC 27002:

Temas del Plan de Tratamiento de Riesgo:

Evaluaciones del nivel de seguridad de la información – Análisis de riesgo – Propuestas con los controles de la norma ISO/IEC 27002

Área de Investigación:

Área de Tecnologías de la Información (TI)

Empresa:

Unión Peruana del Norte

Autores:

Luis Daniel Torres Torres

Samuel Gavidia Mamani

2017

Resumen Ejecutivo

El plan de tratamiento de riesgo que se presenta en este documento, expone la implementación de los controles de seguridad de la información, los cuales ayudarán a reducir y/o mitigar los riesgos que fueron identificados durante el análisis de riesgo, de tal manera esto ayude a gestionar correctamente la información que la organización administra para sus operaciones.
Este documento muestra el análisis de los activos, vulnerabilidades y amenazas priorizadas de la organización. Además, se desarrolló un análisis de riesgo para el procedimiento de este plan, la cual consta de procesos que permitan la elaboración, soporte y mejora de la gestión en la seguridad de la información.
La implementación de estos controles permitirá que la confidencialidad, integridad y disponibilidad tenga un procedimiento mejorado para la seguridad de la información.
Este plan de tratamiento de riesgo siguió las medidas que la norma ISO 27002 establece para su implementación, cumpliendo con los requisitos expuestos se espera un mejor resultado para la organización.

Introducción

Hoy en día la seguridad de la información es uno de los puntos más importantes que toda organización necesita tener, encargada de proteger y salvaguardar la información ante cualquier amenaza.
La confidencialidad, integridad y disponibilidad de la información son importantes para la organización para situarse en niveles altos en competitividad, con los demás entes organizativos.
Las organizaciones pueden ser vulnerables ante cualquier amenaza, perjudicado los activos que interactúan con la información, ello puede generar pérdidas económicas y que la organización no pueda cumplir con sus objetivos.
Hay incidentes que suelen ocurrir accidentalmente o naturalmente dentro de la organización u otras que pueden ser causadas por parte del personal (robos, sabotaje, etc.)
El plan de tratamiento de la información ayuda mejorar los procesos que se tiene en la organización, donde se logra establecer políticas y procedimientos que permita mantener una mejor medición de los riesgos y una seguridad en los activos de la información.

Objetivos

- ✓ Establecer procedimientos que permita reducir los riesgos identificados en la UPN, implementando los controles de la norma ISO 27002, que brinden soporte y ayuda a los diferentes servicios, aplicaciones y equipos informáticos que almacenan o transfieran la información, protegiendo la confidencialidad, integridad y disponibilidad de la organización.

Alcance

- ✓ El alcance del plan de tratamiento de riesgo lleva para su implementación los siguientes controles:
  - ➢ Control 5.1.1: Políticas de seguridad
  - ➢ Control 8.1.1: Inventario de activos
  - ➢ Control 8.2.1: Clasificación de la información
  - ➢ Control 9.1.1: Políticas de control de acceso.
  - ➢ Controles (9.2.1, 9.2.2, 9.2.3, 9.2.5, 9.2.6) – Gestión de acceso de Usuario
  - ➢ Control 9.4.2: Procedimientos seguros de inicio de sesión
  - ➢ Control 11.1.2: Controles físicos de entrada
  - ➢ Control 11.2.1: Emplazamiento y protección de equipos
  - ➢ Control 12.2.1: Controles contra el código malicioso
  - ➢ Control 12.6.1: Gestión de vulnerabilidades técnicas

De un total de 24 controles que fueron seleccionados, se escogieron 14 de ellos, los cuales permitirán reducir los riesgos que fueron identificados durante la etapa de análisis de riesgo, y a la vez mejorar los resultados de la evaluación realizada mediante nuestra auditoria.
Los doce controles restantes no serán tomados en cuenta, puesto que con los 14 controles que fueron seleccionados para el plan de tratamiento de riesgo, cubren en gran parte con la mejora de la seguridad de la información tanto a un nivel físico como lógico, logrando así tener un nivel aceptable de la información y cumpliendo con lo que el proceso DSS05 – Gestionar los servicios de seguridad estipula. Aparte de esto los controles que no fueron seleccionados para la implementación involucran un costo elevado para la organización, lo que conllevaría por el momento a tomarlos en cuenta, pero en un futuro próximo poder aplicarlos para obtener así una completa protección de la información. Este documento estará al alcance de cada uno de los integrantes del área de TI de la UPN.

Propuestas para la implementación con controles
Propuesta01 – Control 5.1.1: Políticas de Seguridad

Identificación de la propuesta	Prop-01
Nombre	Definición de la política de seguridad
Ámbito	Documentación
Activos afectados	Hardware y Software
Descripción	✓ Se establecerá un documento de política de la seguridad de la información que deberá aprobar la dirección, y que será publicado y distribuido a todos los miembros involucrados de la organización. ✓ Este documento será planificado en tiempos para ser revisado y actualizado cuando surjan cambios que implican al documento, esto permitirá que mantenga su eficacia, idoneidad y adecuación. ✓ Este documento estará al alcance de cualquier usuario, logrando el cumplimiento y aceptación para la seguridad de la información. ✓ Esta política tendrá dos etapas las cuales serán: ✓ **Seguridad Física** ✓ Procesos de seguridad física que serán definidos de acuerdo a las políticas internas que maneja la organización. ✓ Registrar las acciones que se realiza para la seguridad física. ✓ Documentar las solicitudes de acceso a las instalaciones de la organización ✓ **Seguridad Lógica** ✓ Implementar controles de acceso lógico a la información ✓ Cumplir con los roles estipulados por cada usuario ✓ Supervisar las actualizaciones de los sistemas operativos ✓ Concientizar al usuario sobre la seguridad de la información ✓ Reducir los riesgos asociados a este control para salvaguardar los activos Buenas acciones y buen uso por parte de los usuarios
Controles	**5.1.1**
Presupuesto	Movilidad = S/. 50.00 Total = S/. 130.00 Logística = S/. 80.00

Propuesta02 – Control 8.1.1: Inventario de activos

Identificación de la propuesta	Prop-02
Nombre	Identificación e inventariado de los activos de información
Ámbito	Documentación
Activos afectados	Activos físicos, documentos de papel y software
Descripción	1) Identificar y documentar los activos tomando en cuenta las siguientes acciones: ✓ Identificar cuáles son los activos con más valor para el ciclo de vida de la información. ✓ El registro de su documentación debe ser sostenida en inventarios dedicados o existentes, según lo que sea apropiado. ✓ El inventario de activos debe estar preciso, actualizado, ser consistente, además de estar en relación con otros inventarios. ✓ En la documentación incluir al propietario de cada activo **2)** Elaborar el registro de activos. **3)** Revisar al detalle los activos de información y ser aprobado por la dirección.
Controles	**8.1.1**
Presupuesto	Movilidad = S/. 50.00 Total = S/. 94.00 Logística = S/. 44.00

Propuesta03 - Control 8.2.1: Clasificación de la información

Identificación de la propuesta	Prop-03
Nombre	Clasificación de la información
Ámbito	Documentación
Activos afectados	Activos físicos, documentos de papel y software
Descripción	La información será clasificada según su valor, los requisitos legales, su sensibilidad y criticidad para la organización. ✓ Realizar el análisis sobre los requisitos de información en base a su confidencialidad, integridad, y disponibilidad para su evaluación. ✓ Clasificar a los activos de acuerdo a la información que almacenan y procesan. ✓ Los propietarios de cada uno de los activos de TI, deben ser responsables de su debida clasificación. ✓ Establecer normas y/o políticas al clasificar la información. ✓ Manipular y etiquetar la información apropiadamente, de acuerdo con el esquema de clasificación adoptado por la organización ✓ Definir un manejo y tratamiento del activo de información. ✓ Actualizar los resultados de la clasificación de la información cuando altere su valor, sensibilidad y criticidad a lo largo de su ciclo de vida. No realizar una clasificación excesiva puesto que le podría a conllevar a la implantación de controles innecesarios con un gasto adicional.

	No realizar una clasificación escasa, puesto puede poner en peligro el logro de sus objetivos de negocio.
Controles	**8.2.1**
Presupuesto	Movilidad = S/. 50.00 Total = S/. 94.00 Logística = S/. 44.00

Propuesta04 – Control 9.1.1: Políticas de control de acceso

Identificación de la propuesta	Prop-04
Nombre	Definición de las políticas de control de acceso
Ámbito	Documentación
Activos afectados	Sistemas UPN y DSA
Descripción	✓ Se establecerá un documento de política de control de acceso que deberá estar aprobada por la dirección, que será publicado y distribuido a todos los miembros involucrados de la organización. ✓ Cada acceso debe constar con los privilegios asignados a cada usuario ✓ Actualizar la asignación de nuevos privilegios cuando surja un cambio de personal imprevisto. ✓ Clasificar los derechos de acceso de los usuarios ✓ Ver, actualizar y eliminar los usuarios que ya no trabajan dentro de la organización ✓ Se debe separar los accesos de acuerdo a las siguientes características: ✓ Hacer peticiones de acceso para los usuarios ✓ Verificar las autorizaciones de acceso para los usuarios ✓ Administrar los perfiles de acceso ✓ Hacer que la gestión de accesos reconozca todos los accesos que se da en cualquier lugar
Controles	**9.1.1**
Riesgos Asociados	PTR-11; PTR-18; PTR-22; PTR-38; PTR-138.
Presupuesto	Movilidad = S/. 50.00 Total = S/. 130.00 Logística = S/. 80.00

Propuesta05 – Controles (9.2.1, 9.2.2, 9.2.3, 9.2.5, 9,2.6): Gestión de Acceso de Usuarios

Identificación de la propuesta	Prop-05
Nombre	Procedimiento seguro sobre la gestión de acceso de Usuarios
Ámbito	Tecnológico y procedimental
Activos afectados	Sistemas UPN y DSA
Descripción	✓ Realizar registro de baja de usuario ✓ Realizar provisión de acceso de usuario ✓ Gestionar los privilegios de acceso de acuerdo con la política de control de acceso ✓ Establecer procedimientos que permitan revisar a intervalos de tiempo los derechos de acceso de los usuarios que tienen acceso a las redes y a las aplicaciones de negocio, y en caso posean demasiados privilegios revisarlo con mayor frecuencia. ✓ Los derechos de acceso de los usuarios que hayan cambiado de rol dentro de la misma organización, deben ser revisados y

	reasignados. En caso el usuario haya finalizado su contrato con la organización se debe revocar su acceso. ✓ Tener un registro de los cambios que se den en las cuentas privilegiadas. ✓ Efectuar retirada de los derechos de acceso cuando finalice el empleo, contrato o ser reasignados en caso de cambio de rol.
Controles	**9.2.1, 9.2.2, 9.2.3, 9.2.5, 9.2.6**
Riesgos Asociados	PTR – 64; PTR – 68; PTR – 148; PTR – 149; PTR – 161; PTR – 162.
Presupuesto	Movilidad = S/. 50.00 Total = S/. 87.00 Logística = S/. 37.00

Propuesta06 – Control 9.4.2: Procedimientos seguros de inicio de sesión

Identificación de la propuesta	Prop-06
Nombre	Procedimientos para el seguro inicio de sesión a los sistemas
Ámbito	Tecnológico y procedimental
Activos afectados	Sistemas UPN y DSA
Descripción	❖ Definir una técnica de autenticación de identidad del usuario ❖ Establecer procedimientos para el diseño de inicio de sesión a los sistemas y/o aplicaciones, de modo que reduzca la oportunidad de accesos no autorizados. ❖ El procedimiento de inicio de sesión debe revelar el mínimo de información sobre la aplicación o el sistema, para impedir prestar ayuda innecesaria hacia un usuario no autorizado. ❖ Establecer procedimientos para un desarrollo seguro, de modo que impida brindar las facilidades a los usuarios no autorizados a acceder a las aplicaciones o sistemas de la organización. ✓ Generar un evento de seguridad cuando se detecte un intento potencial o con éxito de infracción de los controles de inicio de sesión. ❖ Solo cuando se haya completado con éxito el inicio de sesión, se debiese mostrar: La fecha y hora del anterior inicio de sesión que tuvo éxito y las especificaciones de cualquier intento de inicio de sesión sin éxito desde el anterior que tuvo éxito. ✓ Para tener protegida la información que conllevan las aplicaciones y sistemas, tener en cuenta que, al iniciar sesión, no se debiese mostrar a un usuario externo las contraseñas que se están introduciendo, ni transmitir por la red contraseñas que no estén cifradas. ✓ Las sesiones inactivas deben ser terminadas tras periodos cortos de inactividad, especialmente en sitios de mucho riesgo. ❖ Restringir los tiempos de conexión para proveer una seguridad adicional a las aplicaciones que poseen un enorme riesgo.
Controles	**9.4.2**
Riesgos Asociados	PTR – 14; PTR – 19; PTR – 139; PTR – 147; PTR – 151; PTR – 153; PTR – 155; PTR – 160
Presupuesto	Movilidad = S/. 50.00 Total = S/. 87.00 Logística = S/. 37.00

Propuesta07 – Control 11.1.2: Controles físicos de entrada

Identificación de la propuesta	Prop-07
Nombre	Monitorización de los controles físicos de entrada

Ámbito	Documentación
Activos afectados	Activos físicos
Descripción	✓ Supervisar el ingreso de los visitantes previamente aprobado por el personal autorizado. ✓ Entregar un fotocheck que conlleve un código de identificación a todos los visitantes u operarios que ingresan a las instalaciones de la UPN. ✓ Registrar la fecha, hora de entrada y salida, las áreas donde va acceder, código de carnet de identificación y datos personales de todos los visitantes u operarios (personal de apoyo interno) que ingresan a las instalaciones de la UPN. ✓ Notificar al personal de seguridad si se encuentra a un visitante u operario sin la compañía de algún supervisor, o que no llevase una identificación visible (fotocheck). ✓ Elaborar un libro o informe físico de registro de todos los accesos físicos a las instalaciones de la UPN. ✓ Restringir el acceso de los operarios (personal de apoyo interno) a las instalaciones u áreas donde se almacena información sensible para la organización, solo cuando sea requerido, a la vez de ser autorizados y controlados por el personal designado. ✓ Revisar y actualizar regularmente los derechos de accesos a las áreas seguras, y a su vez ser revocados cuando sea necesario.
Controles	**11.1.2**
Riesgos Asociados	PTR-51; PTR-56; PTR-63; PTR-67; PTR-73; PTR-78; PTR-85; PTR-87; PTR-90; PTR-93; PTR-96; PTR-99; PTR-105; PTR-110; PTR-115; PTR-120; PTR-125; PTR-131;
Presupuesto	Movilidad = S/. 50.00 Total = S/. 120.00 Logística = S/. 70.00

Propuesta08 – Control 11.2.1: Emplazamiento y protección de equipos

Identificación de la propuesta	Prop-08
Nombre	Documentación de Políticas para el emplazamiento y protección de equipos
Ámbito	Documentación
Activos afectados	Activos físicos
Descripción	✓ Los equipos tecnológicos (servidores, laptops, monitores, USB, teléfonos, iPads, routers, CPU, cámaras, etc.) deben situarse en ambientes disponibles para su protección de la seguridad de la información. Restringiendo el acceso no autorizado por personal que no corresponde a la organización. ✓ Los equipos tecnológicos (servidores, switches, laptops, CPU, etc.) que transmitan información importante y clasificada dentro del área de TI deben situarse en ambientes apartados al acceso del propio personal que no está autorizado. ✓ Establecer controles para reducir los riesgos ante las posibles amenazas físicas y ambientales. Además de mostrar señalizaciones que indiquen que no se puede comer, beber y fumar en las instalaciones donde los equipos transmiten información sensible para la organización, asimismo de tener un control sobre el ambiente donde se almacena los equipos de información. ✓ Proteger los dispositivos (laptops, teclados, monitores, etc.) que se encuentren en zonas o áreas de tecnología industrial ✓ Usar protecciones contra emanaciones electromagnéticas (que impidan la perdida de información sensible)

Controles	**11.2.1**
Riesgos Asociados	PTR-49; PTR-55; PTR-71; PTR-76; PTR-83; PTR-103; PTR-108; PTR-113; PTR-118; PTR-123; PTR-129; PTR-167; PTR-169; PTR-170; PTR-172
Presupuesto	Movilidad = S/. 50.00 Total = S/. 150.00 Logística = S/. 100.00

Propuesta09 – Control 12.2.1: Controles contra el código malicioso

Identificación de la propuesta	Prop-08
Nombre	Procedimientos para la protección contra el código malicioso
Ámbito	Procedimiento y Documentación
Activos afectados	Activos físicos y de software
Descripción	✓ Instalar un software que permita detectar una amenaza que implica la perdida de información ✓ Tener conciencia de los accesos a páginas web que se encuentren permitidas y no permitidas por el área de TI, para reducir vulnerabilidades que perjudiquen la información. ✓ Analizar las revisiones de los sistemas de información (software) las distintas amenazas que se encontró. ✓ Para actualizar e instalar un software en los ordenadores del área de TI se debe hacer: ✓ Comprobar que el software permita detectar virus ✓ Comprobar que el software compruebe si la descargas son factibles para su uso dentro de la organización y si se encuentra infectado o no ✓ Comprobar que las páginas web sean confiables y se segura para su navegación ✓ Tener un procedimiento que cada periodo de tiempo se recopile la información de software malicioso, que las páginas web, publicaciones, etc. sean confiables y acreditas para luego comunicar al personal sobre el informe que se realizó.
Controles	**12.2.1**
Riesgos Asociados	PTR-28; PTR-88; PTR-91; PTR-94; PTR-97; PTR-100.
Presupuesto	Movilidad = S/. 50.00 Total = S/. 130.00 Logística = S/. 80.00

Propuesta10 – Control 12.6.1: Gestión de Vulnerabilidades Técnicas

Identificación de la propuesta	Prop-09
Nombre	Procedimientos para la gestión de vulnerabilidades técnicas
Ámbito	Procedimiento
Activos afectados	Activos de Software
Descripción	✓ Establecer procedimientos que permita gestionar las vulnerabilidades encontradas en la organización ✓ Obtener un registro de las vulnerabilidades de los sistemas de información utilizados por la organización. ✓ Adoptar medidas que permitan reducir el riesgo que se asocia a las vulnerabilidades encontradas en los sistemas de información de la organización.

	✓ Tener una escala de medición, relacionada a las vulnerabilidades encontradas en los sistemas de información ✓ Establecer procesos de auditorías de los procedimientos que se realizó en los sistemas de información de la organización. ✓ Hacer un estudio (supervisión y evaluación) que garantice la eficacia y efectividad de la gestión de vulnerabilidades ✓ Verificar que los sistemas de información (software) cuenten con la licencia original para garantizar su efectividad en el área de TI.
Controles	**12.6.1**
Riesgo Asociado	PTR-03; PTR-135; PTR-141
Presupuesto	Movilidad = S/. 50.00 Total = S/. 150.00 Logística = S/. 100.00

Cronograma

La propuesta para el plan de tratamiento de riesgo está planificada a realizarse en 10 semanas, iniciando desde la primera semana del mes de octubre y finalizando en la segunda semana del mes de diciembre. En la figura 1 se visualiza el cronograma de actividades, el cual fue planificado para la elaboración de nuestras propuestas para el plan de tratamiento del riesgo.

		Noviembre					Diciembre		
Ítem	**Descripción**	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**S8**
1	Definición de la política de seguridad								
2	Definición de las políticas de control de acceso								
3	Identificación e inventariado de los activos de información								
4	Clasificación de la información								
5	Documentación de Políticas para el emplazamiento y protección de equipos								
6	Monitorización de los controles físicos de entrada								
7	Procedimientos para la gestión de vulnerabilidades técnicas								
8	Procedimientos para la protección contra con el código malicioso								
9	Procedimiento seguro sobre la gestión de acceso de Usuarios								
10	Procedimientos para el seguro inicio de sesión a los sistemas								

Figura 1*:** Cronograma de actividades ***(Fuente: Elaboración propia)

Presupuesto

El presupuesto que se muestra a continuación detalla lo que se invertirá en cada control, las cuales cada control consta de un presupuesto teniendo en cuenta en lo logístico y en la movilidad, la tabla 2 muestra al detalle el presupuesto de cada ello.

Tabla 1:
Presupuesto de los controles seleccionados en el plan de tratamiento de riesgo

CONTROLES DE LA NORMA ISO 27002	TOTAL DEL PRESUPUESTO
CONTROL 5.1.1	S/. 130.00
CONTROL 8.1.1	S/. 94.00
CONTROL 8.2.1	S/. 94.00
CONTROL 9.1.1	S/. 130.00
CONTROLES (9.2.1, 9.2.2, 9.2.3, 9.2.5, 9.2.6)	S/. 87.00
CONTROL 9.4.2	S/. 87.00

CONTROL 11.1.2	S/. 120.00
CONTROL 11.2.1	S/. 150.00
CONTROL 12.2.1	S/. 130.00
CONTROL 12.6.1	S/. 150.00
TOTAL PRESUPUESTO	S/. 1172.00

***Fuente**: Elaboración Propia*

En general nos detalla lo que se invertirá en cada implementación de los controles, la cual como investigadores asumiremos más del 50% del presupuesto. Siendo la totalidad del presupuesto es de S/. 1172.00, en el gráfico 1 muestra que control se invertirá más y con ello planificar el presupuesto

Gráfico 1: Descripción de los controles en barras estadísticas (***Fuente*:** Elaboración propia)

Anexo 23: Manual de Políticas de Seguridad de la Información

Política de Seguridad de la Información

UNIÓN PERUANA DEL NORTE

Área de Tecnología de Información (TI)

Diciembre 2017

INDICE

1. Introducción

El área de tecnología de información (TI) de la Unión Peruana de norte identifica la información como un mecanismo importante para la dirección y obtención de los objetivos definidos por la estrategia de la organización, de tal manera que es necesario que el área de TI proteja la información física y lógica de la organización, para que sea almacenada, tratada, procesada y transmitida. Este documento esta lineado en base a las políticas y normas descritas de seguridad de la información definidas por el área de TI en conjunto con la alta dirección.

Para desarrollar este documento se recolecto como base algunas reglas o normas que el área de TI definía como políticas, además de utilizar los controles de la norma ISO/IEC 27002:2013 que detalla normas para proteger la integridad, confiabilidad y disponibilidad de la información.

La definición de estas normas permite tener un mejor funcionamiento en la seguridad de la información, en el ámbito físico y lógico de la Unión Peruana del Norte, los sistemas de información (Sistemas DSA-UPN) y los equipos de almacenamiento (Laptops, Switch, Servidor, etc.) deben estar protegidos de acuerdo a lo establecido en las normas de la Unión Peruana del Norte.

La seguridad de la información es una prioridad para la Unión Peruana del Norte, que, mediante el área de TI, permite mejorar y brindar una solvente ayuda a las distintas áreas de la organización, por lo tanto, es responsabilidad de todo el personal que trabaja dentro de ella, velar que no existan actividades que perjudiquen la trasmisión, recepción y almacenamiento de la información que se maneja dentro de la Unión Peruana del Norte.

2. Objetivo

Como objetivo de este documento es mejorar la seguridad de la información dentro de la Unión Peruana del Norte, estableciendo políticas de seguridad de la información para el área de Tecnologías de Información (TI).

3. Alcance

Las políticas de seguridad de la información cubren todos los aspectos administrativos y operacionales que son cumplidos por el personal del área, directivo y/o tercero que laboren o tengan relación con la Unión Peruana del Norte, para brindar un nivel aceptable de protección en la seguridad física y lógica de la información.

4. Política General de Seguridad de la Información

La Unión Peruana del Norte menciona que la información es un activo fundamental para la mejora de sus servicios y la toma de decisiones adecuadas, razón por la cual existe una estrategia manejada por el proceso de negocio para la protección de sus propiedades más significativas dentro de la organización.

Teniendo en cuenta las necesidades presentes, el área de TI de la Unión Peruana del Norte implementa estas políticas para la mejora de la seguridad física y lógica de la información, que permite identificar y minimizar los riesgos a los cuales se muestra la información, además que ayuda a reducir los costos en las áreas y en las inversiones de la organización.

El personal del área de TI y todo aquel que tenga responsabilidades sobre las equipos tecnológicos, inmuebles y recursos de procesamiento de la información de la Unión Peruana del Norte, deben aceptar las políticas descritas en el presente documento y en los

documentos relacionados con él, con el fin de mantener la disponibilidad, confidencialidad, y la integridad de la información.
Este documento tendrá las leyes de la organización, las políticas y las normas que están definidas en conjunto con los dominios y objetivos de los controles de la norma ISO/IEC 27002:2013.
El área de TI tendrá la facilidad y la autoridad de cambiar o modificar el documento de Políticas, de acuerdo con las necesidades de la organización que vayan surgiendo en el trayecto.

5. Compromiso de la Alta Gerencia

La dirección de la Unión peruana del Norte aprueba este documento de Política de Seguridad de la Información, como muestra de compromiso, lealtad y apoyo del diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la organización.
Ello muestra su compromiso a través de actividades de evaluación que son:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- Facilitar la divulgación de este manual a todo el personal de la organización.
- El apoyo de los recursos para implementar y mantener las políticas de seguridad de la información.
- La comprobación del desempeño de las políticas indicadas.

6. Sanciones para las infracciones o incumplimientos de las Políticas de Seguridad de la Información

Las políticas de seguridad expuestas en este documento son acciones con fines de mejorar las leyes y legislaciones de la organización, cumpliendo con afianzar la aceptación con el personal de la Unión Peruana del Norte. Es por ello, que, para mitigar y definir falencias en la seguridad de la información, las infracciones realizadas en el documento de Políticas de Seguridad de la Información, son clasificadas según las medidas correctivas que se encontró. Se considera las medidas correctivas lo que se estipulo en conjunto con la organización, desde penalidades disciplinarias hasta penalidades administrativas, de acuerdo a la circunstancia que lo amerita.

7. Políticas para la organización de la seguridad de la información

La Unión Peruana del Norte establece un marco para iniciar y controlar la implementación y operación de la seguridad de la información.

7.1. Roles y responsabilidades en seguridad de la información

- La Alta Gerencia de la Unión Peruana del Norte define y establece los roles y responsabilidades que se relacionen con la seguridad de la información.
- La Alta Gerencia de la Unión Peruana del Norte analiza y aprueba las Políticas de Seguridad de la información establecidas en este documento.
- La Alta Gerencia de la Unión Peruana del Norte define y establece un procedimiento de contacto con los gerentes y/o directores de la organización, teniendo descrita los responsables de dicho contacto.
- La Alta Gerencia promueve constantemente la concientización al personal sobre la importancia de la seguridad de la información en la organización.

- La Alta Gerencia proporciona la divulgación sobre el documento de las Políticas de Seguridad de la Información a todo el personal que se encuentra laborando en la organización.
- El área de TI actualiza y expone ante la Alta Gerencia, la secuencia del proceso para realizar el análisis de riesgos y la metodología para la clasificación de la información, según lo considere adecuado.
- El área de TI analiza e informa los incidentes de seguridad que se encontró, cuando lo requiere necesario a las autoridades de la organización.
- El área de TI verifica e informa si las demás entidades de la organización cumplen con las Políticas de Seguridad de la información mencionadas.

7.1.1. Políticas dirigidas a: Área de tecnología de Información (TI)

- El área de TI debe encabezar los lineamientos establecidos para la mejora de seguridad de la información de la Unión Peruana del Norte, estableciendo controles físicos y lógicos, que permitan reducir el análisis de riesgo realizado.
- El área de TI valida y monitorea de manera periódica la implantación de los controles de seguridad establecidos.
- El área de TI programa y elabora auditorías internas que aseguren el nivel de Seguridad de la Información de la Unión Peruana del Norte a fin de establecer si las políticas, procedimientos y controles, están acordes con los requerimientos de la organización y requerimientos de seguridad.
- El área de TI realiza revisiones de los procesos que forman parte del alcance de la Seguridad de la Información, con la finalidad de que sean conformes.
- El área de TI informa a las áreas responsables los resultados de hallazgos en las auditorías realizadas
- El área de TI asigna las funciones, roles y responsabilidades, a su personal de área para la administración de los sistemas de información de la organización. Dichas funciones, roles y responsabilidades deben estar documentadas y apropiadamente separadas.

7.2. Política para el uso de dispositivos móviles

El área de TI de la Unión Peruana del Norte es la encargada de distribuir las condiciones adecuadas para el debido manejo de los dispositivos móviles (celulares, tabletas e iPad entre otros). Que requieran el uso de los servicios que brinda la organización. Así mismo, vigilará que el personal de la organización utilice de manera correcta y adecuada los equipos y servicios proporcionados por la organización.

- El área de TI revisa y establece configuraciones que se realizó para los dispositivos móviles de la organización, que requiera del uso de los servicios de la Unión Peruana del Norte.
- El área de TI revisa la configuración de los equipos telefónicos, con el fin de eliminar la información que se encuentra dentro de ello, restaurarlos a modo de fábrica, evitando la divulgación no autorizada de información en caso de pérdida o robo.

- ✧ El personal de la Unión Peruana del Norte evita usar los dispositivos móviles en lugares que no cuenten la seguridad adecuada que ocasionen la pérdida o robo del dispositivito
- ✧ El personal de la Unión Peruana del Norte no puede modificar la configuración la cual ha sido dada en los equipos al momento de su entrega
- ✧ El personal de la Unión Peruana del Norte no puede instalar o desinstalar algún software o aplicación en el dispositivo, está bajo su responsabilidad la protección y cuidado de los dispositivos móviles.
- ✧ El personal de la Unión Peruana del Norte solo puede instalar las aplicaciones desde las páginas oficiales de cada aplicación, previo aviso.
- ✧ El personal de la Unión Peruana del Norte actualiza la última versión de IOS o Android en los dispositivos móviles.

8. Políticas de Seguridad para cambio de roles o funciones

La Unión Peruana del Norte tiene como principal elemento, su grupo de trabajo para llegar a sus objetivos trazados, es por ello que se necesita tener un grupo de trabajo calificado y dispuesto a cumplir con las necesidades de la organización, haciendo que sea acorde a lo estipulado por la organización, orientado a las funciones ý roles que desempeñan dentro de la ella.

8.1.1. Política para el cambio de responsabilidades

- ✧ Cada jefe de área informa de forma rápida al área TI, la desvinculación o el cambio del puesto de trabajo del personal que labora dentro de ella
- ✧ El área de TI cumple con el retiro de accesos y privilegios que están de la mano con la desvinculación o el cambio del puesto de trabajo del personal que labora en la organización.
- ✧ El área de TI capacita e instruye al personal de la organización sobre las charlas de concienciación en seguridad de la información, para evitar posibles riesgos que perjudiquen la seguridad.
- ✧ El área de TI controla la asistencia a las charlas y capacitaciones sobre la seguridad de la información, empleando sanciones adecuadas por la inasistencia.

9. Política de Gestión de Activos

EL área de TI establece una identificación de activos que permita definir las responsabilidades adecuada de protección.

9.1.1. Política de Inventario de Activo

- ✧ El área de contabilidad es la encargada de otorgar el registro de activos, bajo la responsabilidad de las áreas sobre sus activos de información.
- ✧ Todos los activos físicos y lógicas (móviles, sillas, cámaras, correos, laptops, licencias, etc.) se considera un activo para la Unión Peruana del Norte, que proporciona a todo el personal con el fin de cumplir con los objetivos de la organización.
- ✧ El área de TI almacena la información sensible(documentos sensibles) de la organización de la Unión Peruana del Norte, así como los activos donde ésta se

almacena y se procesa deben ser asignados por un responsable, inventariados y luego clasificarlo, de acuerdo con los requisitos de la organización.

- ✧ El área de TI actualiza y monitorea el inventario de activos de información que involucra al interior del área y sus perfiles de acceso a la información.
- ✧ El área de TI es la propietaria de los activos de información que se encuentran bajo su custodia, en conclusión, el área debe asegurar su apropiada operación y administración.
- ✧ El área de TI es la encargada de recibir los equipos tecnológicos (Switch, laptops, monitor, servicios, etc.) e inmuebles (sillas, escritorios, etc.) para la organización, el área de TI crea una copia detallada de las características del activo y quien estará a cargo del activo requerido.
- ✧ El área de TI analiza los riesgos de seguridad de forma periódica, sobre los activos que pueden ver perjudicado en la Unión Peruana del Norte.
- ✧ El área de TI define las condiciones de uso y protección de los activos de información, tanto los tecnológicos, inmuebles y servicios.
- ✧ El personal de Unión Peruana del Norte, utiliza de manera correcta los activos físicos y lógicos de la información, cumpliendo con las políticas para el debido cuidado evitando daños o pérdidas en la organización.
- ✧ El personal de la organización no debe instalar y/o utilizar software no autorizado en la organización.
- ✧ El área de TI presenta la lista de aplicaciones o softwares que se encuentran disponibles para el uso adecuado en la organización.

9.1.2. Política de Clasificación

- ✧ El área de TI de la Unión Peruana del Norte expone los tipos de niveles de clasificación de la información expuestos en el área para que sean aprobados por la alta gerencia.
- ✧ El área de TI establece los niveles de clasificación de la información para la Unión Peruana del Norte, para generar la guía de clasificación de la información.
- ✧ El jefe de TI informa sobre la guía de clasificación de la Información al personal que labora dentro del área.

10. Política de Control de Acceso

El área de TI, es el responsable de los sistemas de información que se maneja actualmente en la organización, ellos deben proteger la integridad, confidencialidad y disponibilidad de la información, salvaguardando la información con acceso no autorizados a través de mecanismos y controles de acceso lógico.

Para la información necesaria sobre los controles de acceso, ver el Manual de Políticas de Control de Acceso, especificando la importancia de las políticas necesarias para su mejor control.

11. Política de Criptografía

El área de TI consta que la información clasificada dentro de la organización se encuentre cifrada al momento de almacenarse o transmitirse para cualquier medio la Unión Peruana del Norte.

Para la información necesaria sobre las políticas de criptografía, las acciones que se desarrolla son de inversión para personas certificadas que cumplan la acción de

encriptar, por ello para ver las acciones que fueron transferidas se observa el Manual de Políticas de Criptografía en conjunto con las medidas de la estrategia de riesgo Transferir.

12. Política de seguridad Física

El área de TI supervisa los distintos mecanismos de seguridad física que permita tener un mejor control de los accesos de usuarios no autorizados. Es por ello que tendrá las condiciones adecuadas de protección en las oficinas, áreas o distintas instalaciones de la Unión Peruana del Norte.
Los lugares que cuenten con equipos sumamente importantes para la organización (servidores), son considerados de acceso restringido.

12.1. Política de áreas seguras y protección de Equipos (Servidores, equipos portátiles y Switches)

- Para tener acceso a las instalaciones del área de TI, se gestiona mediante una solicitud de petición de acceso, indicando el motivo de visita, que será aprobada o denegada mediante un sello y firma por el jefe del área de TI.
- El área de TI cerciora que durante la estadía en las instalaciones que la visita debe estar acompañada del personal a cargo designado por ellos.
- El área de TI tiene un registro de las visitas que se realizó en el área o instalaciones, durante el periodo que se encuentra a cargo.
- El área de TI controla el ingreso de los visitantes a los centros de procesamiento de datos que se encuentran bajo la custodia del área.
- El área de TI protege los equipos tecnológicos ubicados en el área y en las instalaciones ante posibles fallas en el suministro eléctrico
- El área de TI corrobora y verifica que las instalaciones estén totalmente protegidas, separadas de productos inflamables que ocasionen cortocircuitos, incendios o cualquier otra catástrofe.
- El área de TI crea un cronograma de mantenimiento para las equipos de procesamiento de datos (servidores) y de equipos que protejan a ello (aire acondicionado), teniendo un mejor control de los equipos tecnológicos.
- El personal porta su identificación visible, mientras estén dentro de la Unión Peruana del Norte, sea como invitado o parte de ella, en caso de pérdida de la identificación son reportado de manera inmediata para su debida restauración de identificación.
- El área de TI asigna perfiles de acceso físico, al personal de apoyo que labora por un periodo de tiempo dentro del área de TI Dichos perfiles de acceso debe estar documentado y apropiadamente separado.
- El área de TI es el principal encargado para asignar los equipos tecnológicos al personal que se encuentre en la Unión Peruana del Norte. Cualquier disposición de equipos que requiera el personal está prohibido sin previo autorización del área encargada
- Si se presenta un problema en el interior de los equipos tecnológicos, que estén en distintas áreas de la Unión Peruana del Norte, se informa al área de TI para que atienda y solucione el problema que se encontró, el personal no debe pretender solucionar el problema.

- El personal de la unión peruana del norte apaga su equipo tecnológico de trabajo al momento de terminar su función laboral en la Unión Peruana del Norte.
- El personal de la Unión Peruana del Norte acepta que está prohibido comer, beber y/o fumar dentro o cerca a equipos tecnológicos que interactúan con la trasmisión y recepción de la información
- El personal de la unión peruana del norte no puede dejar encendido su equipo tecnológico de trabajo en el momento de refrigerio o en horas que no labora.
- La instalación, reparación o desinstalación de software o aplicaciones en los equipos tecnológicos de las áreas o instalaciones de la Unión Peruana del Norte, está permitido por el área de TI para realizar tales actividades.
- Los equipos portátiles o de cómputo no son dejados en zonas públicas o que se encuentren al alcance de cualquier persona ajena a la Unión Peruana del Norte.
- Los equipos portátiles son protegidos durante su traslado en distintas zonas de la Unión Peruana del Norte.
- Si un equipo tecnológico (Switch, Laptop, Servidor, Tablet, etc.) es perdido o robado se informa al área de TI, para que empiece con el informe del equipo y sea enviado a la alta gerencia.

13. Política de seguridad de las operaciones

El área de TI es la que brinda la seguridad en las operaciones de los equipos tecnológicos que están en la Unión Peruana del Norte, donde asigna las funciones de seguridad al personal para que efectuara la documentación necesaria de las funciones que se les encargó.

13.1. Política de protección contra software malicioso

El área de TI proporciona diferentes medios que mejoren la seguridad de la información en los distintos recursos tecnológicos donde se procesa y almacena la información.

- El área de TI promueve la implementación de una herramienta de protección contra software malicioso (antivirus) que ayude a detectar malware (virus), para reducir los riesgos de pérdida de información en la organización.
- El área de TI sigue los pasos de lo establecido en el documento general del software antivirus GDATA, para su uso correcto.
- El área de TI cerciora que la información almacenada sea escaneada por el antivirus instalado, incluyendo correos, descargas, o información transferida por otros medios (USB, disco duro).
- El área de TI constata que el antivirus instalado se encuentre con la licencia actualizada que dispuso el proveedor del servicio. Garantizando su autenticidad y certificando los servicios que brinda.
- El área de TI es la única área aprobada para realizar alguna modificación de la configuración del antivirus, cualquier otro usuario o tercero no puede realizar dicha acción sin previa consulta al área.
- El personal de la Unión Peruana del Norte garantiza que esta actualizado el antivirus con la última licencia que se dispuso, reduciendo vulnerabilidades en los sistemas de información.
- El personal de la Unión Peruana del Norte solo puede realizar la acción escanear el virus a la información que se recibe o transfiere desde su equipo tecnológico.

- El personal debe ser concientizado sobre páginas confiables y no confiables para la descarga, lectura o ejecución de cualquier tipo de archivo que contenga información sensible o pública.
- El personal de la Unión Peruana del Norte que detecte virus en su ordenador, debe comunicar en seguida al área de TI para reducir el impacto del virus.

13.2. Política de copia de respaldo

- El área de TI gestiona las copias de respaldo de la información de la organización, proporcionado dentro de ellas las acciones o procedimientos que se debe realizar.
- El área de TI realiza las pruebas de copias de respaldo, que compruebe la integridad y posibilidad en caso sea requerida por la organización.
- El área de TI tiene conocimiento de cuáles son los equipos de almacenamiento donde se encuentre las copias de respaldo para su rápido y eficiente acceso que contienen la información de la organización.
- El área de TI define las condiciones de la custodia de las copias de respaldo de la información que son almacenadas externamente
- El área de TI almacena las copias de respaldo en la nube (internet), condición que se adquiere ante cualquier pérdida del medio de almacenamiento físico (USB, disco duro).
- El área de TI protege las copias de respaldo almacenadas en la nube, con contraseñas que se modifiquen, actualicen cada cierto periodo de tiempo.
- Es responsabilidad del área de TI la pérdida o robo de las copias de respaldo almacenadas en físico y/o en la nube (internet) que perjudique la estrategia, clasificación y procedimientos de la información.

13.3. Política de Gestión de Vulnerabilidades

- El área de Ti revisa periódicamente la aparición de vulnerabilidades en los diferentes sistemas de información de la Unión Peruana del Norte.
- El área de TI asigna responsabilidades de gestión de vulnerabilidades (supervisión, evaluación y seguimiento), que velen por la seguridad de los sistemas de información.
- El área de TI genera las recomendaciones de las de las vulnerabilidades encontradas en los sistemas de información, para la reducción x del riesgo que se asocian a ello.
- El área de TI crea un registro de las pruebas de vulnerabilidades encontradas, analizarlo y diagnosticar el daño que podría ocasionar cuando esté se convierta en amenaza.
- El personal del área de TI tiene el conocimiento sobre la urgencia del tratado del riesgo en la organización, viendo los cambios que perjudicaría a la organización.
- El área de TI realiza un estudio (supervisión y evaluación) que garantice la eficacia y efectividad de la gestión de vulnerabilidades en los sistemas de información de la Unión Peruana del Norte.

14. Políticas de seguridad en las comunicaciones

El área de TI certifica el resguardo de la información en los recursos de tratamiento de información y la información en las redes.

La estrategia de riesgo que se optó para la seguridad en las comunicaciones es de aceptar, se requiere ver el manual de políticas de comunicaciones en conjunto con las medidas adoptadas en la estrategia de riesgo aceptar.

15. Políticas de Adquisición, desarrollo y mantenimiento de los sistemas de información

El área de TI asegura que la seguridad de la información sea parte integral de los sistemas de información durante todo su ciclo de vida

15.1. Políticas para los requisitos de seguridad en sistemas de información

15.1.1. Norma dirigida a: Desarrolladores del Área de TI

- Los desarrolladores registran los requerimientos fundados y definir una arquitectura de software más eficiente para todas las aplicaciones y softwares que se desee desarrollar, esto en base a los controles requeridos y requerimientos de seguridad
- Los desarrolladores inhabilitan las funciones de autocompletar las interfaces de solicitud de datos que exijan información relevante.
- Los desarrolladores implementan el tiempo de permanencia de las sesiones que se hallan activas en las aplicaciones, finalizándolas estas una vez que se cumpla ese tiempo.
- Los desarrolladores cercioran de que no se admitan conexiones periódicas a los sistemas de información aplicados con el mismo usuario.
- Los desarrolladores cerciora que todos los sistemas en desarrollo utilicen herramientas de software licenciadas y acreditadas.

15.2. Política de seguridad en el desarrollo y en los procesos de soporte

El área de TI certifica la seguridad de la información que se ha implementado y diseñado durante el ciclo de vida de desarrollo en los softwares y aplicaciones.

- Los desarrolladores certifican las migraciones entre los ambientes de desarrollo, pruebas, y de producción de las aplicaciones nuevas y/o modificadas o funcionalidades nuevas.
- El área de TI conlleva a un sistema de control de versiones para gestionar los cambios que se den en las aplicaciones pertenecientes a la Unión Peruana del Norte.
- El área de TI cerciora que los sistemas o softwares obtenidos por terceros, conlleven un arreglo de licenciamiento el cual necesite detallar los términos del manejo del software y de los derechos de propiedad.
- Los desarrolladores tiene que autenticar que los sistemas de información desarrollados certifiquen o validen la información proporcionada por los usuarios previamente al ser procesada.
- Los desarrolladores provee opciones de cierre de sesión en las aplicaciones la cual permita culminar en su totalidad con la conexión o sesión relacionada.
- Los desarrolladores tiene que autenticar la conducción de operaciones críticas en los softwares o aplicaciones desarrolladas, aprobando el manejo de dispositivos adicionales, como ingreso de parámetros adicionales para la verificación o tokens.
- Los desarrolladores cerciora que no se promulgue la información confidencial en respuestas de error, conteniendo identificadores de inicio de sesión, datos del sistema u otros datos importantes.

- ✧ Los desarrolladores desaconsejan las modificaciones en los paquetes de software, limitándose a cambios necesarios, y cada cambio debiese ser objeto de un control riguroso.
- ✧ Los desarrolladores retira todas las funciones, archivos y datos que no sean relevantes para las aplicaciones desarrolladas, antes de la puesta en producción.
- ✧ Los desarrolladores salvaguardan el código fuente de los softwares y aplicaciones desarrolladas, de manera que no pudiese ser descargado ni alterado por los usuarios.
- ✧ Los desarrolladores resguardan e instauran adecuadamente los entornos de desarrollo óptimo para el desarrollo de los softwares y/o aplicaciones y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.
- ✧ Los desarrolladores cercioran que no se permita que las aplicaciones desarrolladas efectúen comandos directamente en el sistema operativo.
- ✧ Los desarrolladores pone en marcha ensayos de seguridad funcional durante el desarrollo de las aplicaciones y softwares. A la vez establecer programas de pruebas de aceptación.

15.3. Política para los datos de prueba

El Área de Ti asegura la protección de los datos de prueba

- ✧ El área de TI borra la información de los ambientes de prueba, una vez que han finalizado.
- ✧ El área de TI evita el uso de datos reales de operación que contengan datos personales o cualquier otra información confidencial para las pruebas.
- ✧ El área de TI realiza una autorización independiente cada vez que la información de operación se copia bajo un entorno de prueba.

16. Políticas de Gestión de incidentes de seguridad de la información

El área de TI garantiza una perspectiva coherente y óptima para la gestión de incidentes de seguridad en base a la información, abarcando en ello la comunicación de eventos de seguridad y las debilidades.

16.1. Política para la gestión de incidentes de seguridad de la información y mejoras

- ✧ El área de TI instaura procedimientos y responsabilidades para certificar una respuesta rápida, aplicada y eficiente frente a incidentes de seguridad de la información.
- ✧ El área de TI registra los eventos relacionados con la seguridad, considerando el nivel de la información
- ✧ El área de TI establece procedimientos que permitan monitorizar, analizar, evaluar, detectar, comunicar y tomar decisiones sobre los incidentes u eventos de seguridad de la información.
- ✧ El área de TI retiene por un periodo apropiado, el registro de los eventos en relación con la seguridad reportado por las herramientas de monitorización, con el fin de reducir la probabilidad o el impacto de los incidentes en un futuro, ayudando así en futuras investigaciones.
- ✧ Los usuarios de la Unión Peruana del Norte conocen los resultados de la recopilación de las evidencias de los incidentes de seguridad, en caso de no percibir la pérdida o publicación no autorizada de información clasificada como un uso interno,

restringida y altamente restringida, deben notificarlo al área encargada de riesgos para que se tome en consideración y se le dé el trámite necesario.

- ✧ El área de TI recopila las evidencias de los incidentes de seguridad.

16.2. Políticas de Cumplimiento

El personal del área de TI evita el incumplimiento de las obligaciones legales, estatutarias, reglamentarias, normativas o contractuales referentes a la seguridad de la información o de los requisitos de seguridad.

- ✧ El área de TI define de forma explícita los requisitos oportunos, tanto legales como estatutarios, contractuales o regulatorios, y el enfoque de la organización para cumplirlos, estos a su vez deben ser documentados y mantenidos actualizados para cada sistema de información de la UPN.
- ✧ El área de TI usa los controles criptográficos de acuerdo con todos los contratos, regulaciones y leyes pertinentes.
- ✧ Los usuarios de la Unión Peruana del Norte no instalan softwares en las estaciones donde laboran o equipos móviles provistos para el desarrollo de sus labores.
- ✧ El área de TI asegura que todos los softwares que son ejecutados en la organización sean licenciados y legítimos o, en su lugar sea software de libre distribución y de uso.
- ✧ El área de TI comprueba habitualmente que los sistemas de información cumplen con estas políticas y normas de seguridad de la información.
- ✧ La protección de los registros de la organización está protegido contra la pérdida, deterioro, adulteración, manifestación o acceso no autorizados en base a los requisitos legales y contractuales.

16.2.1. Normas de protección de datos personales y de privacidad

- ✧ El área de TI instaura controles aptos para resguardar la información personal de funcionarios, beneficiarios u otros usuarios en bases de datos o cualquier otro repositorio e impedir su publicación, modificación o deterioro sin la autorización requerida.
- ✧ Los usuarios de la Unión Peruana del Norte almacenan la discreción adecuada, o absoluta con respecto a la información de la organización, del cual conozcan sus funciones o labores que realizan dentro de la organización.
- ✧ Los usuarios Unión Peruana del Norte corroboran la identidad de todas aquellas personas externas a la organización, a quienes se les hace llegar información por distintos medios como: teléfono, correos electrónicos, mensajes, etc.
- ✧ Las áreas que procesan datos personales de todos los usuarios que forman parte de la Unión Peruana del Norte, se cercioran que solo aquellos usuarios que asuman una necesidad laboral legal puedan acceder a tales datos.

Anexo 24: Manual de Política de Control de Acceso Lógico

Manual de Política de control de Acceso Lógico

UNIÓN PERUANA DEL NORTE

Lugar:

Área de TI

Versión de Documento:

Primera Versión

2017

INDICE

1. Introducción

La implementación de controles de la norma ISO/IEC 27002 permite cumplir con los servicios de seguridad lógica y física, entre ellos el acceso lógico que genera el área de TI dentro de la organización.

Al no tener el control de los accesos a los sistemas de información se genera un acceso no autorizado dentro de las instalaciones del área de TI, ocasionando cambios, perdidas de información, falsificación de derechos, y privilegios no asignados, estas políticas ayuda a dar soporte y un mejor control de los accesos en las instalaciones de los sistemas de información.

Logrando reunir requisitos para tener registrado los accesos que se genera dentro de los equipos tecnológicos que posee la Unión Peruana del Norte.

2. Objetivo

El área de TI, es el responsable de los sistemas de información, servidores y la red y conectividad, que maneja actualmente en la organización, ellos deben proteger la integridad, confidencialidad y disponibilidad de la información, salvaguardando la información con acceso no autorizados a través de mecanismos y controles de acceso lógico.

3. Alcance

Este documento estará alineado con las políticas de seguridad de la información general, además detalla las restricciones de acceso lógico para los sistemas de información.

La política se destina a todos los accesos locales que contenga el área de TI de la Unión Peruana del Norte, teniendo como destino a todos los trabajadores.

4. Políticas de control de Acceso

4.1. Políticas de Acceso a Servidores y Centro de Datos

- El área de TI establece un procedimiento de autorización y controles para salvaguardar el acceso a los servidores y centro de datos.
- El área de TI certifica que los servidores y centros de datos cuenten con métodos de autenticación que impida accesos no autorizados.
- El acceso al centro de datos de la UPN, es exclusivo e intransferible para los usuarios acreditados del área de TI, o a quien la dirección designe.
- Las claves de acceso a los servidores estarán bajo custodia y son responsabilidad exclusiva del área de TI y solo se entregará previa autorización por escrito del Jefe de TI de la UPN.

4.2. Políticas para la Red y Conectividad

- Las conexiones de red están interconectadas dentro de la organización, que permita reconocer la gestión de acceso.
- El área de TI asegura que las redes inalámbricas de la organización, cuente con procesos de autenticación, que evite accesos no autorizados
- El área de TI autoriza la creación o modificación de las cuentas de acceso a las redes o recursos de red de la organización.

4.3. Políticas para los Sistemas de Información (Sistema DSA, Sistemas UPN)

- El área de TI establece los controles de acceso de acuerdo con los requisitos de negocio
- El jefe de TI debe verificar periódicamente los accesos, para los usuarios, con el fin de revisar que dichos usuarios tengan el acceso, solamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.
- La Unión Peruana del Norte cumple con el procedimiento de autorización de acceso a los servicios que el área de TI brinda.
- El área TI garantiza la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la organización, viendo la creación, modificación, bloqueo o eliminación de las cuentas de usuarios.

- Todos los usuarios son responsables sobre las acciones que se hace dentro de los sistemas de información de la organización, usando la contraseña asignada para el acceso sistemas de información (DSA, Gerencial y Académico).
- Los usuarios de la Unión Peruana del Norte que interactúen con los distintos sistemas de información, no deben compartir o brindar sus cuentas de usuario y contraseña a terceras personas. Las cuentas de usuarios y contraseñas son personales y solo pueden ser usadas por la persona autorizada y para fines institucionales.

4.4. Política de clasificación de la información

- El área de TI clasifica a la información según la importancia para la organización, viendo que usuario puede acceder a dicha información de acuerdo a los niveles de seguridad que el área de TI opto.
- El personal de trabajo cumple y acepta los niveles de clasificación de la información que el área de TI informó.
- El jefe de TI establece los derechos de acceso, con las políticas de clasificación de la información.
- El personal que desea tener acceso a información que no le corresponde, necesita constar de una autorización para acceder a la información que se encuentra clasificada depende la criticidad
- El área de TI registra todas las cartas de autorizaciones realizadas para visitar las instalaciones.

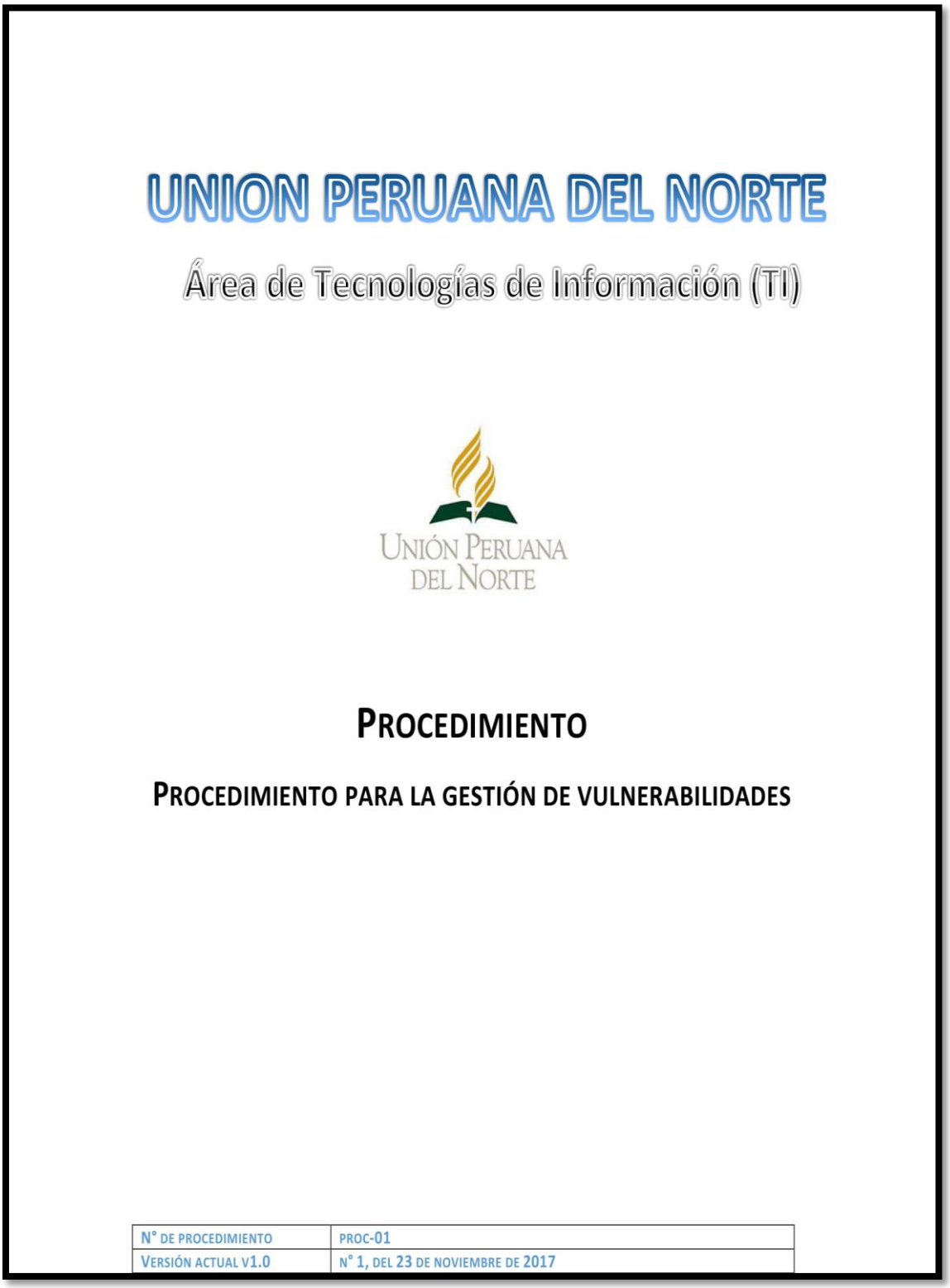
4.5. Limitación de acceso a datos o servicios

- Cada acceso que se efectué dentro de las instalaciones de red de la organización debe constar con la legislación adecuada para su limitación de acceso.
- Las reglas de acceso son documentadas para cada sistema de información de la organización
- Los usuarios de la Unión Peruana del Norte antes de tener acceso por primera vez a la red de datos de la organización, deben esperar a que el área de TI termine con el análisis de privilegios de acceso y creación de las respectivas cuentas de usuarios, luego a ello deben firmar la aceptación sobre la Confidencialidad y Aceptación de Políticas de Seguridad de la Información del área de TI.
- El personal acepta y cumple con las responsabilidades, en conjunto con los requisitos que se tiene documentado.

4.6. Segregación de acceso por roles

- El personal acepta y cumple con los derechos de acceso que se le asigno por roles.
- Los nuevos usuarios en conjunto con su jefe (encargado) de área deben definir los perfiles de usuario y en base a ello, solicitar al área de TI el acceso a sus perfiles definidos en los sistemas de información.
- Las áreas de la Unión Peruana del Norte deben hacer peticiones de acceso al área de TI para los usuarios que no están registrados dentro de la organización.
- El área de TI tiene personal autorizado y capacitado que registre y documente las peticiones de acceso que se solicita.
- El área de TI supervisa y aprueba las autorizaciones de acceso para los usuarios que requieren de un nuevo identificador, ocasionado por tener el ID de usuario igual a otro o que se asemeje en otro campo del registro.
- El área TI establece los lineamientos adecuados que indiquen la configuración de contraseñas de acceso los sistemas de información (DSA, Académico y Gerencial) (cuentas de usuarios en el controlador de dominio, correo electrónico y sistemas de información). Dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, para la autenticación y cambio de contraseña en el primer acceso.
- El personal debe estar capacitado para documentar el procedimiento para el registro, retirada y/o dado de baja por inactividad de los usuarios.

Anexo 25: Procedimiento para la Gestión de Vulnerabilidades



UNION PERUANA DEL NORTE

Área de Tecnologías de Información (TI)

UNIÓN PERUANA DEL NORTE

PROCEDIMIENTO

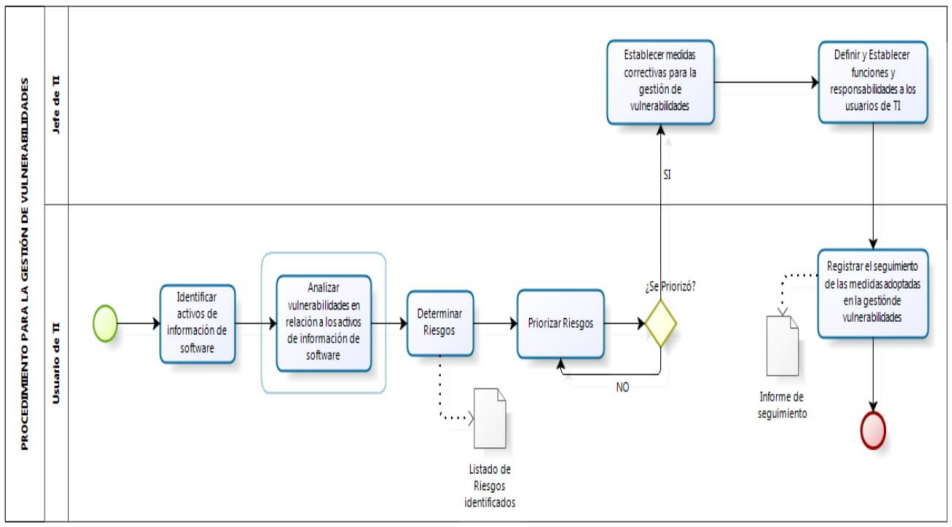
PROCEDIMIENTO PARA LA GESTIÓN DE VULNERABILIDADES

N° DE PROCEDIMIENTO	PROC-01
VERSIÓN ACTUAL V1.0	N° 1, DEL 23 DE NOVIEMBRE DE 2017

I. Cooperaron en la elaboración de este procedimiento

- Jefe del área de TI
- Usuario de TI

II. Flujo grama de información con sus listas de tareas



Actividad 1:

Ítem	Identificar activos de información de software
01	Realizar inventariado de los activos de información
02	Identificar el o los propietarios del activo de software
03	Identificar los proveedores del software
04	Identificar en que sistema se encuentra instalado el software

Actividad 2:

Ítem	Analizar vulnerabilidades en relación a los activos de información de software
05	Asociar las vulnerabilidades que podrían darse en relación con los activos de información de software
06	Realizar una escala de medición de la vulnerabilidad.

Actividad 3:

Ítem	Determinar riesgos
07	Identificar activos de información de software
08	Identificar las amenazas que podrían darse en relación a los activos de información de software
09	Identificar las vulnerabilidades en relación a los activos de información de software

Actividad 4:

Ítem	Priorizar riesgos
10	Establecer un rango de evaluación para medir el nivel de criticidad del riesgo
11	Evaluar la probabilidad de ocurrencia e impacto del riesgo
12	Tratar con importancia los medios y/o activos con mayor nivel de riesgo de información.

Actividad 5:

Ítem	Establecer medidas correctivas para la gestión de vulnerabilidades
13	Llevarse a cabo de acuerdo a la gestión de cambios
14	Seguir los procedimientos de respuesta a incidentes de seguridad de la información
15	Realizar búsqueda de parches para los sistemas de información para una eficiente medida correctiva
16	Verificar las fuentes de donde provienen los parches
17	Instalar los parches

Actividad 6:

Ítem	Definir y Establecer funciones y responsabilidades a los usuarios de TI
18	Establecer reuniones con los usuarios de TI
19	Brindar charlas y capacitaciones
20	Asignar las funciones y responsabilidades a los usuarios de TI de acuerdo a sus funciones y/o actividades

Actividad 7:

Ítem	Registrar el seguimiento de las medidas adoptadas en la gestión de vulnerabilidades.
21	Supervisar el cumplimiento de las medidas adoptados
22	Evaluar periódicamente el cumplimiento de las medidas adoptados
23	Documentar el registro de seguimiento de las medidas adoptados

III. Información general

Evento activador	Procedimiento para la gestión de Vulnerabilidades
Objetivo	Gestionar de manera eficaz y eficiente las vulnerabilidades y reducir los riesgos resultantes tras la explotación de estos.
Dueño	Jefe del área de TI

IV. Roles participantes

Jefe del área de TI: Encargado de la dirección general del área de TI de la Unión Peruana del Norte, además de ello brinda seguridad a la organización y acceso y conectividad a la red a los usuarios de la organización.

Usuario de TI: Encargado de laborar dentro del área de tecnologías de información de la Unión Peruana del Norte, que cumple roles, según el perfil que ha sido asignado.

V. Descripción del flujo

Procedimiento de Gestión de Vulnerabilidades				
ID	**Actividad**	**Rol**	**Tarea**	**Documento**
01	**Identificar activos de información de software**	**Usuario de TI**	Realizar inventariado de los activos de información	Informe de activo de información de software
02			Identificar el o los propietarios del activo de software	
03			Identificar los proveedores del software	
04			Identificar en que sistema se encuentra instalado el software	
05	**Analizar vulnerabilidades en relación a los activos de información de software**	**Usuario de TI**	Asociar las vulnerabilidades que podrían darse en relación con los activos de información de software	Informe de vulnerabilidades identificadas
06			Realizar una escala de medición de la vulnerabilidad.	
07	**Determinar riesgos**	**Usuario de TI**	Identificar activos de información de software	Informe de riesgos identificados
08			Identificar las amenazas que podrían darse en relación a los activos de información de software	
09			Identificar las vulnerabilidades en relación a los activos de información de software	
10	**Priorizar riesgos**	**Usuario de TI**	Establecer un rango de evaluación para medir el nivel de criticidad del riesgo	Informe de riesgos priorizados
11			Evaluar la probabilidad de ocurrencia e impacto del riesgo	
12			Tratar con importancia los medios y/o activos con mayor nivel de riesgo de información.	
13	**Establecer medidas correctivas para la gestión de vulnerabilidades**	**Jefe de TI**	Llevarse a cabo de acuerdo a la gestión de cambios	Informe de medidas correctivas
14			Seguir los procedimientos de respuesta a incidentes de seguridad de la información	
15			Realizar búsqueda de parches para los sistemas de información para una eficiente medida correctiva	
16			Verificar las fuentes de donde provienen los parches	
17			Instalar los parches	
18	**Definir y Establecer funciones y responsabilidades a los usuarios de TI**	**Jefe de TI**	Establecer reuniones con los usuarios de TI	Registro de reuniones
19			Brindar charlas y capacitaciones	Registro de capacitaciones y charlas
20			Asignar las funciones y responsabilidades a los usuarios de TI de acuerdo a sus funciones y/o actividades	Informe de asignación de responsabilidades
21	**Registrar el seguimiento de las medidas adoptadas en la gestión de vulnerabilidades.**	**Usuario de TI**	Supervisar el cumplimiento de las medidas adoptados	Informe de seguimiento
22			Evaluar periódicamente el cumplimiento de las medidas adoptados	
23			Documentar el registro de seguimiento de las medidas adoptados	

VI. Contingencias

Punto 1:

Actualización del inventario: Cuando se encuentren otras herramientas que permitan actualizar el inventario de activos deberá asociarse a la gestión de vulnerabilidades, dependiendo si la herramienta es de utilidad.

Punto 13

Alineamiento de medidas en conjunto con la gestión de cambios: Poner límites a los usuarios para que no surja ningún cambio en el área, los procesos de negocio y sistemas que afectan a la seguridad de la información

Punto 14

Alinear con las actividades de gestión de incidentes: Los incidentes de seguridad deben ser comunicados para su respuesta a un punto de contacto preestablecido así como a otras personas relevantes de la organización o terceras partes

Punto 16

Verificación de fuentes de descarga: Si existe un parche de fuente legítima deberían evaluarse los riesgos asociados con la instalación del mismo.

Punto 17

Instalación de parches: Los parches deberían ser probados y evaluados antes de su instalación para garantizar que son efectivos y que no tienen efectos secundarios que no puedan ser aceptados. En caso no exista o haya un parche disponible, deberían considerarse otros controles como:

- La desactivación de servicios o capacidades con la vulnerabilidad
- La adaptación o inclusión de controles de acceso
- El incremento de la supervisión para detectar o evitar ataques reales
- El aumento de la concienciación sobre la vulnerabilidad

VII. Historial de Revisiones

N° Versión	Fecha	Descripción de cambios
V1.0	23 de Noviembre de 2017	Primera versión

Anexo 26: Procedimientos para la protección contra el código malicioso

UNION PERUANA DEL NORTE

Área de Tecnologías de Información (TI)

UNIÓN PERUANA DEL NORTE

PROCEDIMIENTO

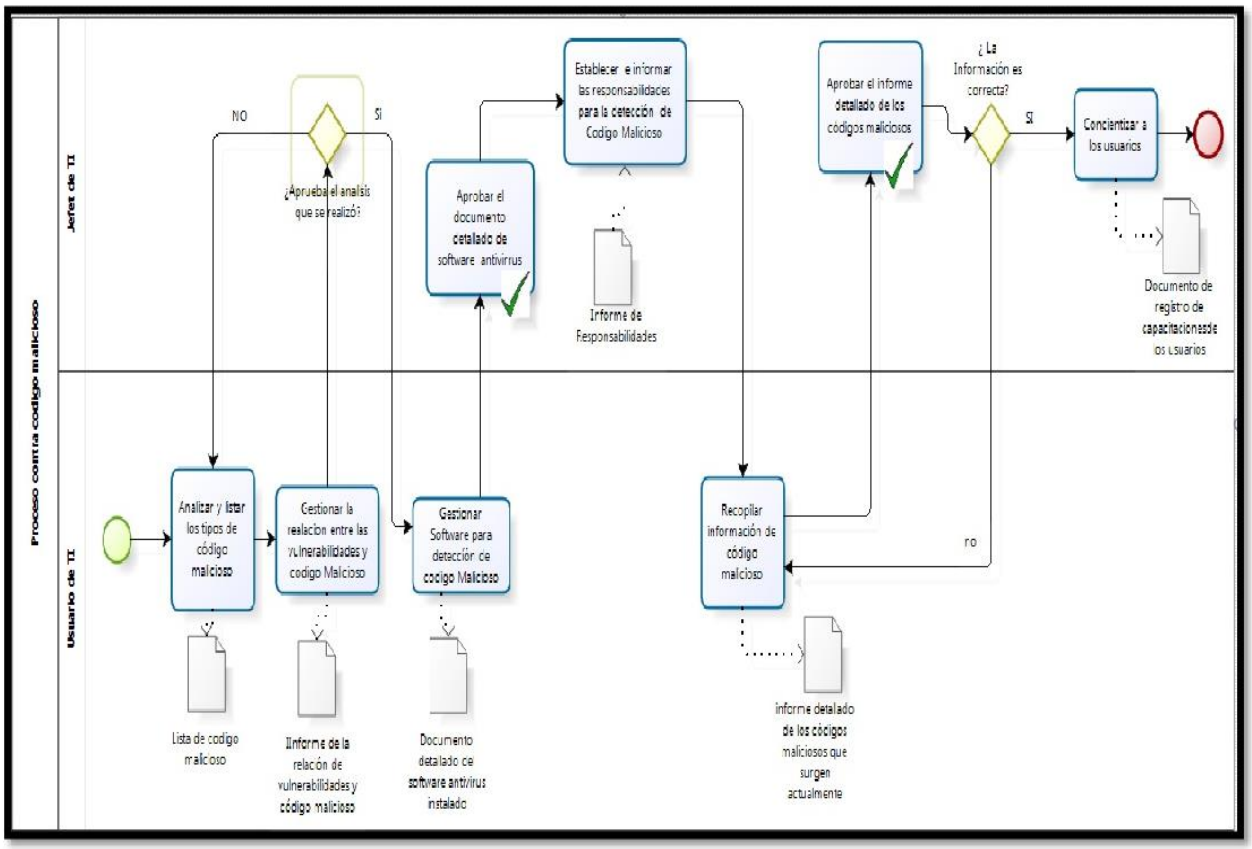
PROCEDIMIENTO PARA LA PROTECCIÓN CONTRA EL CÓDIGO MALICIOSO

N° DE PROCEDIMIENTO	PROC-03
VERSIÓN ACTUAL V1.0	N° 1, DEL 1 DE DICIEMBRE DE 2017

I. Cooperaron en la elaboración de este procedimiento

- Jefe del área de TI

II. Flujograma de información con sus listas de tareas



Actividad 1:

Ítem	Analizar y listar los tipos de código malicioso
01	Elaborar un listado de aplicaciones autorizados a fin de detectar código malicioso.
02	Verificar las fuentes de descarga de las aplicaciones para la detección de software malicioso
03	Revisar de acuerdo a lo descrito en la política de la seguridad de la información, la medida a adaptar para la protección de datos.

Actividad 2:

Ítem	Gestionar la relación entre las vulnerabilidades y software Malicioso
04	Revisar la lista de vulnerabilidades encontradas en el área de TI
05	Revisar los diferentes informes sobre los códigos malicioso que se encontró en los equipos tecnológicos
06	Informar sobre el análisis que se realizó, donde estipula la relación entre la vulnerabilidad y el código malicioso
07	Gestionar el documento de análisis donde se identifique la relación para el tratado contra el código malicioso

Actividad 3:

Ítem	Gestionar software para la detección de software malicioso
08	Llevar acabo revisiones y seguimientos regulares del software antivirus
09	Instalar software para la detección y reparación de códigos maliciosos
10	Informar sobre la detección de software malicioso, y archivar lo descrito para una futura mejora en los servicios.

Actividad 4:

Ítem	Establecer e informar las responsabilidades para la detección de Código Malicioso
11	Definir responsabilidades que permitan reducir el análisis de código malicioso
12	Tener copias de respaldo para la recuperación de datos ante cualquier ataque de código malicioso
13	Establecer revisiones sobre la implantación o reducción del código malicioso

Actividad 5:

Ítem	Recopilar información de código malicioso
14	Definir responsabilidades que permitan reducir el análisis de código malicioso
15	Tener copias de respaldo para la recuperación de datos ante cualquier ataque de código malicioso

Actividad 6:

Ítem	Concientizar a los usuarios sobre las diferencias de código malicioso y correos de spam
16	Realizar informes para repartir al personal sobre la importancia de código malicioso
17	Organizar charlas donde indique las consecuencias y las pérdidas de información
18	Documentar las charlas, capacitaciones y materiales informativos que se dieron para concientizar al usuario

III. Información general

Evento activador	Procedimiento para la protección contra el código malicioso
Objetivo	Asegurar que los recursos de tratamiento de información y la información que se manejan en la Unión Peruana del Norte estén protegidos contra los códigos maliciosos y/o malwares.
Dueño	Jefe del área de TI

IV. Roles participantes

Jefe del área de TI: Encargado de la dirección general del área de TI de la Unión Peruana del Norte, además de ello brinda seguridad a la organización y acceso y conectividad a la red a los usuarios de la organización.

Usuario de TI: Encargado de laborar dentro del área de tecnologías de información de la Unión Peruana del Norte, que cumple roles, según el perfil que ha sido asignado.

V. Descripción del flujo

Proceso de Gestión de Código Malicioso				
id	Actividad	Rol	Tarea	Documento
01	Analizar y listar los tipos de código malicioso	Usuario de TI	Elaborar un listado de aplicaciones autorizados para la detección de software malicioso.	Lista de aplicaciones que permiten detectar código malicioso
02			Verificar las fuentes donde se descarga las aplicaciones para la detección de software malicioso	Lista de fuentes que no está permitido para su descarga de software.
03			Revisar de acuerdo a lo descrito en la política de la seguridad de la información, la medida a adaptar para la protección de datos.	Informe de revisión sobre las medidas de protección de datos y su relación con la gestión de vulnerabilidades
				Listado de los diferentes tipos de código malicioso
04	Gestionar la relación entre las vulnerabilidades y software Malicioso	Usuario de TI	Revisar la lista de vulnerabilidades encontradas en el área de TI	Informe de la relación de vulnerabilidades y código malicioso
05			Revisar los diferentes informes sobre los códigos malicioso que se encontró en los equipos tecnológicos	
06			Informar sobre el análisis que se realizó, donde estipula la relación entre la vulnerabilidad y el código malicioso	
07			Gestionar el documento de análisis donde se identifique la relación para el tratado contra el código malicioso	
08	Gestionar software para la detección de software malicioso	Usuario de TI	Llevar acabo revisiones y seguimientos regulares del software antivirus	Documento detallado del software antivirus instalado
09			Instalar software para la detección y reparación de códigos maliciosos	
10			Informar sobre la detección de software malicioso, y archivar lo descrito para una futura mejora en los servicios.	
11	Establecer Responsabilidades para la detección de Código Malicioso	Jefe de TI	Definir responsabilidades que permitan reducir el análisis de código malicioso	Informe de las responsabilidades y la recuperación de la información ante ataques de código malicioso
12			Tener copias de respaldo para la recuperación de datos ante cualquier ataque de código malicioso	
13			Establecer revisiones sobre la implantación o reducción del código malicioso	
14			Cumplir con el procedimiento que contenga la información de los	

	Recopilar información e código malicioso	Usuario de TI	nuevos códigos maliciosos	informe detallado de los códigos maliciosos que surgen actualmente
15			Cumplir con el procedimiento de revisión, teniendo en cuenta si la información recolectada son confiables para su divulgación en las áreas de la organización	
16	Concientizar a los usuarios sobre las diferencias de código malicioso y correos de spam	Jefe de TI	Realizar informes para repartir al personal sobre la importancia de código malicioso	Registro de capacitaciones y charlas sobre las diferencias entre código malicioso y correo de spam
17			Organizar charlas donde indique las consecuencias y las pérdidas de información	Documento para la concienciación de los usuarios, sobre las diferencias entre códigos maliciosos y correos spam
18			Documentar las charlas, capacitaciones y materiales informativos que se dieron para concientizar al usuario	

VI. Contingencias

Punto 3:
Protección contra los riesgos asociados a las redes externas: Esta protección debe incluir la protección de la obtención de los softwares por medio de las redes externas.
Punto 8:
Revisiones regulares: Ante cualquier modificación no autorizada del software antivirus debiese ser investigada.
Punto 9:
Puntos a tomar en cuenta en las comprobaciones llevadas a cabo ante la instalación y actualización de software antivirus:

- La comprobación frente a código malicioso antes de su uso, de cualquier fichero recibido a través de redes, o vía de cualquier forma de soporte (electrónico u óptico)
- La comprobación frente a código malicioso antes de su uso, de los correos adjuntos al correo electrónico y las descargas; esta comprobación debe ser llevada en distintos lugares tales como: zonas u áreas donde se transmite información sensible, servidores de correo, zonas de red y conectividad, etc.
- Comprobación de páginas web para detectar código malicioso

Punto 14
Recogida de información: La recogida de información sobre los nuevos códigos maliciosos ya sea por medio de la suscripción a listas de correo o por medio de la revisión de las páginas web debe realizarse regularmente.
Punto 15
Verificación de la información relativa al código malicioso: La información que se adquiere acerca del software malicioso debe verificarse que son obtenidas de fuentes de confianza o de publicaciones acreditadas, sitios de internet que desarrollan software de protección contra código malicioso fiable, esto para su debida protección y aseguramiento.

VII. Historial de Revisiones

N° Versión	Fecha	Descripción de cambios
V1.0	1 de Diciembre de 2017	Primera versión

Anexo 27: Procedimiento seguro sobre la gestión de acceso de usuarios

UNION PERUANA DEL NORTE

Área de Tecnologías de Información

UNIÓN PERUANA DEL NORTE

PROCEDIMIENTO

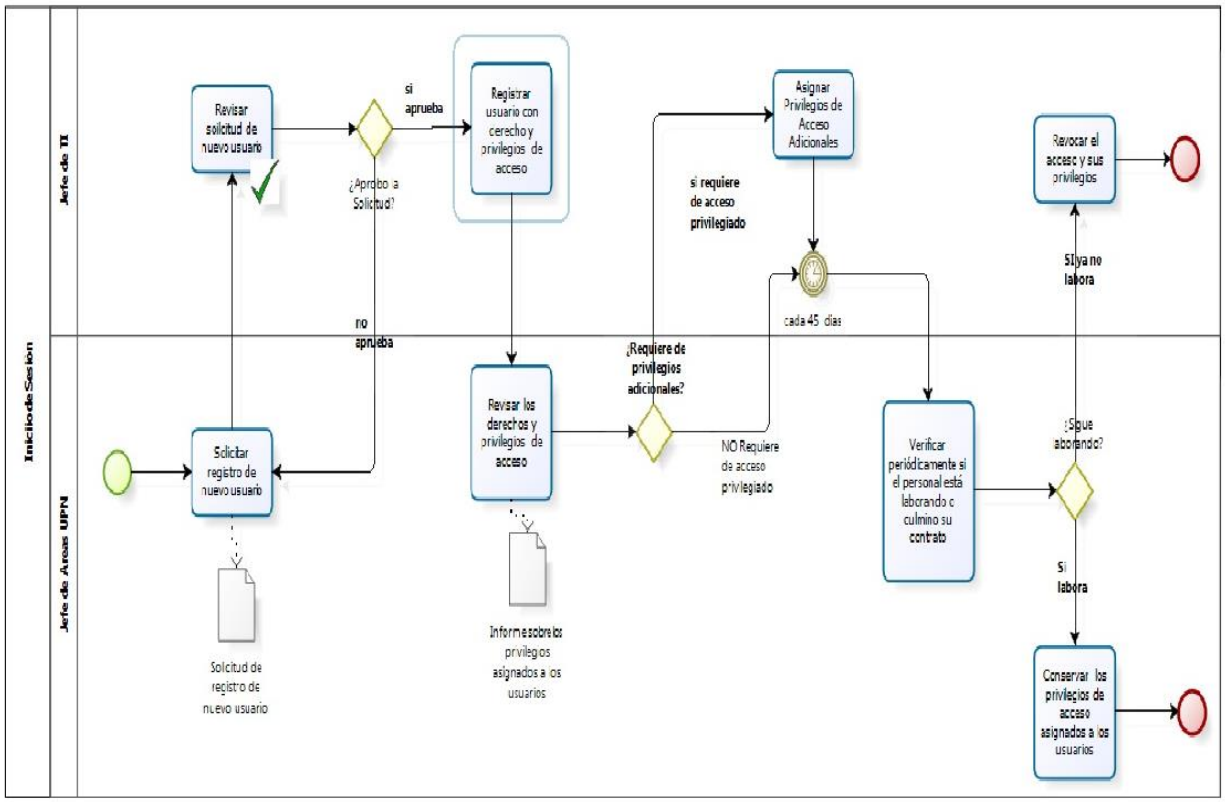
PROCEDIMIENTO SEGURO SOBRE LA GESTIÓN DE ACCESO DE USUARIOS

N° DE PROCEDIMIENTO	PROC-04
VERSIÓN ACTUAL V1.0	N° 1, DEL 5 DE DICIEMBRE DE 2017

I. Cooperaron en la elaboración de este procedimiento

- Jefes de las distintas áreas de la Unión Peruana del Norte (Jefe de área)
- Jefe del área e TI

II. Flujograma de información con sus listas de tareas



Solicitar registro de nuevo usuario
1. Solicitar Nuevo acceso para usuarios nuevos
2. Identificar los derechos de acceso de acuerdo a las funciones del usuario para su registro.
3. Aprobar los derechos de acceso asignados al usuario del área.

Registrar usuario con derecho y privilegios de acceso
1. Revisar el documento de funciones aprobado por el jefe de área
2. Verificar los derechos de acceso asignados al usuario.
3. Registrar el usuario mediante la conformidad del documento.
4. Verificar que su ID y contraseña cumpla con los requisitos requeridos por el sistema, si el ID creado es redundante o se asemeja con otro usuario.

Revisar los derechos y privilegios de acceso
1. Verificar qué los derechos de acceso cumpla con las funciones del usuario.
2. Realizar la segregación de funciones de acuerdo a lo que indica la

clasificación de la información y políticas de seguridad de la información
3. Revisar y Aceptar que los derechos de acceso no se activen hasta cumplir con las políticas de control de acceso.
4. Cumplir los roles mientras se encuentre en el mismo cargo dentro del área.
5. Revisar temporalmente los accesos de los usuarios asignados.
6. Mantener un registro de los documentos de los servicios y/o funciones de todos los usuarios.

Asignar Privilegios de Acceso Adicionales
1. Identificar los privilegios de acceso de los usuarios, de acuerdo a los sistemas a los cuales se encuentran asociados.
2. Mantener el proceso de autorización y registro que el área de TI brinda con todos los privilegios asignados.
3. Definir un cronograma que indique la fecha y el tiempo de utilidad, de los derechos de acceso privilegiados.
4. Asignar un identificador de usuario (ID) para los derechos de acceso privilegiado, distinto al usado en las actividades normales de negocio.
5. Revisar que los derechos de acceso privilegiado de los usuarios cumplan con sus funciones asignadas de acuerdo a las políticas de seguridad de la información.
6. Establecer que el ID de usuario mantenga la confidencialidad de la información cuando el usuario deje o sea removido de la organización.

Verificar periódicamente si el personal está laborando o culmino su contrato
1. Verificar en intervalos de tiempo que no existan acciones no autorizadas en las cuentas de acceso privilegiados.
2. Reasignar los derechos de accesos a los usuarios y acceso privilegiados cuando se haya cambiado de rol.
3. Registrar los cambios que se dieron en la revisión de las cuentas privilegiadas
4. Registrar el control detallado de las cuentas de usuario privilegiado de la organización

Revocar el acceso y sus privilegios
1. Revisar el periodo de contrato según lo estipulado para los usuarios de la organización
2. Según la revisión, que se ejecutó en los derechos de acceso se revoca los accesos al usuario, en caso que sea cambiado de área o rol se reasigna las nuevas funciones y las responsabilidades descritas.

Conservar los privilegios de acceso asignados a los usuarios
1. Revisar el periodo de contrato según lo estipulado para los usuarios de la organización
2. Según la revisión, que se ejecutó en los derechos de acceso se conserva los privilegios para los accesos del usuario.

III. Información general

Evento activador	Procedimiento seguro para la gestión de acceso de usuarios
Objetivo	Garantizar el acceso de usuario acreditados y autorizados a la información y evitar el acceso no autorizado a los sistemas y servicios de la Unión Peruana del Norte por parte de personal y terceros sin autorización.
Dueño	Jefe del área de TI y Jefes de las distintas áreas de la organización

IV. Roles participantes

- **Jefes de las distintas áreas de la Unión Peruana del Norte (Jefe de área):** Personal encargado de la dirección general de cada una de las distintas áreas de la Unión Peruana del Norte, y que llevará a cabo la solicitud de nuevos usuarios que formaran parte de sus áreas al cual ellos dirigen, esa solicitud se entregada al área de TI para su debida creación y habilitación de usuarios. Además los jefes de las distintas áreas de la Unión Peruana del Norte son los que verifican, aceptan y revisan los derechos de acceso de usuario que le fueron asignados a los trabajadores que laboraran en sus áreas.
- **Jefe del área e TI:** Encargado de la dirección general del área de TI de la Unión Peruana del Norte, además de ello brinda seguridad a la organización y acceso y conectividad a la red a los usuarios de la organización.

V. Descripción del flujo

N°	Actividad	Rol	Tareas	Documento
01	Solicitar registro de nuevo usuario	Jefe de áreas UPN	Solicitar Nuevo acceso para usuarios nuevos	Llenar documento de solicitud
02			Identificar los derechos de acceso de acuerdo a las funciones del usuario para su registro.	Documento detalladas de derecho de acceso del usuario
03			Aprobar los derechos de acceso asignados al usuario del área. Con	Aprobado con la firma y sello el documento de roles del usuario
04	Registrar usuario con derecho y privilegios de acceso	Jefe de área TI	Revisar el documento de funciones aprobado por el jefe de área	Informe de validación y registro de datos de los usuarios
05			Verificar los derechos de acceso asignados al usuario.	
06			Registrar el usuario mediante la conformidad del documento.	
07			Verificar que su ID y contraseña cumpla con los requisitos requeridos por el sistema, si el ID creado es redundante o se asemeja con otro usuario.	Informe indicando que se aceptó el registro del nuevo usuario.
08	Revisar los derechos y privilegios de acceso	Jefe de áreas UPN	Verificar qué los derechos de acceso cumpla con las funciones del usuario.	Informe que autorice los accesos por el propietario del sistema.
09			Realizar la segregación de funciones de acuerdo a lo que indica la clasificación de la información y políticas de seguridad de la información	Informe sobre las roles y funciones que realiza los usuarios.
10			Revisar y Aceptar que los derechos de acceso no se activen hasta cumplir con las políticas de control	

			de acceso.	
11			Cumplir los roles mientras se encuentre en el mismo cargo dentro del área.	
12			Revisar temporalmente los accesos de los usuarios asignados.	Llenar informe de seguimiento de accesos
13			Mantener un registro de los documentos de los servicios y/o funciones de todos los usuarios.	Registro de los documentos
14	Asignar Privilegios de Acceso Adicionales	Jefe de área TI	Identificar los privilegios de acceso de los usuarios, de acuerdo a los sistemas a los cuales se encuentran asociados.	Informe de asignación de privilegios por perfil de acuerdo al sistema asociado
15			Mantener el proceso de autorización y registro que el área de TI brinda con todos los privilegios asignados.	Registro de privilegios asignados
16			Definir un cronograma que indique la fecha y el tiempo de utilidad, de los derechos de acceso privilegiados.	Informe de vencimiento de derechos de acceso privilegiado
17			Asignar un identificador de usuario (ID) para los derechos de acceso privilegiado, distinto al usado en las actividades normales de negocio.	Informe de control de asignación de identificador de usuarios y derechos de accesos.
18			Revisar que los derechos de acceso privilegiado de los usuarios cumplan con sus funciones asignadas de acuerdo a las políticas de seguridad de la información.	Informe sobre las revisiones de derechos de acceso privilegiado
19			Establecer que el ID de usuario mantenga la confidencialidad de la información cuando el usuario deje o sea removido de la organización.	
20	Verificar periódicamente si el personal está laborando o culmino su contrato	Jefe de áreas UPN	Verificar en intervalos de tiempo que no existan acciones no autorizadas en las cuentas de acceso privilegiados.	Informe sobre las acciones no autorizada en las cuentas de acceso privilegiada
21			Reasignar los derechos de accesos a los usuarios y acceso privilegiados cuando se haya cambiado de rol.	Informe de cambios en las cuentas privilegiadas
22			Registrar los cambios que se dieron en la revisión de las cuentas privilegiadas	
23			Registrar el control detallado de las cuentas de usuario privilegiado de la organización	Documento de registro
24	Revocar el acceso y sus privilegios	Jefe de área TI	Revisar el periodo de contrato según lo estipulado para los usuarios de la organización	Informe sobre la retirada o la revocada de acceso a los usuarios
25			Según la revisión, que se ejecutó en los derechos de acceso se revoca los accesos al usuario, en caso que sea cambiado de área o rol se reasigna las nuevas funciones y las responsabilidades descritas.	
26	Conservar los privilegios de acceso asignados a los usuarios	Jefe de áreas UPN	Revisar el periodo de contrato según lo estipulado para los usuarios de la organización	Informe sobre conservación de los privilegios de acceso a los usuarios.
27			Según la revisión, que se ejecutó en los derechos de acceso se conserva los privilegios para los accesos del usuario.	

VI. Contingencias

Actividad 2: Registrar usuario con derecho y privilegios de acceso

Punto 7:

Uso de identificadores compartidos: Solo se debería permitir cuando fuera necesario por razones de negocio o de operación, además de ser aprobado y ser documentado

Actividad 3: Revisar los derechos y privilegios de acceso

Punto 11

Se bloquea temporalmente los derechos de acceso en caso no cumpla con los roles establecidos

Actividad 4: Asignar Privilegios de Acceso Adicionales

Punto 15

Los derechos de acceso privilegiado no deberían concederse hasta que se complete el proceso de autorización.

Punto 17

Las actividades normales del negocio no deben ser ejecutadas desde un identificador (ID) privilegiado

Punto 18

Cumplir con las funciones asignadas de derecho de acceso, que evite el uso no autorizado de la cuenta de usuario.

Punto 19

Permita modificar audazmente la contraseña que contenga información sensible de la organización, cuando un usuario haya sido despedido, cambiado o abandonado su centro laboral.

Actividad 5: Verificar periódicamente si el personal está laborando o culmino su contrato

Punto 23

Se debe revisar con mayor rango de frecuencia las autorizaciones de derechos de acceso privilegiado a los usuarios y verificar que no hayan obtenido privilegios no autorizados.

Actividad 6: Revocar el acceso y sus privilegios

Punto 25

En los casos de identificadores de grupo cuando un usuario deja la organización, se debe eliminar su identificador de todas las listas de acceso de grupos e informar a los demás usuarios que ya no compartan información con tal usuario.

VII. Historial de Revisiones

N° Versión	Fecha	Descripción de cambios
V1.0	5 de Diciembre de 2017	Primera versión

Anexo 28: Procedimiento para el seguro inicio de sesión a los Sistemas

UNION PERUANA DEL NORTE

Área de Tecnología de Información (TI)

UNIÓN PERUANA DEL NORTE

PROCEDIMIENTO

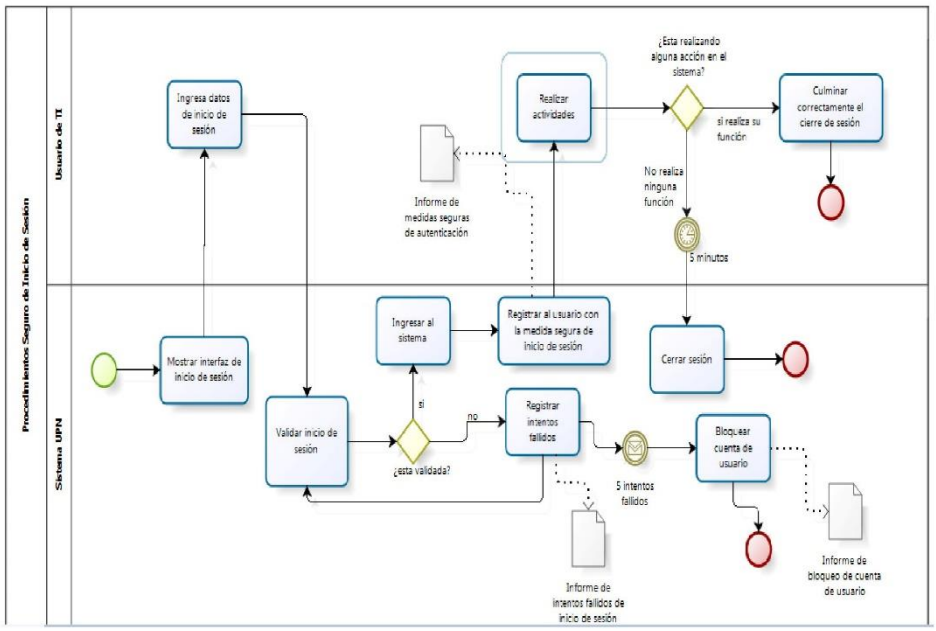
PROCEDIMIENTO PARA EL SEGURO INICIO DE SESIÓN A LOS SISTEMAS

N° DE PROCEDIMIENTO	PROC-05
VERSIÓN ACTUAL V1.0	N° 1, DEL 13 DE DICIEMBRE DE 2017

I. Cooperaron en la elaboración de este procedimiento

- Analistas desarrolladores de la Unión Peruana del Norte

II. Flujograma de información con sus listas de tareas



Actividad 1:

Ítem	Mostrar interfaz de inicio de sesión
01	Gestionar que los identificadores del sistema no se visualicen antes del inicio de sesión.
02	Gestionar un doble interfaz de inicio de sesión que permita acceder a usuarios autorizados por la organización.

Actividad 2

Ítem	Ingresar datos de inicio de sesión
03	Introducir los datos de usuario y contraseña correspondientes

Actividad 3:

Ítem	Validar inicio de Sesión
04	Denegar que la primera interfaz de inicio de sesión proporcione un link que permita la recuperación de código institucional.
05	Validar que los campos de entrada sean completados para su inicio de sesión.

Actividad 4:

Ítem	Registrar intentos fallidos
06	Almacena los intentos fallidos de inicio de sesión

Actividad 5:

Ítem	Bloquear cuenta de usuario
07	Bloquear la cuenta de usuario por un periodo determinado ante cualquier intento de acceso fallido en los inicios de sesión.
08	Almacena el usuario que ha sido bloqueado para la respectiva asignación de su acceso

Actividad 6:

Ítem	Ingresar al sistema
09	Acceso al sistema de acuerdo a los privilegios asignados

Actividad 7:

Ítem	Registrar al usuario con la medida segura de inicio de sesión
10	Almacena datos del inicio correcto de sesión
11	No guarda el usuario y contraseña en los equipos de sistemas de información.
12	Cifrar las contraseñas ante cualquier eventualidad de amenaza.

Actividad 8:

Ítem	Realizar Actividades
13	Realiza sus funciones normalmente

Actividad 9:

Ítem	Cerrar Sesión
14	Cerrar sesión de usuario cuando no se realice ninguna acción por un tiempo de inactividad.
15	Restringir el tiempo de conexión en las sesiones para su debido resguardo

Actividad 10:

Ítem	Culminar correctamente el cierre de sesión
16	Cierra sesión normalmente el sistema UPN

III. Información general

Evento activador	Procedimiento para el seguro inicio de sesión a los sistemas y/o aplicaciones de la organización
Objetivo	Prevenir el acceso no autorizado a los sistemas y aplicaciones implementado procedimientos seguros para un inicio de sesión eficaz y eficiente dentro de la organización
Dueño	Jefe del área de TI

IV. Roles y/o Actores participantes

Usuario de TI: Encargado de laborar dentro del área de tecnologías de información de la Unión Peruana del Norte, que cumple roles, según el perfil que ha sido asignado.

Sistemas UPN: Aplicaciones y/o sistemas de información desarrollado por los analistas desarrolladores de la Unión Peruana del Norte.

V. Descripción del flujo

Procedimientos Seguro de Inicio de Sesión				
ID	**Proceso**	**Rol**	**Actividades**	**Documento**
01	**Mostrar interfaz de inicio de sesión**	**Sistemas UPN**	Gestionar que los identificadores del sistema no se visualicen antes del inicio de sesión.	Informe que indique que se tiene una doble autenticación, una como organización y otro como área.
02			Gestionar un doble interfaz de inicio de sesión que permita acceder a usuarios autorizados por la organización.	
03	**Ingresar datos de inicio de sesión**	**Usuario de TI**	Introducir los datos de usuario y contraseña correspondientes	No genera documento
04	**Validar inicio de Sesión**	**Sistemas UPN**	Denegar que la primera interfaz de inicio de sesión proporcione un link que permita la recuperación de código institucional.	Informe de Validación de interfaces y autenticación de datos
05			Validar que los campos de entrada sean completados para su inicio de sesión.	
06	**Registrar intentos fallidos**	**Sistemas UPN**	Almacena los intentos fallidos de inicio de sesión	Informe de intentos fallidos de inicio de sesión
07	**Bloquear cuenta de usuario**	**Sistemas UPN**	Bloquear la cuenta de usuario por un periodo determinado ante cualquier intento de acceso fallido en los inicios de sesión.	Informe de bloqueo de cuenta de usuario
08			Almacena el usuario que ha sido bloqueado para la respectiva asignación de su acceso	
09	**Ingresar al sistema**	**Sistemas UPN**	Acceso al sistema de acuerdo a los privilegios asignados	No genera documento
10	**Registrar al usuario con la medida segura de inicio de sesión**	**Sistemas UPN**	Almacena datos del inicio correcto de sesión	Informe de medidas seguras de autenticación
11			No guarda el usuario y contraseña en los equipos de sistemas de información.	
12			Cifrar las contraseñas ante cualquier eventualidad de amenaza.	
13	**Realizar Actividades**	**Usuario de TI**	Realiza sus funciones normalmente	No genera documento
14	**Cerrar Sesión**	**Sistemas UPN**	Cerrar sesión de usuario cuando no se realice ninguna acción por un tiempo de inactividad.	Informe de inactividad de usuario en el sistema
15			Restringir el tiempo de conexión en las sesiones para su debido resguardo	Informe de restricción de tiempo de conexión
16	**Culminar correctamente el cierre de sesión**	**Usuario de TI**	Cierra sesión normalmente el sistema UPN	No genera documento

VI. Contingencias

Punto 2:
Inicio de sesión de manera segura: El primer acceso es mediante un código otorgado a los usuarios por la Unión Peruana de Norte, que al ingresar correctamente dicho código, le permita acceder a la segunda interfaz donde ingrese su usuario y contraseña del sistema.

Punto 3:
No mostrar contraseñas: Al ingresar las contraseñas no deberían mostrarles a personas o usuarios sin autorización.

Punto 5:
No mostrar Condición de error: Si ocurre alguna condición de error, el sistema no debería indicar en que parte del dato esta incorrecta o correcta.

Punto 6:
Intentos fallidos de inicio de sesión: Visualizar los intentos fallidos, cuando no se tuvo éxito para el inicio de sesión de manera segura.

Punto 7:
Bloqueo de cuenta de usuario: Ante 5 intentos fallidos o intento de fuerza bruta de inicio de sesión, el sistema debe bloquear por un periodo de 6 horas la cuenta de usuario.

Punto 10
Detalle de inicio de sesión segura: Si los datos de usuario son los correctos el sistema almacena la fecha y hora de inicio de sesión.

Punto 14:
Terminar sesión por inactividad: Si dentro del sistema no se desarrolla ninguna acción por cinco minutos dentro o fuera de la organización (áreas, lugares públicos o dispositivos móviles), automáticamente se cierra la sesión evitando que sea manipulado por terceros a la Unión Peruana de Norte.

VII. Historial de Revisiones

N° Versión	Fecha	Descripción de cambios
V1.0	13 de Diciembre de 2017	Primera versión

Anexo 29: Inventariado de Activos

INVENTARIADO DE ACTIVOS

Grupo de Activo	Código	Nombre del Activo	Descripcion del activo	Propietario	Custodio Técnico	Tipo de Activo	Acceso	Ubicación	Atributos de Clasificación	Valor		
										C	I	D
Hardware Equipos portátiles	AF01	Equipos portátiles (Laptops y Notebook) Cantidad: 5	1 Notebook Dell serie 3000 14" Core i5 1 Laptop Mac book 1 Laptop Latitude 5470 – i5 8 GB 1 TB HD 2 Laptops Latitude E5470 – i7 16 GB 1 TB FHD	Área de TI	Ing. Carlos Saavedra (Jefe de TI) Amelio Apaza Janeth Tenorio Fernando Lazo	Hardware (Activo Físico)	Lectura, Consulta, Escritura	Área de TI (3er piso)	ACL2,ACL3,ACL4	Alta	Alta	Muy Alta
Hardware Equipos Fijos Servidores	AF02	CPU – Servidor	Servidor de correo Power edge R720	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura, Consulta, Escritura	Sede – Data Center Sótano	ACL1,ACL2,ACL3,ACL4	Muy Alta	Muy Alta	Muy Alta
	AF03	CPU – Centro de Datos	Server HP Proliant DL 4 Core 2.4 GZ free BSD	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura, Consulta, Escritura	Sede – Data Center Sótano	ACL1,ACL2,ACL3,ACL4	Muy Alta	Muy Alta	Muy Alta
	AF04	Servidor de Base de datos	Servidor Dell Poweredge R630	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura, Consulta, Escritura	Sede – Data Center Sótano	ACL1,ACL2,ACL3,ACL4	Muy Alta	Muy Alta	Muy Alta
	AF05	Servidor de Archivos	Servidor Dell Poweredge R630	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura, Consulta, Escritura	Sede – Data Center Sótano	ACL2,ACL3,ACL4	Muy Alta	Muy Alta	Muy Alta
	AF06	Servidor Firewall	Servidor Dell Poweredge R230	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura, Consulta, Escritura	Sede – Data Center Sótano	ACL1,ACL2,ACL3,ACL4	Muy Alta	Muy Alta	Muy Alta
	AF07	Servidor Cantidad: 2	2 Servidores Packcable HP Proliant DL 160 GB Intel	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura, Consulta	Sede – Data Center Sótano	ACL2,ACL3,ACL4	Alta	Alta	Muy Alta
	AF08	Servidor	Servidor HP Proliant DL 120 GB 6 Intel XEON 343	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura, Consulta	Sede – Data Center Sótano	ACL2,ACL3,ACL4	Alta	Alta	Muy Alta
	AF09	CPU - Servidor	Servidor Central Telefónica	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura, Consulta	Sede – Data Center Sótano	ACL2,ACL3,ACL4	Alta	Alta	Muy Alta
	AF10	Servidor DHCP	Servidor Dell Poweredge R230	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura, Consulta, Escritura	Sede – Data Center Sótano	ACL2,ACL3,ACL4	Alta	Alta	Muy Alta
	AF11	Servidor Web	Servidor Dell Poweredge R230	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura, Consulta, Escritura	Sede – Data Center Sótano	ACL2,ACL3,ACL4	Alta	Alta	Muy Alta
	AF12	Servidor Redundante	Servidor Dell Poweredge Intel xeon	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura, Consulta	Sede – Data Center Sótano	ACL2,ACL3,ACL4	Alta	Alta	Muy Alta
	AF13	Servidor Redundante	Servidor Dell Power Intel	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura, Consulta	Sede – Data Center Sótano	ACL2,ACL3,ACL4	Alta	Alta	Muy Alta
Hardware Equipos Fijos Equipo Control de Asistencia	AF14	Equipo de control de asistencia	Equipo Hardware para el control de asistencias del personal	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura, Consulta, Escritura	Sala de cómputo	ACL2,ACL3,ACL4	Media	Media	Alta
Hardware Equipos Fijos Cámaras	AF15	Cámara de video vigilancia	Cámaras de video/01 Switch vigilancia	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura, Consulta	Sede – Data Center Sótano	ACL2,ACL3,ACL4	Alta	Alta	Muy Alta
Hardware Equipos Fijos Medios para almacenamiento de datos	AF16	Disco duro – HD	Disco duro externo wster digital	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura	Sede – Data Center Sótano	ACL2,ACL3,ACL4	Alta	Alta	Muy Alta
Hardware Equipos Fijos Estabilizador y Grupo Electrógeno	AF17	Estabilizador - UPS	UPS TRIPP SmarthOnLine servidores	Infraestructura	Arq. Karen Cruzado	Hardware (Activo Físico)	No Aplica	Sótona (Cuarto UPS)	ACL2,ACL3	Baja	Baja	Alta
	AF18	Grupo electrógeno	Transformador de aislamiento de 12 KVA flash Power	Infraestructura	Arq. Karen Cruzado	Hardware (Activo Físico)	No Aplica	Sótona (Cuarto UPS)	ACL2,ACL3	Baja	Baja	Alta

Hardware Equipos Fijos Medios (Accesorios de Informática)	AF19	Switch General Corp.	Switch Dell networking N3048P	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura, Consulta	Sede – Data Center Sótano	ACL1,ACL2,ACL3,ACL4	Muy Alta	Muy Alta	Muy Alta
	AF20	Switches – Accesorios de Informática Cantidad: 8	1 switch Power connect 6224P puertos GbE conmutador Admin 1 switch dlink DES 1210 19" para telefonía 4 switches Dell networking N1524P 2 switches D-Link web Smart	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura, Consulta	Sede – Data Center Sótano Sala de cómputo	ACL2,ACL3,ACL4	Media	Media	Alta
	AF21	Accesorio informática	Kit de transmisión simple y 2 consolas 8 canales	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	No Aplica	Sala de cómputo	ACL2,ACL3,ACL4	Baja	Baja	Media
	AF22	Lector de código de barras	Lector código de barras Heron D130 black USB ki	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura,Consulta	Área de TI (3er piso)	ACL2,ACL3,ACL4	Baja	Baja	Media
	AF23	Amplificadores Cantidad: 2	1 Amplificador Ecualizador 2bx 1215 0101590 con cables 1 Amplificador Compreso SBX 166 cables	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	No Aplica	Sala de cómputo	ACL2,ACL3,ACL4	Baja	Baja	Media
	AF24	Adaptador	Adaptador de video Kramer 4x1 VGA mechanical Sh	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	No Aplica	Sala de cómputo	ACL2,ACL3,ACL4	Baja	Baja	Media
	AF25	IPAD	IPAD MAT Apple	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura,Consulta,Escritura	Sala de cómputo	ACL2,ACL3,ACL4,ACL5	Baja	Baja	Media
	AF26	Impresoras Cantidad: 3	1 impresora Epson Matricial LX300+II 1 impresora Epson TMU – 220A ticketera 1 ticketera impresora inmovilizado	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura	Área de TI (3er piso) Sala de cómputo	ACL2,ACL3,ACL4	Baja	Baja	Media
	AF27	Monitores Cantidad: 7	1 Monitor Led Samsung 20" VGA S20A300N interfaz 1 Monitor Led Samsung 20" vga 1 Monitor DELL P2317H - HBGBPB2 1 Monitor DELL P2317H - 5BGBPB2 1 Monitor DELL P2317H - DBGBPB2 1 Monitor DELL P2317H - 9BGBPB2 1 Monitor DELL P2317H - 8BGBPB2	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura	Área de TI (3er piso) Sala de cómputo	ACL2,ACL3,ACL4	Baja	Baja	Media
	AF28	Proyector	Proyector Epson power Lite 4200	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	Lectura	Área de TI (3er piso)	ACL2,ACL3,ACL4	Muy Baja	Muy Baja	Media
	AF29	Micrófono inalámbrico	Micrófono shure GGX 24E	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Hardware (Activo Físico)	No Aplica	Sala de cómputo	ACL2	Muy Baja	Muy Baja	Baja
Hardware Equipos Fijos Aire Acondicionado	AF30	Aire acondicionado	Aire acondicionado Split	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Activo Físico	No Aplica	Sala de cómputo	ACL2	Muy Baja	Muy Baja	Media
Muebles	AF31	Muebles Cantidad: 4	1 silla operativa Global UPHOLSTERY-MOD. MESH TEA negro 1 Closet con puertas grande con 4 divisiones 1 Escritorio con cajonera en T modular dos personas 1 silla de visita BR-1061VC01 Modelo variety negro	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Activo Físico	No Aplica	Área de TI (3er piso)	ACL2	Muy Baja	Muy Baja	Baja
Red y Conectividad	ARC01	Red y conectividad	Conexiones certificadas para la instalación	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Red y Físico	Lectura, Consulta, Escritura	Área de TI (3er piso)	ACL1,ACL2,ACL3,ACL4	Muy Alta	Muy Alta	Muy Alta
Software Información	AS01	Base de datos	Gestor de Base de datos Oracle	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Activo Software	Lectura, Consulta, Escritura	Área de TI (3er piso)	ACL1,ACL2,ACL3,ACL4	Muy Alta	Muy Alta	Muy Alta
Software Copias de Respaldo	AS02	Back Up	Copia de respaldo de base de datos	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Activo Software	Lectura, Escritura	Área de TI (3er piso)	ACL1,ACL2,ACL3,ACL4	Muy Alta	Muy Alta	Muy Alta
	AS03	Back Up	Copia de respaldo de software	Área de TI	Janeth tenorio (Analista de sistemas) Amelio Apaza (Analista de sistemas)	Activo Software	Lectura, Escritura	Área de TI (3er piso)	ACL1,ACL2,ACL3,ACL4	Muy Alta	Muy Alta	Muy Alta
Software Licencias	AS04	Licencias software	Licencia Antivirus GData versión 2017	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Activo Software	Consulta	Área de TI (3er piso)	ACL2,ACL4	Alta	Alta	Alta
	AS05	Licencias software	Licencia Software Microsoft	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Activo Software	Consulta	Área de TI (3er piso)	ACL2,ACL4	Baja	Baja	Media
	AS06	Licencias software	Licencia Adobe Creative Cloud versión 2017	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Activo Software	Consulta	Área de TI (3er piso)	ACL2,ACL4	Baja	Baja	Media
Software Sistemas	AS07	Sistema DSA	Software que le asigna la iglesia al área de TI	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Activo Software	Lectura, Consulta, Escritura	Área de TI (3er piso)	ACL1,ACL2,ACL3,ACL4	Alta	Alta	Alta
	AS08	Sistema UPN - Académico	Sistema que se brinda a los colegios perteneciente a la iglesia	Área de TI	Janeth Tenorio (Analista de sistemas)	Activo Software	Lectura, Consulta, Escritura	Área de TI (3er piso)	ACL1,ACL2,ACL3,ACL4	Alta	Alta	Alta
	AS09	Sistema UPN - Gerencial	Sistema que se brinda a misiones y gerencias de la iglesia	Área de TI	Amelio Apaza (Analista de sistemas)	Activo Software	Lectura, Consulta, Escritura	Área de TI (3er piso)	ACL1,ACL2,ACL3,ACL4	Alta	Alta	Alta
Software Software Control de Asistencia	AS10	Software Control de Asistencia	Software control de asistencia Premium para el registro de asistencias del personal del área de TI	Área de TI	Ing. Carlos Saavedra (Jefe de TI)	Activo Software	Lectura, Consulta, Escritura	Área de TI (3er piso)	ACL2,ACL3,ACL4	Media	Baja	Alta
Personal Persona a cargo de Toma de decisiones y Analistas de Sistemas	AP01	Jefe de TI	Brinda seguridad al área de TI e infraestructura	Jefe de TI	No Aplica	Personal	No Aplica	Área de TI (3er piso)	ACL2,ACL3,ACL4	Alta	Alta	Muy Alta
	AP02	Analista de sistema académico	Realiza el análisis y desarrollo de los sistemas académicos	Analista de sistema académico	No Aplica	Personal	No Aplica	Área de TI (3er piso)	ACL2,ACL3,ACL4	Alta	Alta	Muy Alta
	AP03	Analista de sistema gerencial	Realiza el análisis y desarrollo de los sistemas gerenciales	Analista de sistema gerencial	No Aplica	Personal	No Aplica	Área de TI (3er piso)	ACL2,ACL3,ACL4	Alta	Alta	Muy Alta
Documentos de Papel e Información	ADP01	Contratos	Documento de compromiso del personal de trabajo	Área de Talento Humano y Legales	Omar Campos Martin Saldaña	Documentos de papel	Lectura, Consulta	Área de Talento Humano y Legales (3er piso)	ACL2,ACL3,ACL4	Alta	Baja	Baja
	AI001	Manuales de Usuario	Documento que brinda asistencia técnica a los usuarios que usan los sistemas de información	Área de TI	Janeth Tenorio (Analista de sistemas) Amelio Apaza (Analista de sistemas)	Información	Lectura, Consulta	Área de TI (3er piso)	ACL2,ACL4	Media	Media	Alta
Servicio	AS01	Helpdesk	Brindar soporte y mantenimiento	Fernando Lazo	No Aplica	Servicio	No Aplica	Área de TI – mesa de soporte (3er piso)	ACL2,ACL3,ACL4	Baja	Baja	Alta
	AS02	Videoconferencia	Charlas o capacitaciones que se obtiene del exterior o local	Fernando Lazo	No Aplica	Servicio	No Aplica	Sala de reuniones	ACL2,ACL3,ACL4	Baja	Baja	Media

Anexo 30: Guía de Clasificación de la información

Guía de Clasificación de la Información

UNIÓN PERUANA DEL NORTE

ÁREA DE TECNOLOGÍA DE INFORMACIÓN

2017

Objetivo de la Clasificación de la información

Asegurar que la información reciba los niveles de protección apropiados para su debido resguardo y correcto manejo de la información.

Alcance

El Proceso de clasificar la información se aplica para todos los propietarios de cada uno de los activos de información del área de TI.

Responsabilidades

Todos los propietarios de los activos de información, deben conocer y poner en práctica las disposiciones dadas en el presente documento.

Definición

Información: "Datos dotados de significado y propósito. Datos relacionados que tienen significado para la Entidad" (Profesional Grupo de AE y del SGI, 2014)
Activos de Información: "Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización." (Parra, 2016)
Propietario: "Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso" (MINTIC, 2016)
Nivel de Clasificación de Activos de información: "Es el valor asignado por el dueño del activo de Información teniendo en cuenta las propiedades de Seguridad de la Información" (Profesional Grupo de AE y del SGI, 2014)
Custodio: "Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. " (MINTIC, 2016)
Usuario: "Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información" (MINTIC, 2016)

Clasificación de la Información

Según (ISOTools Excellence, 2017), "Se debe clasificar la información para indicar la necesidad, las prioridades y el nivel de protección previsto para su tratamiento. La información tiene diversos grados de sensibilidad y criticidad. Algunos ítems podrían requerir niveles de protección adicionales o de un tratamiento especial**.** Debe utilizarse un esquema de clasificación de la información para definir el conjunto adecuado de niveles de protección y comunicar la necesidad de medidas especiales para el tratamiento**.**"
La norma ISO 27001 no establece niveles concretos para la clasificación de la información, sino que esta la debiese hacer cada empresa en base a sus necesidades de negocio y requisitos. legales. (ISOTools Excellence, 2017)

Análisis sobre los requisitos de información en base a su confidencialidad, integridad y disponibilidad para su evaluación.

Este análisis sobre los requisitos de información nos detalla el valor que tiene cada activo para la organización, donde se los valora en base a un rango de evaluación de 4 niveles que va desde Baja hasta Muy Alta, además de esto se los evalúa bajo un nivel de atribución de clasificación,

lo cual permitirá darles un tratamiento adecuado para el manejo de la información, en la tabla 1 se muestra el criterio y descripción de la escala de evaluación en base a la confidencialidad, integridad y disponibilidad de la información por cada activo.

Tabla 1:
Rango de Evaluación en base a la Confidencialidad de la Información

Confidencialidad		
Criterio	**Descripción**	**Significado**
MA	Muy Alta	Altamente Restringida
A	Alta	Restringida
M	Media	Uso Interno
B	Baja	Pública

Fuente: elaboración propia

Tabla 2:
Rango de Evaluación en base a la Integridad de la Información

Integridad		
Criterio	**Descripción**	**Significado**
MA	Muy Alta	No se puede reparar, por lo que ocasionaría pérdidas grandes
A	Alta	Es difícil su reparación y podría causar pérdidas significativas
M	Media	Se puede reparar aunque se podría percibir algunas pérdidas
B	Baja	Se puede reparar con facilidad

Fuente: elaboración propia

Tabla 3:
Rango de Evaluación en base a la Disponibilidad de la Información

Disponibilidad		
Criterio	**Descripción**	**Significado**
MA	Muy Alta	La falta de la inaccesibilidad a la información afecta negativamente a la organización
A	Alta	Durante un periodo no menor a un día podría causar pérdidas significativas
M	Media	La falta de la inaccesibilidad a la información impacta de forma leve el proceso
B	Baja	La falta de la inaccesibilidad a la información no afecta ni tiene un impacto negativo en el área de TI

Fuente: elaboración propia

En la tabla 2 se muestra el código de atributo de clasificación con su respectiva descripción

Tabla 4:
Atributos de Clasificación

Código Atributo de Clasificación	**Descripción**
ACL1	Información que es de mucha importancia por su valor y criticidad para la organización y para sus operaciones internas
ACL2	Información que está restringido a terceros(personal externas a la organización)
ACL3	Información que está restringido a un personal limitado que no labora en el área de TI, pero que labora dentro de la organización.
ACL4	Información que puede ser alterada para corrupción y/o fraudes que perjudiquen a la organización como a sus operaciones.
ACL5	Información que es de conocimiento público tanto para el personal interno o personas externas a la organización.

Fuente: elaboración propia

Niveles de Clasificación adoptada por el área de TI de la UPN

Los niveles de clasificación adoptados por el área de TI de la UPN son los siguientes:

Pública: En este nivel de clasificación cualquier usuario externo o interno de la organización pueden tener acceso a la información sin restricción a ello.

Uso Interno: Es utilizada por un área en específica y no puede ser conocida por terceros sin la autorización del propietario. En caso de ser requerida por un tercero, se debiese solicitar un permiso al encargado o propietario de la información para poder acceder a ella, detallando los puntos por los cuales se desea solicitar dicha información, este mismo proceso se realiza en caso un usuario de otra área de la organización, quisiese acceder a la misma información.

Restringida: Es utilizada por un limitado número de usuarios de un área en específica y no puede ser conocida por otras áreas sin autorización del propietario. En este caso la información no puede ser compartida a terceros sin o con autorización, esto por el grado de importancia y criticidad que esta posee.

Altamente Restringida: Es utilizada por alta gerencia y no pueden ser conocidas por otras áreas o usuarios y/o terceros sin o con autorización. Este tipo de clasificación de la información es la que posee el mayor grado de criticidad e importancia, y su alteración o modificación y/o exposición ocasionaría grandes pérdidas que pudiesen perjudicar a la organización como a sus operaciones y negocios.

Encargado de la Clasificación de los activos priorizados

- ✓ **Activos priorizados – Propietario (Custodio técnico)**

Activo	Custodio técnico
Equipos portátiles	Ing. Carlos Saavedra (Jefe de TI)
CPU – Servidor de correo Power edge R720	Ing. Carlos Saavedra (Jefe de TI)
CPU – Centro de Datos	Ing. Carlos Saavedra (Jefe de TI)
Servidor de Base de datos	Ing. Carlos Saavedra (Jefe de TI)
Servidor de Archivos	Ing. Carlos Saavedra (Jefe de TI)
Servidor Firewall	Ing. Carlos Saavedra (Jefe de TI)
2 Servidores Packcable HP Proliant DL 160 GB Intel	Ing. Carlos Saavedra (Jefe de TI)
Servidor HP Proliant DL 120 GB 6 Intel XEON 343	Ing. Carlos Saavedra (Jefe de TI)
Servidor Central Telefónica	Ing. Carlos Saavedra (Jefe de TI)
Servidor DHCP	Ing. Carlos Saavedra (Jefe de TI)
Servidor Web	Ing. Carlos Saavedra (Jefe de TI)
Servidor Redundante Dell Poweredge Intel xeon	Ing. Carlos Saavedra (Jefe de TI)
Servidor Redundante Dell Power Intel	Ing. Carlos Saavedra (Jefe de TI)
Equipo de control de asistencia	Ing. Carlos Saavedra (Jefe de TI)
Cámara de video vigilancia	Ing. Carlos Saavedra (Jefe de TI)
Disco duro – HD	Ing. Carlos Saavedra (Jefe de TI)
Estabilizador - UPS	Arq. Karen Cruzado
Grupo electrógeno	Arq. Karen Cruzado
Red y conectividad	Ing. Carlos Saavedra (Jefe de TI)
Switch General Corp.	Ing. Carlos Saavedra (Jefe de TI)
Switches – Accesorios de Informática Cantidad: 8	Ing. Carlos Saavedra (Jefe de TI)
Gestor de Base de datos Oracle	Ing. Carlos Saavedra (Jefe de TI)
Copia de respaldo de base de datos	Ing. Carlos Saavedra (Jefe de TI)
Copia de respaldo de software	Janeth tenorio (Analista de sistemas) Amelio Apaza (Analista de sistemas)
Licencia Antivirus GData versión 2017	Ing. Carlos Saavedra (Jefe de TI)
Sistema DSA	Ing. Carlos Saavedra (Jefe de TI)
Sistema UPN - Académico	Janeth Tenorio (Analista de sistemas)
Sistema UPN - Gerencial	Amelio Apaza (Analista de sistemas)
Software Control de Asistencia	Ing. Carlos Saavedra (Jefe de TI)
Jefe de TI	No aplica
Analista de sistema académico	No aplica
Analista de sistema gerencial	No aplica

Contratos	Omar Campos Martin Saldaña
Manuales de Usuario	Janeth Tenorio (Analista de sistemas) Amelio Apaza (Analista de sistemas)
Helpdesk	Fernando Lazo

Manejo y Tratamiento de activo de información

La clasificación de los activos de información del área de TI de la UPN define un manejo y tratamiento del activo de información en base a:

- Etiquetado
- Métodos de distribución de la información recomendados
- Almacenamiento y archivado
- Eliminación
- Transmisión oral
- Seguridad física
- Fotocopiado de la información

Políticas definidas para la clasificación

Ver manual de políticas de seguridad de la información donde se establece las normas y puntos necesarios para la debida clasificación de la información, esto para su correcto manejo de la información.

1. **Procedimiento de Clasificación para los diferentes niveles de clasificación adoptado por el área de TI**

En la Imagen 1 se visualiza el procedimiento de clasificación para los diferentes niveles de clasificación adoptados por el área de TI.

	Nivel de Clasificación			
	Pública	Uso Interno	Restringida	Altamente Restringida
Definición	En este nivel de clasificación todas las personas pueden tener acceso a la información sin restricción a ello.	Es utilizada por un área en especifica y no puede ser conocida por terceros sin la autorización del propietario. En caso de ser requerida por un tercero, se debiese solicitar un permiso al encargado o propietario de la información para poder acceder a ella, detallando los puntos por los cuales se desea solicitar dicha información, este mismo proceso se realiza en caso un usuario interno de la organización, quisiese acceder a la	Es utilizada por un limitado número de usuarios de un área en especifica y no puede ser conocida por otras áreas sin autorización del propietario. En este caso la información no puede ser compartida a terceros sin o con autorización, esto por el grado de importancia y criticidad que esta posee.	Es utilizada por alta gerencia y no pueden ser conocidas por otras áreas o usuarios y/o terceros sin o con autorización. Este tipo de clasificación de la información es la que posee el mayor grado de criticidad e importancia, y su alteración o modificación y/o exposición ocasionaría grandes pérdidas que pudiesen perjudicar a la organización como a sus operaciones y negocios.
Rango de evaluación	Baja	Media	Alta	Muy Alta
Atributo de Clasificación	ACL5	ACL2	ACL2,ACL3	ACL1,ACL2,ACL3,ACL4
Acceso Privilegiado	Todos(Cualquier persona, ya sea interna o externa a la organización)	Todos los usuarios del área de TI, solo en el caso de terceros y usuarios de otras áreas, necesitan la autorización mediante una solicitud enviada al propietario de la información para su manejo.	Número limitado de usuarios del área de TI, en el caso lo solicitasen otras áreas es firmando un compromiso de confidencialidad y de no divulgación de la información.	Alta gerencia de la organización y usuarios acreditados
ID de clasificación de la información	CLA-01	CLA-02,CLA-03,CLA-04,CLA-05,CLA-06	CLA-07,CLA-08,CLA-09	CLA-10,CLA-11

Etiquetado				
Documentos especiales	No es requerido para su uso	No es solicitado, esta en la disposición del propietario de la información si es que lo hace. En caso de etiquetarse, si un documento se hubiese impreso y no poseyese en ello un campo de Nivel de confidencialidad, se le deberá etiquetar con una sello en referencia a su clasificación en sus primeras hojas.	Es de obligación del propietario de la información etiquetarlo. Si un documento se hubiese impreso y no poseyese en ello un campo de Nivel de confidencialidad, se le deberá etiquetar con un sello y firma en referencia a su clasificación en sus primeras hojas	Es de obligación del propietario de la información etiquetarlo. Si un documento se hubiese impreso y no poseyera un campo de Nivel de confidencialidad, se le deberá etiquetar con un firma y sello de alta gerencia en referencia a su clasificación en sus primeras hojas
Archivos electrónicos (Texto, Word, Excel, imágenes, etc.)	No es requerido para su uso	No es solicitado, queda a disposición del propietario de la información si es que lo hace. En caso de que se etiqueten los documentos o información que se encuentren en archivos electrónicos, se les debiese añadir un campo de información que mostrase el nivel de clasificación y que hagan parte de los formatos manejados	Si es de obligación del propietario de la información realizarlo. Los documentos o información que se encuentren en archivos electrónicos, se les debiese añadir un campo de información que mostrase el nivel de clasificación y que hagan parte de los formatos manejados	Si es de obligación del propietario de la información realizarlo. Los documentos o información que se encuentren en archivos electrónicos, se les debiese añadir un campo de información que mostrase el nivel de clasificación en referencia a alta gerencia, y que hagan parte de los formatos manejados
Aplicaciones	No es requerido para su uso	No es solicitado, queda a disposición del propietario de la información si es que lo hace. En caso de que se etiqueten, los sistemas o aplicaciones que guarden y procesen información, se le debiese añadir un cuadro de mensaje donde se visualice su nivel de clasificación	Si es de obligación del propietario de la información realizarlo. Los sistemas o aplicaciones que guarden y procesen información, se le debiese añadir un cuadro de mensaje donde se visualice su nivel de clasificación	Si es de obligación del propietario de la información realizarlo. Los sistemas o aplicaciones que guarden y procesen información relacionada a alta gerencia, se le debiese añadir un cuadro de mensaje donde se visualice su nivel de clasificación
Método de distribución recomendado				
Internamente	Esta información es de libre distribución tanto para personal interno como externo	Electrónica: Mediante el sistema de correo electrónico brindado a la secretaria u otras áreas de la organización, además del sistema de correo electrónico del área de TI. Esta información no puede estar almacenada en dispositivo de almacenamiento externo como: USB, CD, Disco duros, memorias, etc. Física: Proceso de uso de correspondencia interna.	Electrónica: Únicamente mediante el sistema de correo electrónico del área de TI. Esta información no puede estar almacenada en dispositivo de almacenamiento externo como: USB, CD, Disco duros, memorias, etc. Física: Proceso de uso de correspondencia interna, comprobando que el destinatario, es un usuario acreditado para el manejo de informes networking de la organización o copias de Backup, de otra manera se solicita la autorización por medio del propietario de la información	Electrónica: Solo en la red correspondiente a alta gerencia de la UPN, los archivos deben estar protegidos mediante el cifrado, esta entrega se hace únicamente a un destinatario acreditado. Física: La entrega se realiza directamente, con la firma y sello de recepción personal requerida no transferible, dado directamente por el propietario de la información.
hacia terceros	Al igual que al método de distribución interno, es de libre distribución tanto para el personal interno como a terceros	Debe ser proporcionado a un tercero, solo en el caso que fuese para un estudio o investigación, obligación contractual o en tal caso para un negocio, esto con la previa autorización del propietario de la información. Electrónica: Si se le hace llegar archivos o informes, estos debe tener acceso de lectura únicamente, este envío se debe realizar con cuentas de correos electrónicos ajenos a la organización. Física: Se recomienda realizar la entrega por medio de documentos, el menor numero de copias que sea posible, y únicamente al receptor acreditado, firmando un compromiso de que recibió la información.	La información no puede ser compartida a terceros	La información no puede ser compartida a terceros
Almacenamiento y archivado				
Información impresa	No necesita prevención o resguardo especial	Se debe asegurar el seguimiento de las acciones de personas externas(terceros) en las áreas de trabajo o instalaciones	Se debe archivar en áreas seguras bajo un debido resguardo	Se debe archivar en áreas seguras bajo llaves o medios de identificación. Cada vez que se archivase se debiese asegurar que no fuese vista por personas externas o internas a la organización.
Información electrónica	No necesita prevención o resguardo especial	Puede ser almacenada en algún repositorio o sistema y cuando se cerciore que no es accesible a terceros por fuera de las redes y sistemas de información del área de TI.	Debe ser almacenada en repositorios o sistemas, estrictamente controlados y administrados donde se comparta la información. Esta en la obligación de autenticarse mediante ingreso de usuario y contraseña. Debe evitarse almacenar este tipo de información en equipos que no posean administración formal de seguridad.	Los controles obligatorios sugeridos para la información por medio digital son: autenticación con usuario y password al sistema donde se retiene la información, esta información debiese encontrarse cifrada para su debido resguardo. Si esta información se encontrase en equipos portátiles o de escritorio, solo deben tener acceso personas autorizadas aplicando autenticación fuerte de mínimo dos factores.
e-mail	No necesita prevención o resguardo especial	Se debe cerciorar que esta información no sea enviada a personas externas a la organización(terceros) sin autorización para obtenerla por este medio	Se recomienda de que la información no se quede guardada en la lista de mensajes enviados, además que la copia de respaldo del correo electrónico se desarrolle de manera eficiente y segura	Se debe obviar en lo posible la utilización de este medio, solo si es que fuese de mucha urgencia se debiese manejar por medio de certificados digitales.

Eliminaciòn				
Información impresa	No ostenta prevención alguna	No necesita precaución alguna	Se recomienda el uso de equipos para la destrucción de papel y documentos.	Se recomienda el uso de equipos para la destrucción de papel y documentos, esta acción debe ser supervisada por el propietario del activo de información.
Reciclaje de papel	Es autorizado sin impedimento	Es permitido únicamente para uso interno	No se permite este medio de destrucción	No se permite este medio de destrucción
Medios de almacenamiento	No ostenta prevención alguna	Eliminación o borrado seguro de la información, destrucción física de medios que serán desechados.	Eliminación o borrado seguro de la información, destrucción física de medios que serán desechados.	Eliminación o borrado seguro de la información, destrucción física de medios que serán desechados.
Transmisión Oral				
Conversaciones y reuniones	No muestra precaución alguna	Se debe obviar referenciar esta información por fuera de las instalaciones de la organización, y cuando sean realizadas deben realizarse en voz baja y no llamando la atención, y sobre todo evitarlo en zonas de libre acceso.	Se debe obviar referenciar esta información por fuera de las instalaciones de la organización, al menos que fuese una reunión formal por fuera de las mismas. No se debiese reunir en salones en salones de fácil acceso y que no permitan aislar el ruido. Si la información fuese escrita o redactada en medios físicos como; pizarras o papelotes, estas debiesen ser borradas o desechadas sea el caso, cuando esta reunión culminase y cuando abandonasen los salones donde se tuvo dicha reunión.	Se debe obviar referenciar esta información por fuera de las instalaciones de la organización, al menos que fuese una reunión formal por fuera de las mismas. No se debiese reunir en salones de fácil acceso y que no permitan aislar el ruido. Si la información fuese escrita o redactada en medios físicos como; pizarras o papelotes, estas debiesen ser borradas o desechadas sea el caso, cuando esta reunión culminase y cuando abandonasen los salones donde se tuvo dicha reunión.
telefónica	No muestra precaución alguna	No se debiese proporcionar información de uso interno por este medio a terceros sin autorización	Evitar de la mejor manera posible establecer conversaciones por vía telefónica en zonas públicas, en caso se transmita la información por este medio debiese ser en zonas seguras y aisladas al público y personal no autorizado	Evitar a toda costa establecer conversaciones por vía telefónica en zonas públicas y de libre tránsito, en caso se transmita la información por este medio debiese ser en zonas seguras y aisladas al público y personal no autorizado como: salas de reuniones u oficinas
Seguridad Física				
Estaciones de trabajo	Se debe tener un riguroso control de vigilancia para el retiro de estaciones de trabajo por fuera de las instalaciones de trabajo	Se solicita bloquear y/o obstruir los equipos tecnológicos con protección de passwords apenas se prescinda, e incluso poseer un protector de pantalla que bloque el equipo cuando este en desuso. En caso transcurra un tiempo amplio, se debiese configurar el equipo para que se apagase automáticamente. Se debe tener un control de vigilancia para el abandono de estación de trabajo por fuera de las instalaciones de la organización.	Se solicita bloquear y/o obstruir los equipos tecnológicos con protección de passwords robustas apenas se prescinda, e incluso poseer un protector de pantalla que bloque el equipo cuando este en desuso. En caso transcurra un tiempo amplio, se debiese configurar el equipo para que se apagase automáticamente y no este disponible en la red. Se debe tener un control riguroso de vigilancia para el abandono de estación de trabajo por fuera de las instalaciones de la organización.	Se solicita de manera rigurosa bloquear y/o obstruir los equipos tecnológicos con protección de passwords robustas apenas se prescinda, e incluso poseer un protector de pantalla que bloque el equipo cuando este en desuso. En caso transcurra un tiempo amplio, se debiese configurar el equipo para que se apagase automáticamente y no este disponible en la red. Se debe tener un control riguroso de vigilancia para el abandono de estación de trabajo por fuera de las instalaciones de la organización. Las estaciones de trabajo deben estar conectadas lo menos posible a las redes
Acceso a oficinas	No necesita prevención o resguardo especial	No necesita prevención o resguardo especial	El acceso a oficinas las cuales posean información relevante y de confidencialidad debe poseer un tipo de restricción de acceso físico (tarjetas, huellas dactilares, puertas con llaves u otro medio), este proceso de control debe aplicarse cuando la oficina se encuentre sin resguardo alguno.	El acceso a oficinas las cuales posean información relevante y de confidencialidad para la alta gerencia, esta debe poseer un tipo de restricción mas riguroso de acceso físico (tarjetas, huellas dactilares, puertas con llaves u otro medio), este proceso de control debe aplicarse cuando la oficina se encuentre sin resguardo alguno.
Fotocopiado de la Información				
Tipo de copias permitidas	No necesita prevención especial	No necesita prevención especial	Solo cuando sea necesario u solicitado	En este caso debe ser autorizado por el dueño o propietario de la información

Imagen 1: Procedimiento de clasificación para los diferentes niveles de clasificación adoptados por el área de TI (***Fuente:*** adoptado de *(Angarita & Tabares, 2012)*)

Bibliografía

Angarita, A. A., & Tabares, C. A. (Diciembre de 2012). *Análisis de riesgos para el proceso administrativo: Departamento de informática en la empresa de Acueducto y Alcantarillado de Pereira S.A E.S.P, basados en la norma ISO 27005.* Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/3914/T0058A581.pdf?sequence=1&isAllowed=y

ISOTools Excellence. (14 de Setiembre de 2017). *ISO 27001 ¿Cómo se debe realizar la clasificación de la información?* Obtenido de SGSI Blog especializado en Sistemas de Gestión de seguridad de la información: http://www.pmg-ssi.com/2017/09/iso-27001-clasificacion-de-la-informacion-2/

ISOTools Excellence. (24 de Agosto de 2017). *Norma ISO 27002: ¿Como se lleva a cabo la gestión de activos?* Obtenido de SGSI Blog espeacializado en Sistemas de Gestión de seguridad de la Información: http://www.pmg-ssi.com/2017/08/norma-iso-27002-como-se-lleva-a-cabo-la-gestion-de-activos/

MINTIC. (15 de Marzo de 2016). *Guía para la Gestión y Clasificación de activos de Información - Seguridad y privacidad de la información*. Obtenido de mintic: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Parra, Y. A. (2016). *Manual inventario de activos, clasificación y publicación de la información*. Obtenido de COLCIENCIAS: http://www.colciencias.gov.co/sites/default/files/upload/paginas/g104m02-manual-de-activos-de_-informacion.pdf

Profesional Grupo de AE y del SGI. (23 de Mayo de 2014). *Procedimiento de clasificación y etiquetado de activos de información*. Obtenido de Superintendencia de Sociedades: http://www.supersociedades.gov.co/superintendencia/oficina-asesora-de-planeacion/polinemanu/sgi/Documents/Documentos%20Calidad/DOCUMENTOS/GC-PR-004%20Procedimiento%20Clasificacion%20y%20Etiquetado%20de%20Activos%20de%20Informacion.pdf

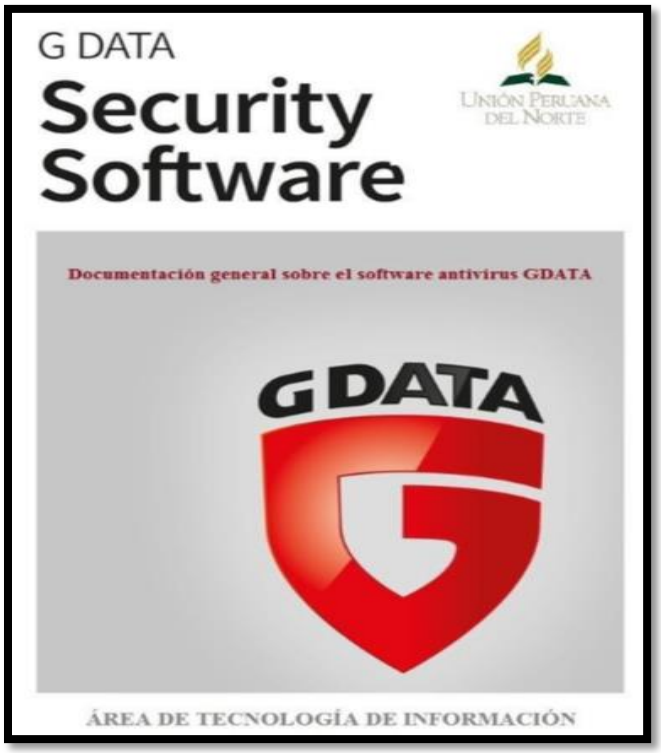
Anexo 31: Registro de Inventariado de la Clasificación de la información

Registro de Inventario de la Clasificación de la información							
NOMBRE DEL ÁREA ENCARGADA :	Area de Tecnologías de Información (TI)			CICLO :	PRIMER SEMESTRE (DICIEMBRE- ABRIL)		
NOMBRE DE LA ORGANIZACIÓN :	Unión Peruana del Norte			FECHA DE INICIO :	07/12/2017		
ID de clasificación	Codigo de (documento/Archivo /Software)	Fecha recibida	Descripción	Valor	Encargado de la clasificación	Nivel de clasificacion	Estado
CLA-01	MU-01	15/01/2017	Manuales de Usuarios	Baja	Amelio Apaza, Janeth Tenorio	Pública	Activo
CLA-02	LIC-01	15/01/2017	Licencias Software, Antivirus, Adobe	Media	Carlos Saavedra	Uso Interno	Activo
CLA-03	HE-01	15/01/2017	Hoja de entrega	Media	Fernando Lazo	Uso Interno	Activo
CLA-04	HR-01	15/01/2017	Hoja de recepción	Media	Fernando Lazo	Uso Interno	Activo
CLA-05	LI-01	15/01/2017	Lista de Inventarios	Media	Carlos Saavedra	Uso Interno	Activo
CLA-06	ICA-01	15/01/2017	Informe de Control de Asistencias	Media	Carlos Saavedra	Uso Interno	Activo
CLA-07	IN-01	15/01/2017	Informe networking	Alta	Carlos Saavedra	Restringida	Activo
CLA-08	CB-01	15/01/2017	Copias de Backup(Sotware y Base de Datos)	Alta	Amelio Apaza, Janeth Tenorio	Restringida	Activo
CLA-09	CON-01	15/01/2017	Contratos	Alta	Área de Legales y Recursos Humanos y/o Carlos Saavedra	Restringida	Activo
CLA-10	IPROY-01	15/01/2017	Informe Presupuesto	Muy Alta	Alta gerencia	Altamente Restringida	Activo
CLA-11	IPRES-01	15/01/2017	Informe de Proyectos	Muy Alta	Alta gerencia	Altamente Restringida	Activo

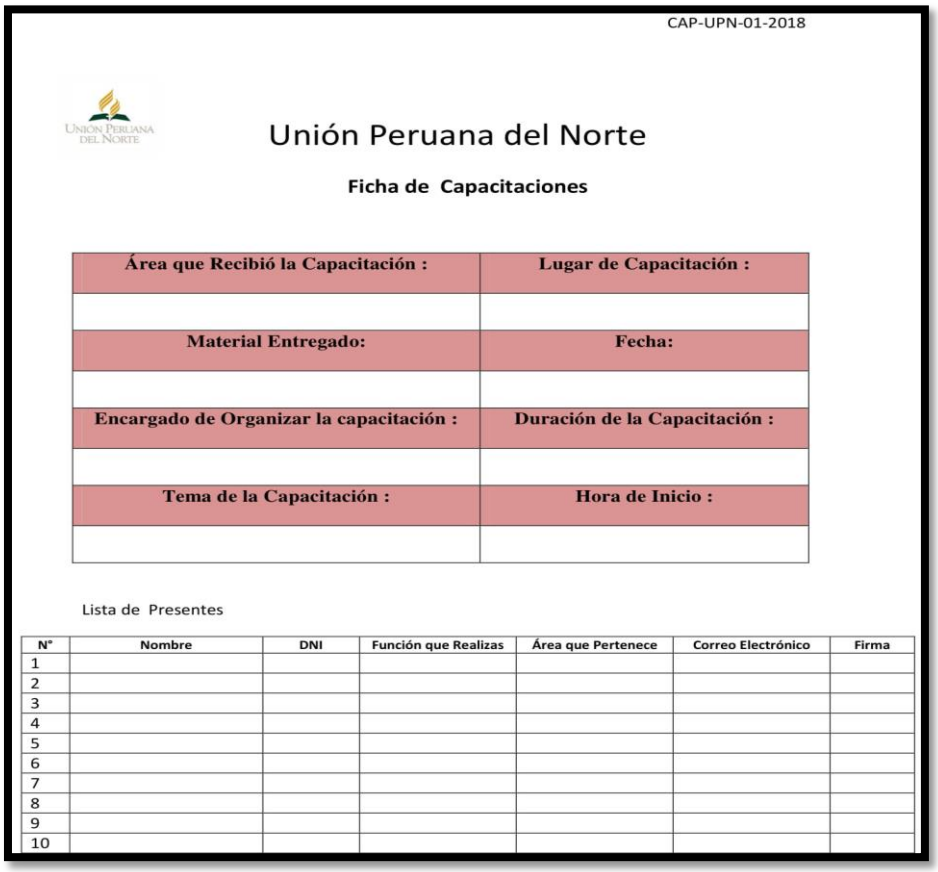
SIGLA	Nombre
AR	Altamente restringido
R	Restringido
UI	Uso Interno
P	Público

Estados	Descripción
Activo	Activo de informacion que se encuentra habilitado para su libre uso y manejo
Inactivo	Activo de información que se encuentra inhabilitado para su uso
Eliminado	Activo de informacion que ya no forma parte de la organización y quedo desechado y sin ningun uso alguno

Anexo 32: Documentación general sobre el software antivirus GDATA



Anexo 33: Formato de Ficha de Capacitaciones



CAP-UPN-01-2018

Unión Peruana del Norte

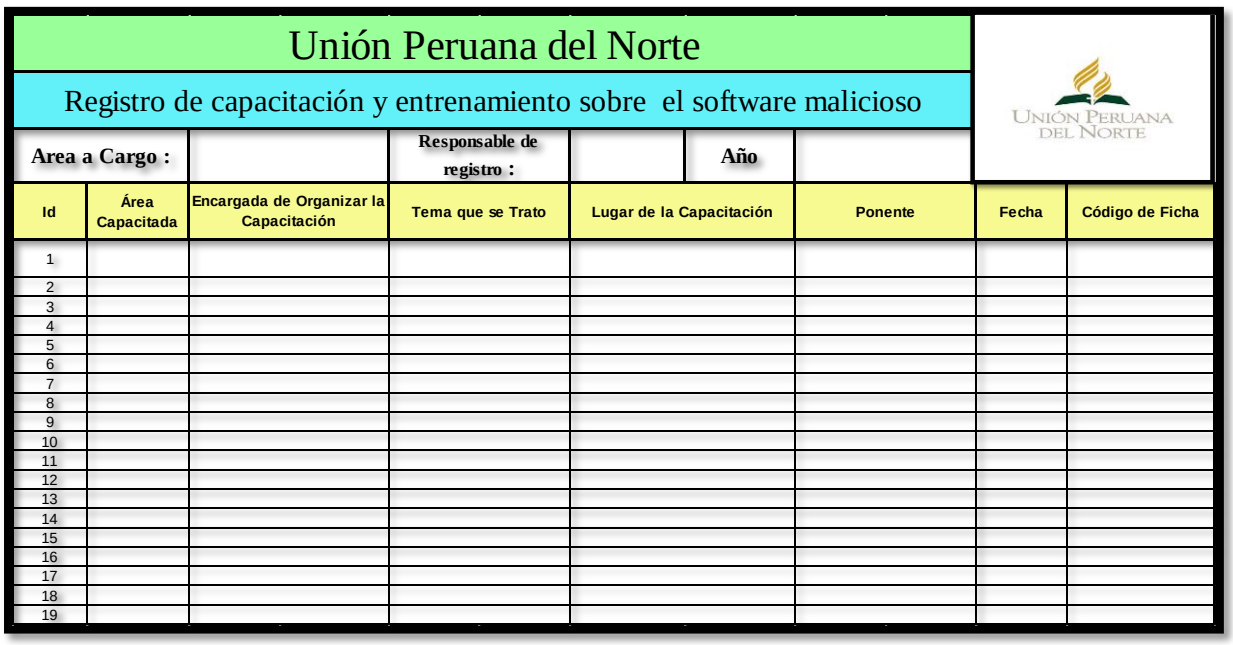
Ficha de Capacitaciones

Área que Recibió la Capacitación :	Lugar de Capacitación :
Material Entregado:	**Fecha:**
Encargado de Organizar la capacitación :	**Duración de la Capacitación :**
Tema de la Capacitación :	**Hora de Inicio :**

Lista de Presentes

N°	Nombre	DNI	Función que Realizas	Área que Pertenece	Correo Electrónico	Firma
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Anexo 34: Formato de Registro de capacitación y entrenamiento sobre el software malicioso



Unión Peruana del Norte

Registro de capacitación y entrenamiento sobre el software malicioso

Area a Cargo :		Responsable de registro :		Año	

Id	Área Capacitada	Encargada de Organizar la Capacitación	Tema que se Trato	Lugar de la Capacitación	Ponente	Fecha	Código de Ficha
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							

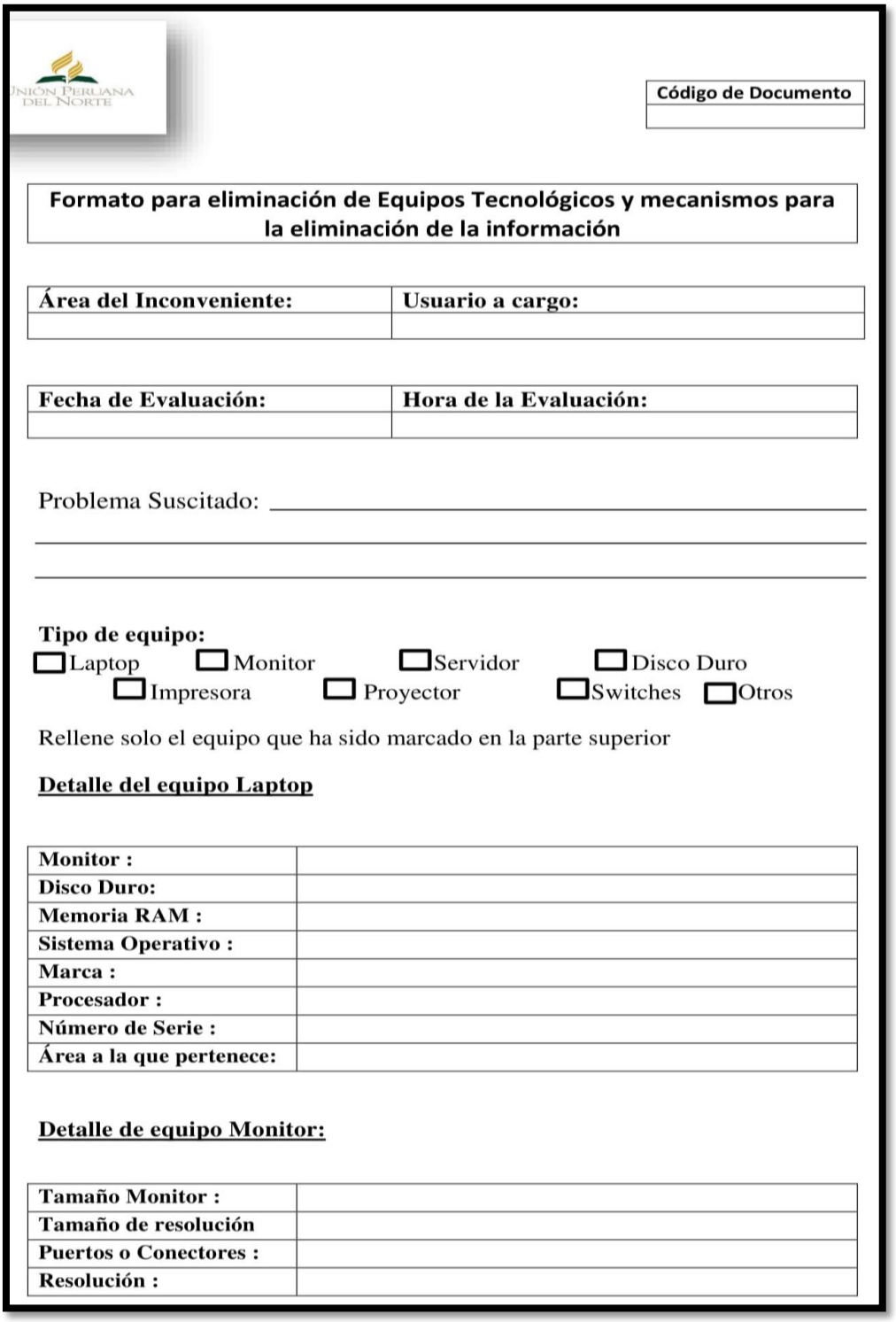
Anexo 35: Formato de Registro de Amenazas identificadas en las evaluaciones de los activos

Registro de Amenazas identificadas en las Evaluaciones de los Activos							
Area a Cargo:	Area Tecnología de Información			Nombre de la Organización :	Unión Peruana del Norte		
ID	ID AMENAZA	TIPO AMENAZA	ID ACTIVO	Tipo de Activo	DESCRIPCIÓN DE LA AMENAZA	PROPIETARIO DEL ACTIVO	FECHA DE DETECCIÓN
IDE-01							
IDE-02							
IDE-03							
IDE-04							
IDE-05							
IDE-06							
IDE-07							
IDE-08							
IDE-09							
IDE-10							
IDE-11							
IDE-12							
IDE-13							
IDE-14							
IDE-15							
IDE-16							
IDE-17							
IDE-18							
IDE-19							
IDE-20							

Anexo 36: Formato de Registro de dispositivos autorizados a la información y a la red

Registro de Dispositivos Autorizados a la Información y a la Red								
Area a Cargo:	Area Tecnolgía de Información				Nombre de la Organización :	Unión Peruana del Norte		
ID	MARCA DEL DISPOSITIVO	MODELO DEL DISPOSTIVO	IMEI O MAC DEL DISPOSITIVO	PROPIETARIO	ÁREA DEL PROPIETARIO	DESCRIPCIÓN DEL TIPO DE ACCESO A LA INFORMACIÓN QUE TENDRA EL DISPOSITIVO	DURACIÓN DEL DISPOSITIVO CON EL PROPIETARIO	FECHA DE ENTREGA DEL DISPOSITIVO

Anexo 37: Formato para la eliminación de Equipos Tecnológicos y mecanismos para la eliminación de la información



UNIÓN PERUANA DEL NORTE

Código de Documento

Formato para eliminación de Equipos Tecnológicos y mecanismos para la eliminación de la información

Área del Inconveniente:	Usuario a cargo:

Fecha de Evaluación:	Hora de la Evaluación:

Problema Suscitado: _____

_____

_____

Tipo de equipo:

☐ Laptop ☐ Monitor ☐ Servidor ☐ Disco Duro
☐ Impresora ☐ Proyector ☐ Switches ☐ Otros

Rellene solo el equipo que ha sido marcado en la parte superior

Detalle del equipo Laptop

Monitor :	
Disco Duro:	
Memoria RAM :	
Sistema Operativo :	
Marca :	
Procesador :	
Número de Serie :	
Área a la que pertenece:	

Detalle de equipo Monitor:

Tamaño Monitor :	
Tamaño de resolución	
Puertos o Conectores :	
Resolución :	

Número de Serie :	
Área a la que pertenece:	
Marca :	

Detalle de equipo Servidor:

Tipo de Servidor	☐ Servidor de Bastidor	☐ Servidores de Torre
Microprocesador :		
Memoria RAM:		
Placas del Sistema:		
Disco Duro :		
Marca :		
Número de Serie :		
Área a la que pertenece:		

Descripción:
Servidor de Bastidor: Son servidores muy delgados, que se colocan con Racks, cuentan con poca puertos de expansión, pero que si tiene n la capacidad de procesar mucha información.
Servidor de Torre: Son los que ocupan más espacio, y cuentan con mayor escalabilidad, para soportar conexiones de más equipos, este tipo de servidor no se coloca en Racks mayormente se coloca en el suelo o en mesas

Detalle de equipo Disco Duro:

Tipo de Disco Duro	☐ Disco Duro Externo	☐ Disco Duro Interno
Memoria:		
Marca :		
Número de Serie :		
Área a la que pertenece:		

Detalle de equipo Impresora:

Marca :	
Resolución:	
Cuantos Cartuchos Carga :	
Conectores :	
¿Carga mucho papel? :	
Número de Serie :	
Área a la que pertenece:	

Detalle de Proyector:

Marca :		
Consumo de energía:	☐ Ahorra energía	☐ No ahorra energía
Conectores de Entrada y Salida :		
Altura, Anchura y Peso :		
Número de Serie :		
Área a la que pertenece:		

Detalle de Switches:

Marca :	
Compatibilidad:	
¿Es altamente peligroso?:	
Color :	
Número de Serie :	
Área a la que pertenecía	

Porque se decidió prescindir del equipo:_____

_____

_____

_____

Cuáles fueron los mecanismos que se utilizó para su destrucción de la información contenida dentro del equipo tecnológico.

_____

_____

_____

_____

_____ _____

Firma del Jefe de TI Firma del Usuario Responsable

Anexo 38: Formato de Registro de los derechos de acceso según los roles y responsabilidades de los usuarios

Registro de los derechos de acceso según lo roles y responsabilidades de los usuarios					
Área Encargada :	Área de TI	Nombre del Personal a cargo :		Fernando Lazo	
Codigo de Registro :	RE-ACCE-01	DNI del personal encargado :		12345678	
ID de Usuario	Nombre Completo	Cargo en la organización	Área que Pertenece	Responsabilidades del cargo	Derecho de acceso del Usuario (Modulos)

Anexo 39: Formato de la Ficha de capacitaciones sobre la importancia de la seguridad física

CAP-SF-UPN-01-2018

Unión Peruana del Norte

Ficha de Capacitaciones sobre la importancia de la Seguridad Física

Área que recibió la Capacitación :	Lugar de Capacitación :
Material Entregado:	**Fecha:**
Encargado de Organizar la capacitación :	**Duración de la Capacitación :**
Tema de la Capacitación :	**Hora de Inicio :**

Lista de Presentes en la capacitación

N°	Nombre	DNI	Función que Realiza	Área al cual Pertenece	Correo Electrónico	Firma
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Anexo 40: Formato de Registro de capacitación sobre la importancia de la seguridad física

Unión Peruana del Norte

Registro de capacitación sobre la importancia de la Seguridad Física

Área a Cargo :		Responsable de registro :		Año	

Id	Área Capacitada	Encargado de Organizar la Capacitación	Tema que se Trato	Lugar de la Capacitación	Ponente	Fecha	Código de Ficha
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							

Anexo 41: Formato de Solicitud de Peticiones de Acceso a las instalaciones

Código de Documento
GVT

Solicitud de Peticiones de Acceso a las instalaciones

Sres.: Unión Peruana del Norte

Área a quien va dirigida: _____

Instalaciones del área donde solicita acceso: _____

Nombre del Visitante: _____

DNI del visitante: _____

Me dirijo a Usted, con el debido respeto, para que me permita tener acceso a las instalaciones del área de Tecnologías de Información (TI), para la fecha _____ , para realizar un estudio de investigación en el área mencionada, por el tiempo que usted me brinde.

Correo Electrónico:	Numero telefónico:

☐ Ingreso cochera ☐ Ingreso Puerta Peatonal

Esperando verme favorecido en mi petición, le agradezco de antemano su atención, no sin antes reiterarle que nosotros nos comprometemos a mostrar cordura durante la visita a las instalaciones.

_____

Firma del Visitante

Nombre:

Presentar en una copia más, contando el original. La persona que firme está presente carta se hará responsable de sus actos si en caso sucediese algo inesperado, quedara registrado al detalle para que no hubiese ningún inconveniente.

Anexo 42: Formato de Registro de las peticiones formales de acceso

Unión Peruana del Norte								
Registro de las peticiones formales de acceso								
Área a Cargo :		Responsable de registro :		Periodo				
Id	Codigo de documento de petición de acceso	Instalaciones del área donde solicita acceso	Nombre del emisor	DNI del emisor	Fecha de envio de solicitud	Fecha de recepcion de la solicitud	Estado de Peticion (Aprobada o Denegada)	Observacion
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								

Anexo 43: Formato de Registro de visitas u operarios a las instalaciones del área de TI de la UPN

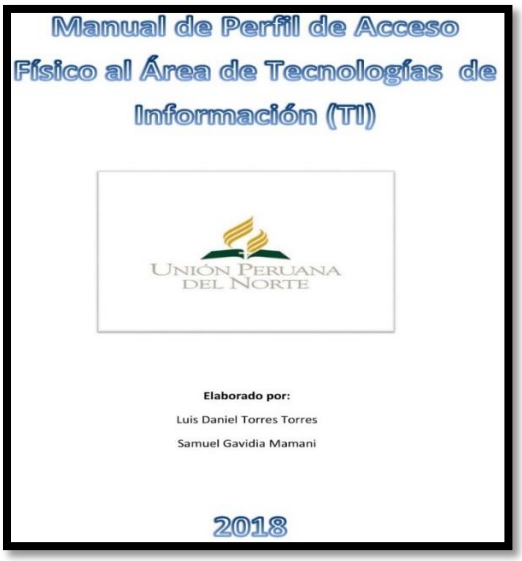
Registro de Visitas u Operarios a las instalaciones del Área de TI de la Unión Peruana del Norte										
Área Encargada :			Nombre del Personal Encargado :			Nombre de Supervisor:				
Código de Registro :			DNI del Personal Encargado :			DNI del Supervisor:				
Id	Fecha de Ingreso a las instalaciones	Hora de Ingreso a las instalaciones	Hora de Salida de las instalaciones	Tipo (Visitante - Operario)	Area de Visita (Destino)	Nombre Completo de la visita u Operario	DNI del Visitante u Operario	Codigo del Carnet Visitante u Operario	Código de solicitud de petición de Acceso	Acompañante del Visitante u Operario

Anexo 44: Formato de Registro del personal no autorizado y que no lleve identificación en las instalaciones de la UPN

Registro del Personal no Autorizado y que no lleve Identificación en las Instalaciones de la Unión Peruana del Norte										
Área Encargada :		Nombre del Personal Encargado :		Nombre de Supervisor:						
Código de Registro :		DNI del Personal Encargado :		DNI del Supervisor:						
Id	Fecha	Hora	Nombre de la Persona:	Área o Instalación donde se localizó	Nombre del personal que lo ubicó	DNI de la persona	Tiene Carnet SI o NO	Nombre del Acompañante durante la visita	Observación o motivo	Código de Pecitción
Re-PE-01										
Re-PE-02										
Re-PE-03										
Re-PE-04										
Re-PE-05										
Re-PE-06										
Re-PE-07										
Re-PE-08										
Re-PE-09										
Re-PE-10										
Re-PE-11										
Re-PE-12										

Anexo 45: Fotocheck de visitantes y operarios & Señalizaciones

Anexo 46: Manual de perfil de acceso físico al área de TI



Anexo 47: Formato de Registro de Inventariado de dispositivos y/o Activos de salida

INVENTARIADO DE DISPOSITIVOS Y/O ACTIVOS DE SALIDA												
Uniòn Peruana del Norte												
Àrea a cargo:			Periodo:			Persona a cargo del registro :						
ID del Dispositivo	Nombre del Dispositivo y/o activo	Descripcion del Dispositivo y/o activo	Persona a cargo del Custodio Técnico del activo y/o dispositivo	Tipo de Activo y/o dispositivo (H/S)	Tipo de acceso a la informaciòn (Lectura, Escritura, Consulta)	Valor de criticidad del dispositivo y/o activo	Estado del activo y/o dispositivo antes de salir	Fecha de salida del dispositivo y/o activo	Fecha de llegada del dispositivo y/o activo	Lugar de Destino	Responsable de la recepciòn, devolucion y cuidado del activo y/o dispositivo	Estado del activo y/o dispositivo retornado

Anexo 48: Formato de Registro de Inventariado de documentos sensibles

INVENTARIADO DE DOCUMENTOS SENSIBLES						
Unión Peruana del Norte						
Área a cargo:		Periodo:		Persona a cargo del registro :		
ID de D. Sensible	Código de documento	Nombre del Documento	Descripción del Documento	Propietario del Documento	Nivel de Clasificación (Pública, Uso Interno, Restringida, Altamente restringida)	Valor de criticidad del documento (Baja, Media, Alta, Muy Alta)

Anexo 49: Formato de Registro de Inventariado de conciliación de documentos sensibles y dispositivos de salida

INVENTARIADO DE CONCILIACIÓN DE DOCUMENTOS SENSIBLES Y DISPOSITIVOS DE SALIDA

Unión Peruana del Norte

Área a cargo:		Periodo:			Persona a cargo del registro :						
ID	ID del Dispositivo	Descripción del dispositivo	Nombre de personal a cargo del dispositivo	Nivel de Clasificación del dispositivo	Valor de criticidad del dispositivo (Baja, Media, Alta, Muy Alta)	ID de D. Sensible	Descripción del D. Sensible	Nombre de personal a cargo del D. Sensible	Nivel de Clasificación del D. Sensible	Valor de Criticidad del D. Sensible (Baja, Media, Alta, Muy Alta)	Fecha

Anexo 50: Validación de los procedimientos por parte de los especialistas

Constancia de Validación del Procedimiento Gestión de vulnerabilidades

Quien suscribe, María Antonieta Vidalón Aliaga, con documento de identidad 10149876, de profesión en Ingeniería de Sistemas con grado de Licenciada, ejerciendo actualmente como Directora de Extensión Cultural y Proyección Social.

Por medio de la presente hago constar que he revisado con fines de validación la elaboración de la propuesta de mejoramiento de procesos, el procedimiento Gestión de vulnerabilidades, que está diseñado bajo el control 12.6.1 – "Gestión de las vulnerabilidades técnicas" de la norma ISO/IEC 27002:2013, el cual permitirá cumplir en gran parte lo que manifiesta este control, para su eficiente resguardo y debido aseguramiento de la seguridad de la información.

Por todo lo mencionado anteriormente doy mi conformidad y validación correspondiente.

Fecha: 23/11/2017

Firma

Constancia de Validación del Procedimiento para la protección contra el código malicioso

Quien suscribe, María Antonieta Vidalón Aliaga, con documento de identidad 10149876, de profesión en Ingeniería de Sistemas con grado de Licenciada, ejerciendo actualmente como Directora de Extensión Cultural y Proyección Social.

Por medio de la presente hago constar que he revisado con fines de validación la elaboración de la propuesta de mejoramiento de procesos, el procedimiento para la protección contra el código malicioso, que está diseñado bajo el control 12.2.1 – "Controles contra el código malicioso" de la norma ISO/IEC 27002:2013, el cual permitirá cumplir en gran parte lo que manifiesta este control, para su eficiente resguardo y debido aseguramiento de la seguridad de la información.

Por todo lo mencionado anteriormente doy mi conformidad y validación correspondiente.

Fecha: 01/12/2017

Firma

Constancia de Validación del Procedimiento Gestión de acceso de usuarios

Quien suscribe, María Antonieta Vidalón Aliaga, con documento de identidad 10149876, de profesión en Ingeniería de Sistemas con grado de Licenciada, ejerciendo actualmente como Directora de Extensión Cultural y Proyección Social.

Por medio de la presente hago constar que he revisado con fines de validación la elaboración de la propuesta de mejoramiento de procesos, el procedimiento Gestión de acceso de usuarios, que está diseñado bajo los controles 9.2.1 – "Registro y baja de usuario"; 9.2.2 - "Provisión de acceso de usuario"; 9.2.3 – "Gestión de privilegios de acceso"; 9.2.5 – "Revisión de los derechos de acceso"; 9.2.6 – "Retirada o reasignación de los derechos de acceso", estos forman parte de la norma ISO/IEC 27002:2013, los cuales permitirán cumplir en gran parte lo que manifiestan estos controles, para su eficiente resguardo y debido aseguramiento de la seguridad de la información.

Por todo lo mencionado anteriormente doy mi conformidad y validación correspondiente.

Fecha: 05/12/2017

Firma

Constancia de Validación del Procedimiento Gestión de inicio de sesión

Quien suscribe, María Antonieta Vidalón Aliaga, con documento de identidad 10149876, de profesión en Ingeniería de Sistemas con grado de Licenciada, ejerciendo actualmente como Directora de Extensión Cultural y Proyección Social.

Por medio de la presente hago constar que he revisado con fines de validación la elaboración de la propuesta de mejoramiento de procesos, el procedimiento Gestión de inicio de sesión, que está diseñado bajo el control 9.4.2 – "Procedimientos seguros de inicio de sesión" de la norma ISO/IEC 27002:2013, el cual permitirá cumplir en gran parte lo que manifiesta este control, para su eficiente resguardo y debido aseguramiento de la seguridad de la información.

Por todo lo mencionado anteriormente doy mi conformidad y validación correspondiente.

Fecha: 13/12/2017

Firma

Constancia de Validación del Procedimiento para la protección contra el código malicioso

Quien suscribe, Immer Elías Cuellar Rodríguez, con documento de identidad Nº 40964219, de profesión en Ingeniería de Sistemas con grado de Magister, ejerciendo actualmente como Director de Digeti en la Universidad Peruana Unión.

Por medio de la presente hago constar que he revisado con fines de validación la elaboración de la propuesta de mejoramiento de procesos, el procedimiento para la protección contra el código malicioso, que está diseñado bajo el control 12.2.1 – "Controles contra el código malicioso" de la norma ISO/IEC 27002:2013, el cual permitirá cumplir en gran parte lo que manifiesta este control, para su eficiente resguardo y debido aseguramiento de la seguridad de la información.

Por todo lo mencionado anteriormente doy mí conformidad y validación correspondiente.

Fecha: 01/12/2017

Firma

Constancia de Validación del Procedimiento Gestión de vulnerabilidades

Quien suscribe, Immer Elías Cuellar Rodríguez, con documento de identidad Nº 40964219, de profesión en Ingeniería de Sistemas con grado de Magister, ejerciendo actualmente como Director de Digeti en la Universidad Peruana Unión.

Por medio de la presente hago constar que he revisado con fines de validación la elaboración de la propuesta de mejoramiento de procesos, el procedimiento Gestión de vulnerabilidades, que está diseñado bajo el control 12.6.1 – "Gestión de las vulnerabilidades técnicas" de la norma ISO/IEC 27002:2013, el cual permitirá cumplir en gran parte lo que manifiesta este control, para su eficiente resguardo y debido aseguramiento de la seguridad de la información.

Por todo lo mencionado anteriormente doy mí conformidad y validación correspondiente.

Fecha: 23/11/2017

Firma

Constancia de Validación del Procedimiento Gestión de acceso de usuarios

Quien suscribe, Immer Elías Cuellar Rodríguez, con documento de identidad Nº 40964219, de profesión en Ingeniería de Sistemas con grado de Magister, ejerciendo actualmente como Director de Digeti en la Universidad Peruana Unión.

Por medio de la presente hago constar que he revisado con fines de validación la elaboración de la propuesta de mejoramiento de procesos, el procedimiento Gestión de acceso de usuarios, que está diseñado bajo los controles 9.2.1 – "Registro y baja de usuario"; 9.2.2 - "Provisión de acceso de usuario"; 9.2.3 – "Gestión de privilegios de acceso"; 9.2.5 – "Revisión de los derechos de acceso"; 9.2.6 – "Retirada o reasignación de los derechos de acceso", estos forman parte de la norma ISO/IEC 27002:2013, los cuales permitirán cumplir en gran parte lo que manifiestan estos controles, para su eficiente resguardo y debido aseguramiento de la seguridad de la información.

Por todo lo mencionado anteriormente doy mí conformidad y validación correspondiente.

Fecha: 05/12/2017

Firma

Constancia de Validación del Procedimiento Gestión de inicio de sesión

Quien suscribe, Immer Elías Cuellar Rodríguez, con documento de identidad Nº 40964219, de profesión en Ingeniería de Sistemas con grado de Magister, ejerciendo actualmente como Director de Digeti en la Universidad Peruana Unión.

Por medio de la presente hago constar que he revisado con fines de validación la elaboración de la propuesta de mejoramiento de procesos, el procedimiento Gestión de inicio de sesión, que está diseñado bajo el control 9.4.2 – "Procedimientos seguros de inicio de sesión" de la norma ISO/IEC 27002:2013, el cual permitirá cumplir en gran parte lo que manifiesta este control, para su eficiente resguardo y debido aseguramiento de la seguridad de la información.

Por todo lo mencionado anteriormente doy mí conformidad y validación correspondiente.

Fecha: 13/12/2017

Firma

Anexo 51: Evaluación con la segunda lista de chequeo

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad		Código de checklist	2017DS01
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo	System Auditors	
Área a Auditar	Área de tecnologías de información (TI)	Auditor	Luis Torres Torres	
Práctica de Gestión del Proceso	DSS05.01 Proteger Contra Software Malicioso			

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	El usuario final está capacitado sobre qué es un software malicioso.	X		Si realizan capacitaciones y lo tienen registrado
2	Existe un procedimiento de prevención frente al ataque de un software malicioso.	X		Si cuenta con un proceso adecuado
3	Existe una herramienta de protección actualizada para el usuario final y también para la seguridad perimetral.	X		Lo realiza y cuenta con documentación
4	Se programa la actualización del software antivirus según las políticas del área.	X		Lo realiza y cuenta con documentación
5	Se realiza evaluaciones para detectar vulnerabilidades antes de que sean una amenaza.	X		Si realizan de acuerdo al proceso descrito
6	Existe un registro de amenaza identificadas en las evaluaciones.	X		Si está documentado
7	Existe alguna aplicación instalada que analice y evalúe el contenido del tráfico entrante para prevenir software malicioso.	x		
8	Existe política de permisos para instalar cualquier software	x		Si cuenta con política

ASOCIACION IGLESIA ADVENTISTA DEL SÉPTIMO DIA PERUANA DEL NORTE – TECNOLOGÍA DE INFORMACIÓN

CARLOS SAAVEDRA

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad		Código de checklist	2017DS02
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo	System Auditors	
Área a Auditar	Área de tecnologías de información (TI)	Auditor	Luis Torres Torres	
Práctica de Gestión del Proceso	DSS05.02 Gestionar la seguridad de la red y las conexiones			

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	Existe una política de seguridad para la red y conexiones.	X		Si tienen políticas definidas para ello
2	Solo los dispositivos autorizados tienen acceso a la información y a la red de la empresa.	X		Si realizan y si tienen documentado
3	Existen políticas y herramientas que controlen el tráfico entrante y saliente de la red.	X		Si tienen herramienta, y están definidas las políticas
4	La información de la empresa está clasificada según su criticidad e importancia.	X		Si existe una clasificación
5	La información está cifrada para su tránsito en la red según su clasificación.		X	La información no se encuentra cifrada, pero están definidas
6	Tienen conexiones certificadas de red.	X		Si está certificada
7	Los equipos de red son configurados siguiendo la política de seguridad definida.	X		Está definida como política
8	Se realiza pruebas de intrusión para ver el nivel de seguridad que se encuentra la red.		X	No lo realizan, pero están definidas

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad			Código de checklist	2017DS03
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo		System Auditors	
Área a Auditar	Área de tecnologías de información (TI)		Auditor	Luis Torres Torres	
Práctica de Gestión del Proceso	DSS05.03 Gestionar la seguridad de los puestos de usuario final				

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	El sistema operativo de todas las computadoras (portátiles, de escritorio y servidores), cuenta con la última actualización publicada.	X		Se estableció una política que indique que es obligatorio tener actualizados los sistemas operativos en los equipos en general
2	Se tiene mecanismos de bloqueo que permita el libre acceso a la información y red de la empresa.	X		Lo realizan en forma virtual
3	Se cifra la información almacenada de la organización según su clasificación.		X	No está cifrada en su totalidad, pero están definidas
4	Se controla los accesos al dispositivo de usuario final.	X		Lo realizan mediante dominios
5	Se configura la red a través de un servidor DHCP.	X		Si lo realizan y se encuentra documentada
6	Se implementa el filtrado de tráfico de red en dispositivos de usuario final.		X	No lo realizan, pero están definidas
7	La integridad de la información es protegida en los puestos de usuario final.		X	No lo realizan, pero están definidas
8	Se cuenta con equipos de protección física a los dispositivos de usuario final (Ups, estabilizadores).	X		Si lo tienen
9	Cuando se deteriora un dispositivo se elimina físicamente y lógicamente de todo el contenido de la información que se encuentra dentro.	X		Si lo realizan y si está documentado

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad			Código de checklist	2017DS04
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo		System Auditors	
Área a Auditar	Área de tecnologías de información (TI)		Auditor	Luis Torres Torres	
Práctica de Gestión del Proceso	DSS05.04 Gestionar la identidad del usuario y el acceso lógico				

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	Se mantiene los derechos de acceso de los usuarios de acuerdo al proceso de negocio.	X		Están definidas las políticas de derechos de acceso
2	Se alinea la gestión de identidades y derecho de acceso a los roles y responsabilidades definidos.	X		Si lo realizan
3	Se identifica los activos de la información por roles funcionales	X		Si lo realiza, poseen un formato interno
4	Mediante una clasificación de seguridad se realiza la autenticación en el acceso del usuario final a los activos de información.	X		Si lo realizan y cuentan con documentación
5	Las unidades de negocio gestionan la autenticación con aplicaciones para ver si los accesos a los activos de información fueron bien administrados.	X		Tienen un procedimiento y documentación de ello
6	Los cambios efectuados en los perfiles de usuario se registran y monitorea solo con la aprobación del responsable del área.	X		Tienen un procedimiento y documentación de ello
7	Separan cuentas de usuarios privilegiadas.	X		Lo realizan y tienen documento
8	Se revisa periódicamente los privilegios asignados a las cuentas del usuario.	X		Tienen un procedimiento y documentación de ello
9	Se identifica unívocamente todas las actividades de proceso realizadas por el usuario.		X	Está definido como política pero no lo realizan
10	Se mantiene un registro del acceso lógico a la información altamente sencilla.	X		Si tienen un registro de acceso lógico

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad			Código de checklist	2017DS05
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo		System Auditors	
Área a Auditar	Área de tecnologías de información (TI)		Auditor	Samuel Gavidia	
Práctica de Gestión del Proceso	DSS05.05 Gestionar el acceso físico a los activos de TI				

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	Se gestiona las peticiones de acceso a las instalaciones de procesamiento.	X		Si lo realizan y si tienen un formato
2	Se gestiona las concesiones de acceso a áreas de instalación y procesamiento.	X		Si lo realizan
3	Son completadas las peticiones formales de acceso	X		Si lo realizan y tienen documentado
4	Las peticiones formales de acceso son autorizados por la dirección de TI.	X		Son autorizados y son registrados
5	Los perfiles de acceso físico al área de TI están definidas y actualizadas. (Basándose en las funciones y responsabilidades del usuario).	X		Si lo realizan y tienen un registro
6	Se registra y supervisa el acceso a las ubicaciones de TI. (Visitantes, proveedores, personal, etc.).	X		Si se registra
7	El personal del área de TI mantiene visible la identificación en todo momento (fotocheck, placa o tarjeta).	X		Si lo conllevan
8	Se escolta a los visitantes en todo momento mientras estén en la ubicación.	X		Si se escolta y si tienen un registro
9	Se alerta al personal de seguridad si se encuentra a un individuo que va sin la compañía de alguien que pertenezca a la organización.	X		Si se alerta y si tienen un registro
10	Se alerta al personal de seguridad si se encuentra a un individuo que no lleva visible algo que lo identifique como visitante o empleado.	X		Lo realizan y tienen registro
11	Se establecen restricciones en el perímetro tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores para restringir el acceso a ubicaciones de TI sensibles.	X		Si lo realizan
12	Se tiene informado al personal sobre la importancia de la seguridad física.	X		Si lo realizan y está registrado

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad			Código de checklist	2017DS06
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo		System Auditors	
Área a Auditar	Área de tecnologías de información (TI)		Auditor	Samuel Gavidia	
Práctica de Gestión del Proceso	DSS05.06 Gestionar Documentos sensibles y dispositivos de salida				

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	Existen procedimientos para la recepción de documentos especiales.	X		Existe un procedimiento
2	Existen procedimientos para el uso de documentos especiales.	X		Existe un procedimiento y tienen un registro
3	Existen procedimientos para la eliminación de documentos especiales.	X		Existe un procedimiento y tienen un registro
4	Se asigna privilegios de acceso a documentos sensibles de acuerdo a su importancia.	X		Si lo realizan y si cuentan con asignación de privilegios
5	Existe un inventario de documentos sensibles.	X		Si tienen un registro
6	Existe un inventario de dispositivos de salida.	X		Si tienen un registro
7	Se realiza un inventario de conciliaciones de documentos sensibles y dispositivos de salida.	X		Si tienen un registro
8	Existen controles de seguridad físicas para los formularios especiales.		X	Se está implementando las políticas para ser consideradas a futuro
9	Existen controles de seguridad física para los dispositivos sensibles.		X	Se está implementando las políticas para ser consideradas a futuro
10	Se tiene los mecanismos necesarios para eliminar cualquier dispositivo de memoria o papeles lleno de información.	X		Si tienen mecanismos y si está registrado
11	Se tiene un modelo de arquitectura de la información.		X	Se está implementando las políticas para ser consideradas a futuro

Proceso Cobit	DSS05: Gestionar los servicios de Seguridad			Código de checklist	2017DS07
Empresa a Auditar	Unión Peruana del Norte	Empresa a cargo		System Auditors	
Área a Auditar	Área de tecnologías de información (TI)		Auditor	Samuel Gavidia	
Práctica de Gestión del Proceso	DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad				

Ítem	Actividad a Evaluar	Nivel de Cumplimiento Actual		
		Si	No	Observación
1	Se registran los eventos relacionados con la seguridad, considerando el nivel de la información.		X	Hay políticas definidas que falta implementar
2	Los registros de seguridad son guardados durante un periodo apropiado para ayudar en futuras investigaciones.		X	Hay políticas definidas que falta implementar
3	La naturaleza y características de los incidentes potenciales relacionados con la seguridad están definidas.	X		
4	La naturaleza y característica de los incidentes potenciales relacionados con la seguridad están comunicadas con el personal.	X		
5	Se revisa regularmente los registros de eventos para la detección de incidentes potenciales.	X		
6	Existe un procedimiento que recopile la evidencia de los incidentes de seguridad.		X	Hay políticas definidas que falta implementar
7	Los empleados conocen los resultados de la recopilación de la evidencia de un incidente de seguridad.		X	Hay políticas definidas que falta implementar

Anexo 52: Informe de la segunda auditoria

INFORME DE AUDITORÍA			
Proceso COBIT	DSS05 - Gestionar servicios de seguridad	**Fecha Auditada**	23/01/18
Área Auditada	Área de tecnología de información (TI) de la Unión Peruana del Norte	**Fecha de entrega de informe**	30/01/18

I. Datos generales de la auditoría:

- **Alcance:**

El alcance de la auditoría fue el Área de TI de la Unión Peruana del Norte. La revisión realizada abarcó los servicios de seguridad según lo especifican las prácticas de gestión del proceso DSS05 - Gestionar los servicios de seguridad del COBIT 5.

- **Criterios de Auditoría:**
  - **COBIT 5**
  - **Proceso DSS05** – Gestionar los Servicios de Seguridad
  - **Prácticas del Proceso:** Actividades del proceso para su evaluación.
    - DSS05.01 – Proteger contra software malicioso.
    - DSS05.02 – Gestionar la seguridad de la red y las conexiones.
    - DSS05.03 – Gestionar la seguridad de los puestos de usuario final.
    - DSS05.04 – Gestionar la identidad del usuario y el acceso lógico.
    - DSS05.05 – Gestionar el accesos físico a los activos de TI.
    - DSS05.06 – Gestionar documentos sensibles y dispositivos de salida.
    - DSS05.07 – Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

- **Objetivo de la Auditoría**

Verificar si los servicios de seguridad implementados en el área de TI de la Unión Peruana del Norte cumplen con lo especificado en las prácticas de gestión del proceso DSS05 - Gestionar servicios de seguridad del COBIT 5.

- **Dependencia Auditada**
  - Área de TI de la Unión Peruana del Norte

- **Equipo Auditor**
  - Luis Daniel Torres Torres
  - Samuel Gavidia Mamani

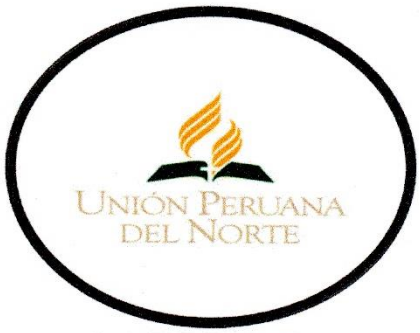
CRITERIOS DE EVALUACIÓN	ESCALA DE EVALUACIÓN			
	No Logrado (0-15%)	**Parcialmente logrado (15% -50%)**	**En gran medida logrado (50% - 85%)**	**Totalmente logrado (85% - 100%)**
C1) DSS05-O1 Las redes y la seguridad de las comunicaciones responden a las necesidades del negocio.			73%	
C2) DSS05-O2 La información procesada, almacenada y transmitida por dispositivos de punto final está protegida.			84%	
C3) DSS05-O3 Todos los usuarios son identificables de forma única y tienen derechos de acceso de acuerdo con su función comercial.				90%
C4) DSS05-O4 Se han implementado medidas físicas para proteger la información del acceso, daño e interferencia no autorizados al ser procesados, almacenados o transmitidos.				100%
C5) DSS05-O5 La información electrónica está debidamente protegida cuando se almacena, transmite o destruye.			73%	

Resultado de la evaluación del proceso	84% - En gran medida logrado

De acuerdo a la Escala de Calificación del PAM, la Gestión de los Servicios de Seguridad en el Área de TI de la Unión Peruana del Norte alcanza el 84% lo que significa que el proceso se encuentra En gran medida logrado.

Anexo 53: Informe de evaluación de la mejora

Informe de evaluación de la mejora



Realizado por:

Gavidia Mamani, Samuel

Torres Torres, Luis Daniel

Tema:

Resultados sobre la investigación realizada en el área de TI, para la mejora del nivel de seguridad física y lógica de la información.

2018

Índice

1. Introducción

Este documento informa sobre las evaluaciones realizadas en el área de Tecnologías de información de la Unión Peruana del Norte, teniendo como objetivo mejorar la seguridad física y lógica de la información, esta auditoria se realizó teniendo como referencia las amenazas que pueden surgir en el día a día en los sistemas de información perjudicando los activos físicos y lógicos que la organización trasmite en todo su entidad, la auditoria consta de dos etapas las cuales mencionan los resultados de cada auditoría realizada.

Teniendo en cuenta los inconvenientes que pueden surgir ocasionando pérdidas y deterioro de infraestructura, se desarrolló este análisis para mejorar el nivel de seguridad de la organización.

2. Objetivo

Verificar que los servicios de seguridad implementados en el área de Tecnologías de información de la Unión Peruana del Norte cumplen con lo especificado en las prácticas de gestión de proceso DSS05 – Gestionar servicios de seguridad del COBIT 5

3. Alcance

El alcance de la auditoria fue el Área de Tecnologías de información de la Unión Peruana del Norte, la revisión realizada abarca los servicios de seguridad según lo especifican las prácticas de gestión del proceso DSS05 – Gestionar los servicios de seguridad del COBIT 5.

4. Resultados de la auditoria

4.1.Resultados de la primera auditoria

4.1.1. DSS05.01 - Proteger Contra Software Malicioso

Durante la primera evaluación en referencia a la primera lista de chequeo, la cual se realizó en base a la práctica de gestión DSS05.01 – "Proteger contra el código malicioso", se formularon 8 ítems que contenían actividades a evaluar, de los cuales permitían con cumplir en gran parte con lo que estipulaba dicha práctica de gestión, obteniendo en esta primera evaluación un porcentaje positivo puesto que de los 8 ítems, 5 de ellos lo realizaba el área de TI de la Unión Peruana de Norte obteniendo un porcentaje de 62% como se puede apreciar en el gráfico, a diferencia del 38% el cual no cumplía con lo que

describía esta práctica, con lo que se espera en la segunda evaluación en cumplir gran parte con lo descrito en esta práctica de gestión. Tal como muestra la figura 1 sobre el nivel alcanzado en esta lista de chequeo.

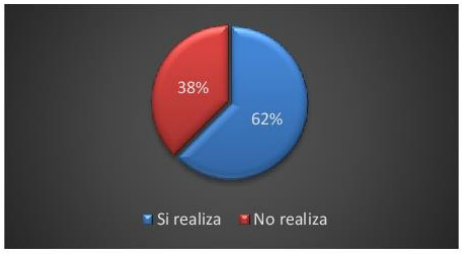


Figura 1: Porcentaje de la primera lista de chequeo – Primera evaluación
(**fuente:** elaboración propia)

4.1.2. DSS05.02 - Gestionar la seguridad de la red y las conexiones

En la primera evaluación en referencia a la segunda lista de chequeo, la cual se realizó en base a la práctica de gestión DSS05.02 – "Gestionar la seguridad de la red y las conexiones", se formularon 8 ítems que contenían actividades a evaluar, de los cuales permitían con cumplir en gran parte con lo que estipulaba dicha práctica de gestión, obteniendo en esta primera evaluación un porcentaje positivo puesto que de los 8 ítems, 5 de ellos lo realizaba el área de TI de la Unión Peruana de Norte obteniendo un porcentaje de 62% como se puede apreciar en el gráfico, a diferencia del 38% el cual no cumplía con lo que describía esta práctica, con lo que se espera en la segunda evaluación en cumplir gran parte con lo descrito en esta práctica de gestión. Tal como muestra la figura 2 sobre el nivel alcanzado en esta lista de chequeo.

Figura 2: Porcentaje de la segunda lista de chequeo – Primera evaluación
(**fuente:** elaboración propia)

.

4.1.3. DSS05.03 - Gestionar la seguridad de los puestos de usuario final

En la primera evaluación en referencia a la tercera lista de chequeo, la cual se realizó en base a la práctica de gestión DSS05.03 – "Gestionar la seguridad de los puestos de usuario final", se formularon 9 ítems que contenían actividades a evaluar, de los cuales permitían con cumplir en gran parte con lo que estipulaba dicha práctica de gestión, obteniendo en esta primera evaluación un porcentaje positivo puesto que de los 9 ítems, 5 de ellos lo realizaba el área de TI de la Unión Peruana de Norte obteniendo un porcentaje de 56% como se puede apreciar en el gráfico, a diferencia del 44% el cual no cumplía con lo que describía esta práctica, con lo que se espera en la segunda evaluación en cumplir gran parte con lo descrito en esta práctica de gestión. Tal como muestra la figura 3 sobre el nivel alcanzado en esta lista de chequeo.

Figura 3: Porcentaje de la tercera lista de chequeo – Primera evaluación (**fuente:** elaboración propia)

4.1.4. DSS05.04 - Gestionar la identidad del usuario y el acceso lógico

En la primera evaluación en referencia a la cuarta lista de chequeo, la cual se realizó en base a la práctica de gestión DSS05.04 – "Gestionar la identidad del usuario y el acceso lógico", se formularon 10 ítems que contenían actividades a evaluar, de los cuales permitían con cumplir en gran parte con lo que estipulaba dicha práctica de gestión, obteniendo en esta primera evaluación un porcentaje no muy positivo puesto que de los 10 ítems, 4 de ellos lo realizaba el área de TI de la Unión Peruana de Norte obteniendo un porcentaje de 40% como se puede apreciar en el gráfico, a diferencia del 60% el cual no cumplía con lo que describía esta práctica, con lo que se espera en la segunda evaluación en cumplir gran parte con lo descrito en esta práctica para su buena gestión y resguardo. Tal como muestra la figura 4 sobre el nivel alcanzado en esta lista de chequeo.

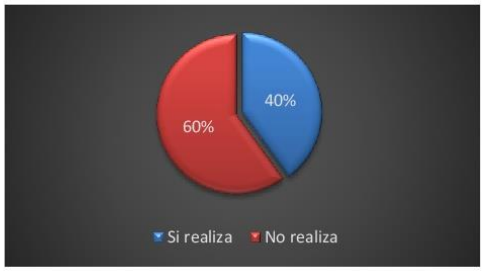


Figura 4: Porcentaje de la cuarta lista de chequeo – Primera evaluación
(**fuente:** elaboración propia)

.

4.1.5. DSS05.05 - Gestionar el acceso físico a los activos de TI

En la primera evaluación en referencia a la quinta lista de chequeo, la cual se realizó en base a la práctica de gestión DSS05.05 – "Gestionar el acceso físico a los activos de TI", se formularon 12 ítems que contenían actividades a evaluar, de los cuales permitían con cumplir en gran parte con lo que estipulaba dicha práctica de gestión, obteniendo en esta primera evaluación un porcentaje aceptable puesto que de los 12 ítems, 7 de ellos lo realizaba el área de TI de la Unión Peruana de Norte obteniendo un porcentaje de 58% como se puede apreciar en el gráfico, a diferencia del 42% el cual no cumplía con lo que describía esta práctica, con lo que se espera en la segunda evaluación en cumplir gran parte con lo descrito en esta práctica de gestión. Tal como muestra la figura 5 sobre el nivel alcanzado en esta lista de chequeo.

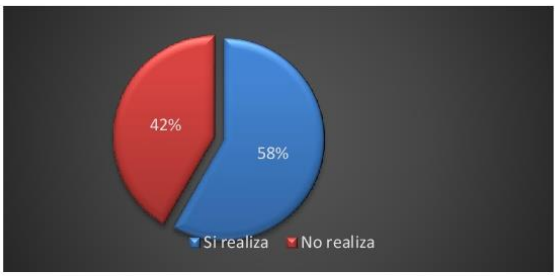


Figura 5: Porcentaje de la quinta lista de chequeo – Primera evaluación
(**fuente:** elaboración propia)

4.1.6. DSS05.06 - Gestionar Documentos sensibles y dispositivos de salida

En la primera evaluación en referencia a la sexta lista de chequeo, la cual se realizó en base a la práctica de gestión DSS05.06 – "Gestionar documentos sensibles y dispositivos de salida", se formularon 11 ítems que contenían actividades a evaluar, de los cuales permitían con cumplir en gran parte con lo que estipulaba dicha práctica de gestión, obteniendo en esta primera evaluación un porcentaje negativo puesto que de los 11 ítems, 3 de ellos lo realizaba el área de TI de la Unión Peruana de Norte obteniendo un porcentaje de 27% como se puede apreciar en el gráfico, a diferencia del 73% el cual no cumplía con lo que describía esta práctica, con lo que se espera en la segunda evaluación en cumplir gran parte con lo descrito en esta práctica de gestión. Tal como muestra la figura 6 sobre el nivel alcanzado en esta lista de chequeo

Figura 6: Porcentaje de la sexta lista de chequeo – Primera evaluación (**fuente:** elaboración propia)

4.1.7. DSS05.07 - Supervisar la infraestructura para detectar eventos relacionados con la seguridad

En la primera evaluación en referencia a la séptima lista de chequeo, la cual se realizó en base a la práctica de gestión DSS05.07 – "Supervisar la infraestructura para detectar eventos relacionados con la seguridad", se formularon 7 ítems que contenían actividades a evaluar, de los cuales permitían con cumplir gran parte con lo que estipulaba dicha práctica de gestión, obteniendo en esta primera evaluación un porcentaje negativo puesto que de los 7 ítems, 2 de ellos lo realizaba el área de TI de la Unión Peruana de Norte obteniendo un porcentaje de 29% como se puede apreciar en el gráfico, a diferencia del 71% el cual no cumplía con lo que describía esta práctica, con lo que se espera en la segunda evaluación en cumplir gran parte con lo descrito en esta práctica de gestión. Tal como muestra la figura 7 sobre el nivel alcanzado en esta lista de chequeo

Figura 7: Porcentaje de la séptima lista de chequeo – Primera evaluación
(**fuente:** elaboración propia)

4.2.Resultados de la segunda auditoria

4.2.1. DSS05.01 – Proteger contra software malicioso

En la segunda evaluación que se desarrolló en el área de TI, tal como fue mencionada en la anterior evaluación se utilizó la práctica de gestión DSS05.01 – "Proteger contra el software malicioso", se formuló 8 ítems que contienen actividades a evaluar, las cuales permiten cumplir gran parte del proceso Cobit, se obtuvo en esta evaluación un porcentaje positivo, logrando cumplir en su totalidad con la lista de evaluación, se cumplió con los 8 ítems, logrando mejorar al 100% en su totalidad a comparación de la anterior evaluación. Tal como muestra la figura 8 sobre el nivel alcanzado en esta lista de cheque

Figura 8: Porcentaje de la primera lista de chequeo – Segunda evaluación
(**fuente:** elaboración propia)

4.2.2. DSS05.02 - Gestionar la seguridad de la red y las conexiones

En la segunda evaluación que se desarrolló en el área de TI, tal como fue mencionada en la anterior evaluación se utilizó la práctica de gestión DSS05.02 – "Gestionar la seguridad de la red y las conexiones", se formuló 8 ítems que contienen actividades a evaluar, las cuales permiten cumplir gran parte del proceso Cobit, se obtuvo en esta evaluación un porcentaje altísimo que permitió mejorar a la anterior evaluación, logrando cumplir con 75% de aprobación y un 25 % que falta implementar, se cumplió con los objetivos trazados anteriormente. Tal como muestra la figura 9 sobre el nivel alcanzado en esta lista de cheque

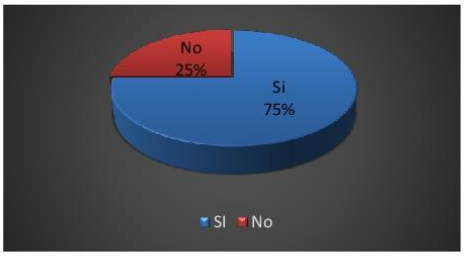


Figura 9: Porcentaje de la segunda lista de chequeo – Segunda evaluación
(**fuente:** elaboración propia)

4.2.3. DSS05.03 - Gestionar la seguridad de los puestos de usuario final

En la segunda evaluación que se desarrolló en el área de TI, tal como fue mencionada en la anterior evaluación se utilizó la práctica de gestión DSS05.03 – "Gestionar la seguridad de los puestos de usuario final", se formuló 9 ítems que contienen actividades a evaluar, las cuales permiten cumplir gran parte del proceso Cobit, se obtuvo en esta evaluación un porcentaje altísimo que permitió mejorar a la anterior evaluación, logrando cumplir con 67% de aprobación y un 33 % que falta implementar, se cumplió con los objetivos trazados anteriormente. Tal como muestra la figura 10 sobre el nivel alcanzado en esta lista de cheque

Figura 10: Porcentaje de la tercera lista de chequeo – Segunda evaluación
(**fuente:** elaboración propia)

4.2.4. DSS05.04 - Gestionar la identidad del usuario y el acceso lógico

En la segunda evaluación que se desarrolló en el área de TI, tal como fue mencionada en la anterior evaluación se utilizó la práctica de gestión DSS05.04 – "Gestionar la identidad del usuario y el acceso lógico", se formuló 10 ítems que contienen actividades a evaluar, las cuales permiten cumplir gran parte del proceso Cobit, se obtuvo en esta evaluación un porcentaje altísimo que permitió mejorar a la anterior evaluación, logrando cumplir con 90% de aprobación en total 9 ítems alcanzados y un 10 % que falta implementar, se cumplió con los objetivos trazados anteriormente. Tal como muestra la figura 11 sobre el nivel alcanzado en esta lista de chequeo

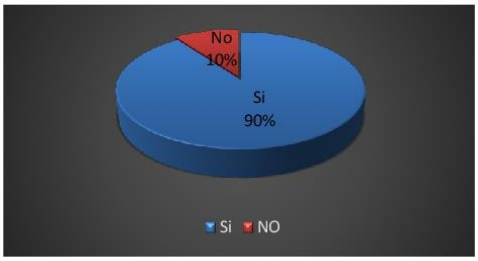


Figura 11: Porcentaje de la cuarta lista de chequeo – Segunda evaluación
(**fuente:** elaboración propia)

4.2.5. DSS05.05 - Gestionar el acceso físico a los activos de TI}

En la segunda evaluación que se desarrolló en el área de TI, tal como fue mencionada en la anterior evaluación se utilizó la práctica de gestión DSS05.05 – "Gestionar el acceso físico a los activos de TI", se formuló 12 ítems que contienen actividades a evaluar, las cuales permiten cumplir gran parte del proceso Cobit, se obtuvo en esta evaluación un porcentaje altísimo que permitió mejorar a la anterior evaluación, se cumplió con los 12 ítems, logrando mejorar al 100% en su totalidad a comparación de la anterior evaluación., se cumplió con los objetivos trazados anteriormente. Tal como muestra la figura 12 sobre el nivel alcanzado en esta lista de chequeo.

Figura 12: Porcentaje de la quinta lista de chequeo – Segunda evaluación
(**fuente:** elaboración propia)

4.2.6. DSS05.06 - Gestionar Documentos sensibles y dispositivos de salida

En la segunda evaluación que se desarrolló en el área de TI, tal como fue mencionada en la anterior evaluación se utilizó la práctica de gestión DSS05.06 – "Gestionar Documentos sensibles y dispositivos de salida", se formuló 11 ítems que contienen actividades a evaluar, las cuales permiten cumplir gran parte del proceso Cobit, se obtuvo en esta evaluación un porcentaje altísimo que permitió mejorar a la anterior evaluación, logrando cumplir con 8 ítems la cual nos muestra el 73% de aprobación y un 27 % quei

falta implementar, se cumplió con los objetivos trazados anteriormente. Tal como muestra la figura 13 sobre el nivel alcanzado en esta lista de chequeo.

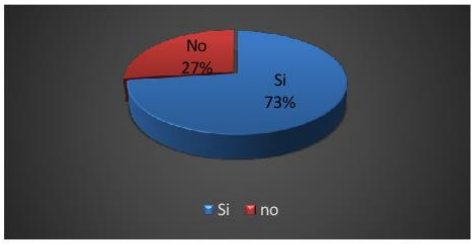


Figura 13: Porcentaje de la sexta lista de chequeo – Segunda evaluación
(**fuente:** elaboración propia)

4.2.7. DSS05.07 - Supervisar la infraestructura para detectar eventos relacionados con la seguridad

En la segunda evaluación que se desarrolló en el área de TI, tal como fue mencionada en la anterior evaluación se utilizó la práctica de gestión DSS05.07 – "Supervisar la infraestructura para detectar eventos relacionados con la seguridad", se formuló 7 ítems que contienen actividades a evaluar, las cuales permiten cumplir gran parte del proceso Cobit, se obtuvo en esta evaluación un menor por que permitió reducir a la anterior evaluación, no se logró en su totalidad aprobar la lista de chequeo pero aumento la aprobación del porcentaje como lista de chequeo un 43% positivo y un 57% negativo que falta implementar, falta cumplir con la mejora de esta lista de chequeo. Tal como muestra la figura 14 sobre el nivel alcanzado en esta lista de chequeo.

Figura 14: Porcentaje de la primera lista de chequeo – Segunda evaluación
(**fuente:** elaboración propia)

5. Comparación de auditoria primera y segunda evaluación

5.1. Cuadro de Comparabilidad

Durante la etapa de auditoria se realizó dos evaluaciones para medir en el nivel que se encuentra la seguridad de la información en la Unión Peruana del Norte, esto permite conocer al detalle cómo se cumplió los criterios de evaluación del PAM de Cobit, los 5 criterios de evaluación que te brinda el PAM se asocian a las 7 prácticas de gestión definidas por el proceso DSS05- Gestionar la servicios de seguridad.

Logrando ver el figura 15 que en la primera evaluación de color azul, las 5 prácticas están por debajo de lo previsto llegando a cumplir el 100% en cada criterio de evaluación, alcanzando un 47% que significa que se encuentra el nivel de seguridad "**Parcialmente logrado**" la segunda escala que el PAM define, luego vemos que en la segunda de evaluación de color rojo hay un incremento en el porcentaje luego de la implementación de los controles, alcanzado un 84% en el nivel de seguridad "**En gran medida logrado**" mejorando la seguridad de la información de la Unión Peruana del Norte, cumpliendo con los objetivos trazados en la investigación.

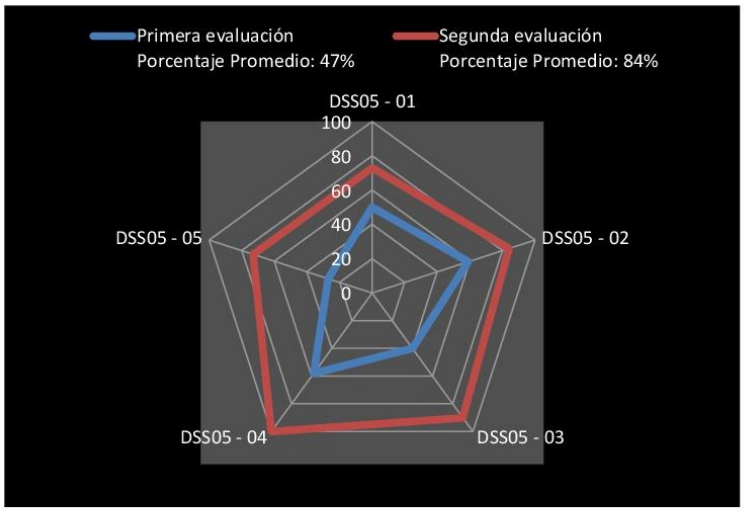


Figura 15: Comparativa de Resultados de la Primera evaluación con la Segunda evaluación usando los criterios de evaluación del PAM *(***Fuente:** *Elaboración propia)*

5.2.Mejoras en seguridad física

La mejora en seguridad física en la organización fue:

- Se le brindo Políticas de Acceso físico
- Se le brindo restricciones para impedir el acceso a instalaciones
- Se realizó un formato para la solicitud de petición de acceso
- Se gestionó correctamente la gestión de solicitud de peticiones de acceso, mediante registros
- Se le brindo un identificador (fotocheck) a los visitantes y Operarios para que acceden al área de TI, esto para tener un mejor control
- Se estableció compromisos con el personal que labora dentro
- Se realizó registros de aquellas personas que no cuenten con un identificador y que no están escoltadas por un responsable del área
- Se realizó capacitaciones sobre las distintas amenazas que pueden surgir dentro de la organización
- Se realizó un registro las capacitaciones brindadas a los usuarios
- Se realizó un inventario de los activos físicos de información
- Se realizó un registro de inventariado de dispositivos de salida y de documentos sensibles
- Se realizó un proceso de clasificación de documentos sensibles de información
- Se establecieron formatos para la eliminación de equipos tecnológicos y mecanismos para la eliminación de la información

5.3.Mejoras en seguridad lógica

La mejora en seguridad física en la organización fue:

- Se le brindo políticas de control de acceso lógico
- Se le brindo un procedimiento de Gestión de Vulnerabilidades
- Se le brindo un procedimiento para la protección contra el Código malicioso
- Se le brindo un procedimiento seguro sobre la Gestión de acceso de usuarios
- Se le brindo un procedimiento de Inicio de Sesión
- Se le brindo un manual de cómo cumplir la criptografía en la organización
- Se le brindo un manual de políticas sobre las redes y comunicaciones
- Se realizó un inventario de los activos de software
- Se realizó un proceso de clasificación de activos de información lógico
- Se realizó un registro sobre las capacitaciones y entrenamiento sobre software malicioso brindada a los usuarios de TI
- Se realizó un registro de amenazas lógicas ligadas al código malicioso
- Se realizó un registro de los dispositivos autorizados a la información y a la red

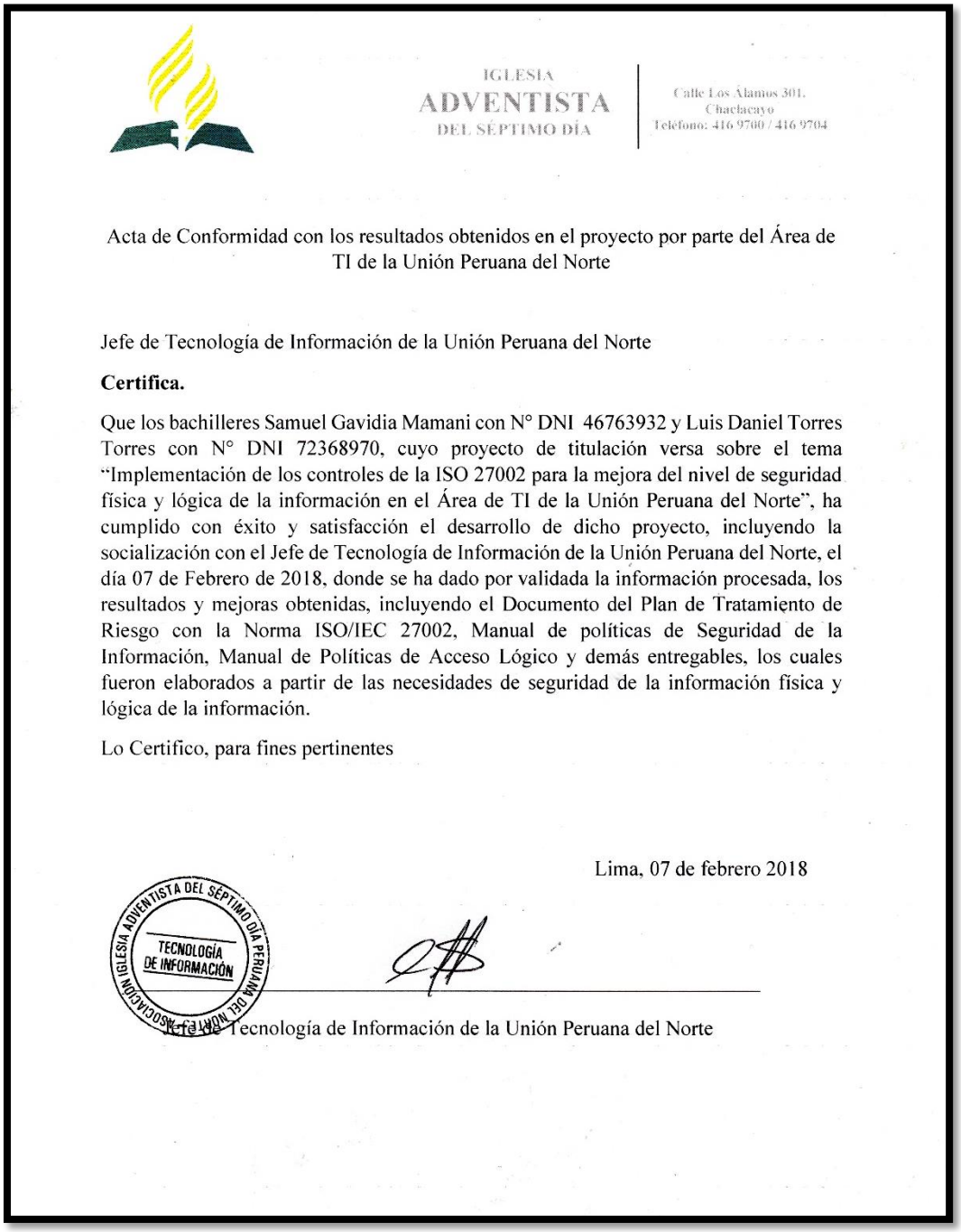
- Se realizó un registro de los derechos de acceso según los roles y responsabilidades de los usuarios

Todo lo realizado en la seguridad lógica y física de la información, ayudaran a tener segura e integra la información y así cumplir con el objetivo de mejorar en gran medida la seguridad de la información.

6. Conclusiones

- La lista de chequeo son instrumentos que muestran el resultado de la primera y segunda evaluación, el cumplimiento de los objetivos y del alcance, por ello son importantes para realizar mejoras y un análisis correcto.
- La auditoría de sistemas es un instrumento que se adapta a cualquier organización, brindando procesos que mejoren las inversiones de la organización, teniendo un mejor control del presupuesto en la organización.
- Los procesos Cobit brinda prácticas de gestión que ayudan a mejorar en gestión, seguridad, administración, informática, etc. Estableciendo actividades que puedan brindar soluciones para mejoras futuras.
- Realizar el análisis de riesgo ayuda a gestionar y tener un mejor control sobre los riesgos identificados.
- Elaborar un plan de tratamiento de riesgo ayuda establecer los controles los cuales ayudaran a reducir los riesgos que fueron identificados durante el análisis de riesgo, y así tener un mejor control sobre estos, para de esta manera tener integra y protegida la información.

Anexo 54: Acta de Conformidad con los resultados obtenidos en el proyecto por parte del Área de TI de la Unión Peruana del Norte



IGLESIA ADVENTISTA DEL SÉPTIMO DÍA

Calle Los Álamos 301,
Chaclacayo
Teléfono: 416 9700 / 416 9704

Acta de Conformidad con los resultados obtenidos en el proyecto por parte del Área de TI de la Unión Peruana del Norte

Jefe de Tecnología de Información de la Unión Peruana del Norte

Certifica.

Que los bachilleres Samuel Gavidia Mamani con N° DNI 46763932 y Luis Daniel Torres Torres con N° DNI 72368970, cuyo proyecto de titulación versa sobre el tema "Implementación de los controles de la ISO 27002 para la mejora del nivel de seguridad física y lógica de la información en el Área de TI de la Unión Peruana del Norte", ha cumplido con éxito y satisfacción el desarrollo de dicho proyecto, incluyendo la socialización con el Jefe de Tecnología de Información de la Unión Peruana del Norte, el día 07 de Febrero de 2018, donde se ha dado por validada la información procesada, los resultados y mejoras obtenidas, incluyendo el Documento del Plan de Tratamiento de Riesgo con la Norma ISO/IEC 27002, Manual de políticas de Seguridad de la Información, Manual de Políticas de Acceso Lógico y demás entregables, los cuales fueron elaborados a partir de las necesidades de seguridad de la información física y lógica de la información.

Lo Certifico, para fines pertinentes

Lima, 07 de febrero 2018

IGLESIA ADVENTISTA DEL SÉPTIMO DÍA ASOCIACIÓN PERUANA DEL NORTE
TECNOLOGÍA DE INFORMACIÓN

Jefe de Tecnología de Información de la Unión Peruana del Norte