UNIVERSIDAD PERUANA UNIÓN
FACULTAD DE INGENIERÍA Y ARQUITECTURA
Escuela Profesional de Ingeniería de Sistemas

Seguridad de la información en el proceso de desarrollo de sistemas y del producto mediante la implementación de controles de seguridad basado en la norma ISO 27002:2015 en la empresa BITNESS CORP S.A.C., 2020

Tesis para optar al Título Profesional en Ingeniero de Sistemas

Por

Bach. Gaby Milagros Alvarado Limaymanta

Bach. Miryam Raquel Sánchez Torre

Asesor:

Mg. Lizeth Geanina Huanca López

Lima, 2020

DECLARACIÓN JURADA

DE AUTORÍA DEL INFORME DE LA TESIS

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

DECLARO:

Que el presente informe de investigación titulado **"Seguridad de la información en el proceso de desarrollo de sistemas y del producto mediante la implementación de controles de seguridad basado en la norma ISO 27002:2015 en la empresa BITNESS CORP S.A.P., 2020"** constituye la memoria que presentan las Bachilleres Gaby Milagros Alvarado Limaymanta y Miryam Raquel Sánchez Torre, para aspirar al título profesional de Ingeniero de Sistemas, ha sido realizada 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 el presente documento en Lima, el 06 de junio del año 2021.

Mg. Huanca López, Lizeth Geanina

ACTA DE SUSTENTACIÓN DE TESIS

EnLima, Ñaña,VillaUnión, alos **07** días día(s)delmes de **mayo** del año **2021** siendo las **08:30** horas,sereunieron en modalidad virtual u online sincrónica, bajo la dirección del Señor Presidente del jurado: **Dra. Erika Inés Acuña Salinas**, el secretario: **Mg. Daniel Lévano Rodríguez** … y los demás miembros: **Mg. Fernando Manuel Asin Gomez** y la **Mg. Geraldine Verónica Alvizuri Llerena** …. y el asesor **Mg. Lizeth Geanina Huanca López**, con el propósito de administrar el acto académico de sustentación de la tesis titulada**:"Seguridad de la información en el proceso de desarrollo de sistemas y del producto mediante la implementación de controles de seguridad basado en la norma ISO 27002:2015 en la empresa BITNESS CORP S.A.C., 2020"** ……de el(los)/la(las) bachiller/es: a)…….**GABY MILAGROS ALVARADO LIMAYMANTA**.....…… b)……**MIRYAM RAQUEL SÁNCHEZ TORRE**…… ……conducente a la obtención del título profesional de ….....…….....INGENIERO DE SISTEMAS……..……..……..… Nombre del Título Profesional) con mención en…….....

El Presidente inició el acto académico de sustentación invitando …a los … candidato(a)/s hacer uso del tiempo determinado para su exposición. Concluida la exposición, elPresidente invitó a los demás miembros del jurado a efectuarlas preguntas, y aclaraciones pertinentes, las cuales fueron absueltas por … los … candidato(a)/s. Luego, se produjo un receso para las deliberaciones y la emisión del dictamen del jurado. Posteriormente, el jurado procedió a dejar constancia escrita sobre la evaluación en la presente acta, con el dictamen siguiente:

Candidato (a): …… GABY MILAGROS ALVARADO LIMAYMANTA

CALIFICACIÓN	ESCALAS			Mérito
	Vigesimal	Literal	Cualitativa	
Aprobado	17	B+	Con nominación muy bueno	Sobresaliente

Candidato (b): …… MIRYAM RAQUEL SÁNCHEZ TORRE

CALIFICACIÓN	ESCALAS			Mérito
	Vigesimal	Literal	Cualitativa	
Aprobado	17	B+	Con nominación muy bueno	Sobresaliente

(*) Ver parte posterior

Finalmente, el Presidente del jurado invitó … a los … candidato(a)/s a ponerse de pie, para recibir la evaluación final y concluir el acto académico de sustentación procediéndose a registrar las firmas respectivas.

Presidente Dra. Erika Inés Acuña Salinas		Secretario Mg. Daniel Lévano Rodríguez
Asesor Mg. Lizeth Geanina Huanca López	Miembro Mg. Fernando Manuel Asin Gomez	Miembro Mg.Geraldine Veronica Alvizuri Llerena
Candidato/a (a) Gaby Milagros		Candidato/a (b) Miryam Raquel

DEDICATORIA GABY

Dedico con todo mi corazón mi tesis a mis padres
por estar siempre motivándome a seguir cumpliendo
mis metas, también el apoyo incondicional de mi pareja.
Asimismo para la personita mas importante en mi vida
mi hijo quien es la razón de seguir esforzándome cada dia más.
Es por ello que les dedico mi trabajo que con mucho
esfuerzo y animó me ayudaron a lograrlo.

DEDICATORIA MIRYAM

A Dios por darme la vida, salud y fuerzas para culminar esta meta tan importante. A mis padres Luis y Raquel, por el apoyo incondicional. A mis hermanos Isabel, Silvia y Rafaelito por su aliento sincero y porque siempre estuvieron ahí cuando los necesite. A mi tía Carmen Cecilia por motivarme y ser una gran consejera. A mi novio Sergi, quien me apoyo y me motivo durante todo este proceso. Muchas gracias a cada uno de ustedes por estar presentes no solo en esta meta cumplida sino por estar siempre presentes en mi vida.

AGRADECIMIENTOS

Agradecemos a Dios por hacer que culminemos una etapa más como profesionales en nuestras vidas.
A la Mg. Lizeth Geanina Huanca López, por su asesoramiento, por su dirección y por compartir sus conocimientos durante el desarrollo del proyecto de tesis. A la escuela de Ingeniería de Sistemas de la Universidad Peruana Unión, a la Dra. Erika Acuña, al Mg. Daniel Lévano, Ing. Fernando Asin y a la Mg. Geraldine Alvizuri por brindarnos su tiempo y enseñanzas para seguir creciendo en nuestros propósitos.

INDICE

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

LISTADO DE ANEXOS

RESUMEN

Esta tesis tiene por objetivo mejorar el nivel de seguridad durante el desarrollo del sistema y del producto en la empresa BITNESS CORP. S.A.C.

En base a la norma ISO/IEC 27002:2015, se diseño el Instrumento de Evaluación el cual es la base de la investigación.

Se implementó una metodología de elaboración propia, para el desarrollo del proyecto, la cual se complementó en 4 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 estableció el primer contacto con la empresa BITNESS CORP. S.A.C. para la cual se desarrolló el diseño el instrumento de evaluación. El cual permitió conocer el nivel de seguridad inicial que posibilitó establecer un compromiso para la implementación del proyecto.

En la fase 2 se diseñaron las propuestas de las oportunidades de mejora priorizadas con el objetivo de mejorar el nivel de seguridad de acuerdo al contexto actual. Estas oportunidades de mejora fueron presentadas formalmente a la empresa BITNESS CORP. S.A.C. para su aprobación.

En la fase 3 se implementó las oportunidades de mejora diseñadas, conforme al contexto actual. Se contó con la participación activa del personal de BITNESS CORP. S.A.C. en las capacitaciones informativas.

En la fase 4 se realizó la evaluación final con la implementación de los controles basados en la ISO 27002: 2015 obteniendo como resultado las mejoras del nivel de seguridad.

La implementación de los controles de seguridad mejoró significativamente el nivel de seguridad con un 81.80% en la empresa BITNESS CORP. S.A.C.

Palabras Claves: Controles de seguridad, ISO 27002:2015, Nivel de seguridad de la Información.

INTRODUCCIÓN

Actualmente, la seguridad de la información es un punto importante en toda organización. Se necesita proteger y salvaguardar la información ante cualquier amenaza.

Tener la inseguridad de la información 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 empresa BITNESS CORP. S.A.C., una empresa dedicada el desarrollo de sistemas y marketing digital necesita proteger la información brindada por sus clientes para el desarrollo de sistemas.

Para la investigación realizada se le brindo a la organización documentos, registros, procesos y políticas de seguridad de la información, establecidas por los controles de la norma ISO/IEC 27002:2015, que permiten mejorar el nivel de la seguridad de la organización.

Este trabajo de investigación esta compuesto por 7 capitulos que se describen a continuación:

En el capitulo 1 se realiza la definición de los objetivos generales como específicos que se tuvieron presentes en la elaboración del proyecto. A su ves, se referenciaron casos en los cuales las carencias de normas y/o políticas de seguridad causaron problemas frecuentes.

En el capitulo 2 se profundizará más en el tema sustentándonos en cada una de las partes que conforman la matriz de trazabilidad.

En el capitulo 3 se describe la metodología de investigación a trabajar, las variables y sus indicadores y la obtención de la información.

En el capitulo 4 se realiza la descripción del objetivo de estudio siendo la empresa BITNESS CORP. S.A.C.

En el capitulo 5 se realiza la ingeniería de la propuesta de investigación, que consta de 4 fases.

En el capitulo 6 se analizaron y discutieron los resultados de la implementación de los controles de seguridad de la ISO 27002:2015. .

En el capitulo 7 se describen las conclusiones y recomendaciones para la empresa BITNESS CORP. S.A.C.

CAPÍTULO I:

EL PROBLEMA

1.1. TÍTULO DE LA INVESTIGACIÓN

Seguridad de la información en el proceso de desarrollo de sistemas y del producto mediante la implementación de controles de seguridad basado en la norma ISO 27002:2015 en la empresa BITNESS CORP S.A.C., 2020.

1.2. PROBLEMA OBJETO DE INVESTIGACIÓN

1.2.1. IDENTIFICACIÓN DEL PROBLEMA

En ese sentido [1], en referencia a Aguirre y Aristizabal advierten que el desarrollo de las tecnologías aumenta el riesgo de ataques cibernéticos en las organizaciones, se deben tomar medidas que ayuden con la protección de la información.

Por otro lado, en el boletín de seguridad de Kaspersky 2019 hace referencia que el 19,8% de los equipos de usuarios sufrieron al menos una vez un ataque web de la clase malware. El antivirus web registró 273 782 113 URL únicas que provocaron reacciones del antivirus web. Se registró 24 610 126 objetos maliciosos únicos. Todos los datos estadísticos se obtuvieron de la red de nube global Kaspersky Security Network, esta recibe información de los componentes de soluciones de seguridad de 203 países de todo el mundo. [2]

El reporte de ESET Security 2019 en Latinoamérica refiere que el 61% de las empresas sufrió por lo menos un accidente de seguridad, siendo la infección con códigos maliciosos lo más frecuente. La mitad de los incidentes son de ransomware. El número de casos de ransomware disminuyó en un 10%. [3]

Tras el avance tecnológico se han encontrado herramientas que permiten tener una gestión total en las organizaciones con ello se logra proteger la información importante de las organizaciones. Cuando las organizaciones no poseen controles para lograr un sistema de gestión de la seguridad de la información, pueden ocurrir graves prejuicios en la organización. La seguridad de la información debe ser un objetivo importante en toda organización y a su vez debe establecer puntos importantes como: las políticas de seguridad de la información, requisitos de la seguridad de la información, políticas de desarrollo seguro, control de cambios, pruebas funcionales, protección de datos, entre otros.

La entidad a investigar es la empresa BITNESS CORP. S.A.C., es una empresa neófita dedicada al desarrollo de software. BITNESS CORP. S.A.C. desarrolla todo tipo de sistemas para empresas de cualquier índole. Tras haber realizado entrevistas al Gerente de Operaciones se detectaron problemas como el manejo inadecuado de los requisitos de desarrollo de sistemas, no existe un procedimiento o proceso para los cambios del sistema, la empresa no advierte a los empleados la importancia de no difundir información de la organización, la falta de documentación de la metodología de desarrollo, entre otros. Como resultado ante estos problemas, la seguridad de la información esta expuesta a cualquier tipo de amenazas como: perdida de la información, establecer passwords fácilmente vulnerables, copias de respaldo mal realizados, excesiva confianza a los empleados, etc.

El punto de partida de todo proyecto de desarrollo de sistemas es la identificación de los requisitos de seguridad, esta información es confidencial tanto para el cliente como para el equipo de desarrollo, por lo tanto esta información debería ser protegida. La situación de no tener cuidado o protección sobre la información puede provocar diversos riesgos como: perdidas, fallas en la información o que cualquier persona no autorizada pueda acceder a ella.

Otro punto importante, es que cada vez que se identifica una necesidad de cambio no hay un registro de ello. Estos cambios no son evaluados, ni clasificados de acuerdo al estado critico que puedan alcanzar, simplemente se realizan sin hacer ningún tipo de medición de las consecuencias que puedan afectar la seguridad de la información. En consecuencia los riesgos que pueden ocurrir son: soluciones ineficientes, problemas de implementación en el entorno de aplicación del cambio o la redefinición de requisitos.

Asimismo, un problema que se ha detectado es la excesiva confianza que el Gerente de Operaciones tiene en los miembros del equipo de desarrollo siendo similar a la confianza que se tiene en una familia porque son conocidos o amigos. Pero que según los estándares de calidad para mantener una mejor seguridad de la información todos los integrantes de un equipo de desarrollo deberían firmar un contrato o convenio de confidencialidad sobre la información que van a utilizar. Los posibles riesgos que se darían al no cumplir con este criterio es: robo de información, extorsión por parte de los empleados, distribución de información no autorizada, entre otros.

En ese sentido como investigadoras nos sentimos motivadas a proponer la implementación controles de seguridad para la mejora del nivel de seguridad de la información en el proceso de desarrollo de sistemas y del producto.

1.2.2. FORMULACIÓN DEL PROBLEMA

A. PROBLEMA GENERAL

¿En qué medida la implementación de los controles de seguridad basado en la norma ISO 27002:2015 mejoran la seguridad de la información en el proceso de desarrollo de sistemas y del producto de la empresa BITNESS CORP. S. A. C., 2020?

B. PROBLEMAS ESPECÍFICOS.

¿En qué medida la implementación de los controles de seguridad basado en la norma ISO 27002:2015 mejoran la seguridad de la información en el proceso de desarrollo de sistemas de la empresa BITNESS CORP. S. A. C., 2020?

¿En qué medida la implementación de los controles de seguridad basado en la norma ISO 27002:2015 mejoran la seguridad de la información del producto de la empresa BITNESS CORP. S. A. C., 2020?

1.3. OBJETIVOS.

1.3.1. OBJETIVO GENERAL.

Determinar la mejora de la seguridad de la información en el proceso de desarrollo de sistemas y del producto con la implementación de controles basado en la norma ISO 27002:2015 en la empresa BITNESS CORP. S.A.C., 2020.

1.3.2. OBJETIVOS ESPECÍFICOS

- Determinar la mejora de la seguridad de la información en el proceso de desarrollo de sistemas con la implementación de controles basado en la norma ISO 27002:2015 en la empresa BITNESS CORP. S.A.C., 2020.
- Determinar la mejora de la seguridad de la información del producto con la implementación de controles basado en la norma ISO 27002:2015 en la empresa BITNESS CORP. S.A.C., 2020.
-

1.4. JUSTIFICACIÓN.

1.4.1. JUSTIFICACIÓN TEÓRICA.

La seguridad de información que las entidades emplean en la actualidad gracias a la norma ISO 27002: 2015, es muy importante ya que mediante las evaluaciones que se realizan se identifican los posibles carencias a las que están expuestos. Debido a esta circunstancia, la presente investigación aporta un instrumento de evaluación de seguridad de la información del producto (sistema) y en las etapas del proceso de desarrollo de sistemas basado en la norma ISO 27002: 2015. Ante la evaluación y análisis de los resultados se diseñarán medidas preventivas que mitigarán las diversas amenazas a las que estan expuestas actualmente los sistemas de información de la empresa BITNESS CORP. S.A.C.

1.4.2. JUSTIFICACIÓN PRÁCTICA

Mediante los resultados obtenidos gracias a la implementación de los controles de seguridad basados en la norma ISO 27002: 2015 la empresa tendrá como beneficio práctico el control de la seguridad del sistema desde las primeras etapas de desarrollo, mantener un seguimiento de cambios del sistema, generando documentación relativa para la seguridad de la información que contemple procedimientos de cumplimiento y responsabilidades en todos los niveles. Estas oportunidades de mejora como: métodos, procedimientos y documentos permitirán mantener un entorno de desarrollo seguro durante las etapas de desarrollo de sistemas y del producto en la empresa BITNESS CORP S.A.C., mejorando el nivel de seguridad de la información en base a la confidencialidad, integridad y disponibilidad.

1.5. ALCANCES DE LA INVESTIGACIÓN.

La investigación se elabora en base a los principios básicos de la Seguridad de la Información de acuerdo a la norma ISO 27002: 2015, enfocándose en el dominio 14 siendo la Adquisición, desarrollo y mantenimiento de los sistemas de información, que enmarcan las disposiciones sobre la seguridad que deben darse a lo largo de las etapas del desarrollo de sistemas y que deben constituir al sistema. La implementación de los lineamientos y normas consagrados en la presente investigación, se han realizado progresivamente de acuerdo a la prioridad establecida una vez ejecutado el instrumento. Esta prioridad se define de acuerdo a las necesidades de la empresa y el contexto actual.

1.6. LIMITACIONES DE LA INVESTIGACIÓN.

De acuerdo a las limitaciones identificadas en la presente investigación, el factor tiempo ha sido primordial para la implementación de los controles. Se deja de lado aquellos controles que requieren una ejecución presencial y que conllevan un plazo extenso en su ejecución. Otra de las limitaciones ha sido la situación actual, dado que nos encontramos en estado de emergencia por el COVID 19, que perjudica la presencia física en la unidad de estudio por lo cual se han realizado todas las reuniones con el jefe de desarrollo de software de manera virtual.

CAPÍTULO II:

MARCO TEÓRICO CONCEPTUAL

2.1. ANTECEDENTES.

Bermúdez, realizó la tesis titulada "Análisis en seguridad informática de la información basado en la Norma ISO/IEC 27001- Sistemas de Gestión de Seguridad de la Información dirigido a una empresa de servicios financieros" tiene como finalidad reconocer las vulnerabilidades a las que está expuesta la información por la falta de aplicación de controles de seguridad. El objetivo del proyecto de investigación fue el estudio de la seguridad en los procesos críticos, a través de diversos procesos se identificaron los riesgos a los cuales se exponen los datos físicos, lógicos y sistemas de procesamiento de información. El análisis de riesgos da a conocer el nivel de impacto que tiene la ocurrencia de amenazas identificadas pudiendo afectar las actividades propias del negocio. Los resultados reconocen que para minimizar los riesgos existentes es necesario implementar controles de seguridad que fortalecen los aspectos importantes de la seguridad de la información. El estudio contempla una investigación de campo porque se apoya de la información levantada y obtenida mediante observaciones del proceso y reuniones, es descriptiva porque se detalla las actividades llevadas a cabo en los procesos conociendo las falencias que se presentan, es no experimental porque no se puede modificar deliberadamente y es explicativo porque establece aspectos que causan el objeto de investigación. El estudio establece como conclusiones: los activos de información de las áreas consideradas críticas y la situación de la empresa refleja potenciales riesgos que exponen la información a daños, robo o modificaciones pudiendo causar un impacto negativo en el negocio. La implementación de controles de seguridad basados en la Norma ISO/IEC 27001 mejora las características de confiabilidad, integridad y disponibilidad, a su vez se reconoce que la seguridad total no existe, pero la gestión de controles de seguridad en el proceso y manejo de información es un complemento esencial y asegura la información de la empresa y de los clientes. [4]

Guzmán, desarrollo la tesis titulada "Metodología para la seguridad de tecnologías de información y comunicaciones en la Clínica Ortega" refiere que los sistemas de gestión e información contienen diversos procesos, por ello requieren ser seguros para preservar la calidad de los servicios y velar por la eficacia y eficiencia de los procesos de negocio. Se

busca proponer una metodología que mejore la seguridad de tecnologías de información y comunicaciones que además integre lo mejor de cada enfoque. A su vez se describen las características y funcionalidades deseables de un software que apoya la metodología. Se menciona que los requisitos de seguridad de los sistemas incluyen la infraestructura, las aplicaciones de negocio y las aplicaciones desarrolladas por el usuario. Las aplicaciones deben tener medidas de control y registros de actividad, validar datos de entrada, el tratamiento interno y los datos de salida. El estudio contempla una investigación descriptiva porque mide o recoge información sobre conceptos o variables, es de tipo analítico o explicativo porque analiza y explica las metodologías de seguridad. El estudio establece como conclusiones: el análisis de riesgos detectó las amenazas hacia los activos y los requerimientos, esto delimitó el modelo y la estructura. El modelo de seguridad propuesto implementa controles de seguridad para cada uno, midiendo el nivel de seguridad a través de una valoración. Para el desarrollo del modelo de seguridad se tuvo en cuenta las Normas técnicas y el modelo ISO. Finalmente se implementaron controles de seguridad que deben ser supervisados, revisados y deben estar en constante movimiento. [5]

Contero, realizó la tesis "Diseño de una política de seguridad de la información basada en la norma ISO 27002:2013, para el sistema de botones de seguridad del Ministerio del Interior", menciona que la problemática del sistema era que no contaban con un procedimiento y controles en la asignación de perfiles y cuentas de usuario, administración de servicios y además procesos internos, por lo cual eran vulnerables ante cualquier amenaza que pueda afectar la seguridad de la información, debido a ello como objetivo se propuso diseñar una política de seguridad de la información basada en la ISO 27002:2013 que permite establecer las medidas necesarias para garantizar la seguridad de la información de la plataforma tecnológica del sistema, el tipo de investigación es no experimental. Asimismo, la metodología que se utilizó fue Magerit para el análisis de riesgos y mediante ello tomar decisiones del uso de las tecnologías de la información y sus entornos, en conclusión, se llegó a seleccionar 25 controles de la ISO 27002 los cuales se adaptan mejor a minimizar el riesgo logrando así diseñar políticas de seguridad para el sistema.[6]

Sota & Mechan, efectuó la tesis titulada "Implementación de controles y cumplimiento de requisitos de la ISO/IEC 27001:2013 para la seguridad de información en

una PYME consultora" da a conocer que la problemática es la deficiencia en la seguridad de la información, está se encontraba disponible para todo el personal. Asimismo, se identificó la carencia de concientización y capacitación al personal acerca de la seguridad de la información. cuyo objetivo es identificar el nivel de cumplimiento de la norma ISO/IEC 27001:2013, realizando análisis de brechas tanto de los requisitos como de los controles, el tipo de investigación es no experimental y la metodología que se usó para el desarrollo de la investigación fue el Ciclo DEMING, el cual se divide en cuatro fases: planear, hacer, verificar y actuar; para establecer, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI). Como resultado, se consiguió mejorar la seguridad de la información, se identificó el estado de cumplimiento inicial y final de la ISO/IEC 27001:2013 en la empresa. Además, se realizó la evaluación de riesgos, la implementación de los controles, el cumplimiento de los requisitos y la concientización del personal. Todo esto sirvió para sentar las bases hacia una certificación futura en dicha norma.[7]

Romo & Valarezo, realizó la tesis titulada "Análisis e implementación de la norma ISO 27002 para el Departamento de Sistemas de la Universidad Politécnica Salesiana sede Guayaquil", realiza la investigación acerca de las buenas prácticas de la seguridad de la información teniendo como objetivo el impedir los accesos no autorizados, violaciones de las normas, reglamentos, políticas y procedimientos de los estándares de seguridad en la Universidad Politécnica Salesiana, ya que una gran preocupación para la universidad es el control de riesgos que atenta contra la seguridad de la información de sus activos, tras observar el departamento de sistemas encontraron factores de inseguridad, fuga de información, entre otros que ocasionaron daños económicos y de prestigio. Para reducir estos riesgos es necesaria la elaboración de normas y políticas basadas en normas de las buenas prácticas. El estudio contempla una investigación descriptiva porque se trabajó con actividades, procedimiento y características para comprobar los riesgos por la falta de políticas a su vez es experimental porque se definen políticas para reducir riesgos. La investigación fue realizada con el método científico, ya que se rige y alinea a la norma ISO/IEC 27002:2005; con el método deductivo, plantea una guía de implementación aplicada a todo tipo de organización; con el método inductivo; basada en datos particulares (investigación) para realizar políticas generales y detalladas. El estudio establece las siguientes conclusiones: Se detectaron muchas deficiencias por parte de la seguridad de la

información. Resaltan que al cumplirse el 100% de las políticas desarrolladas no se garantiza que no sucedan problemas de seguridad al 100% con el cumplimiento del manual se minimiza los riesgos asociados a los activos, gracias al manual diseñado para la Universidad se proporciona una guía para trabajar aspectos de seguridad. El departamento de Sistemas de la universidad debe realizar proyectos de enmendadura basados en las políticas de seguridad.[8]

Huacanés, desarrollo la tesis "Implementación de la norma ISO 27002:2013, sección "Control de Acceso" para las aplicaciones informáticas de la Aseguradora del Sur", realiza un estudio con el propósito de administrar los aplicativos de la Aseguradora del Sur a través del proceso de seguridad de información, estableciendo políticas y procedimientos que garanticen disponibilidad, integridad, confidencialidad, control de accesos y legalidad de información. En ese sentido Huacanés observó que existía un proyecto de políticas de seguridad de la información fundamentado en estándares internacionales pero que se encontraba suspendido y por lo poco implementado empíricamente, dicho proyecto nos habla del "Control de acceso de aplicaciones", las aplicaciones de la Aseguradora del Sur poseen una diversidad de arquitecturas. No existe un inventario ni perfiles de acceso, además de no presentarse un sistema confidencial. El estudio contempla la metodología científica, deductiva e inductiva que se alinean al ISO 27002:2013, se aplica una investigación experimental porque se identifican riesgos y se definen políticas para reducirlos. La investigación concluye que el acceso de aplicaciones de la Aseguradora del Sur presenta riesgos en la integridad de la información. Teniendo en cuenta la diversidad de las aplicaciones no es posible aplicar el control de acceso en todas. Se cumple parcialmente con lo establecido en el estándar ISO 27001:2013, esto minimizará los riesgos asociados a los activos de la información.[9]

Gavidia & Torres, efectuó la tesis "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" tiene como objetivo mejorar el nivel de seguridad física y lógica de la información del área de TI, la problemática que se encontró en la Unión Peruana del Norte fue que carecían de una infraestructura apropiada para el desarrollo de sus actividades, además se observaba que no tenían un buen manejo en sus políticas de seguridad

de la información por lo que se observó un bajo nivel de gestión de la seguridad física y lógica de la información. Mediante una entrevista con el personal de TI manifestó que como consecuencia de ello era muy probable que se dieran ataques y riesgos en los activos de la información es por ello que se utilizó la ISO/IEC 27002:2013 juntamente con los framework objetivos de control para la información y tecnologías relacionadas al modelo COBIT. La metodología que se usó consta de 5 fases: a) Estudio de la organización, b) Evaluación del nivel de seguridad con COBIT, c) Análisis de riesgos de TI, d) Elaboración del plan de tratamiento de riesgo con la ISO 27002, e) Evaluación de la mejora del nivel de seguridad con la ISO 27002. Asimismo, el tipo de investigación que se realizó fue aplicada debido a que el estudio de la problemática se realizó en el área de TI con la finalidad de obtener resultados confiables y satisfactorios en dicha área. Finalmente se obtuvo como resultado un cuadro comparativo de la primera evaluación que se realizó mediante los criterios de evaluación del PAM de COBIT se asocian a las 7 prácticas de gestión definidas por el proceso DSS05 / Gestión de servicios de la seguridad alcanzando un 47% que significa que se encuentra en un nivel "Parcialmente alcanzado" y la segunda revisión posterior a la implementación de los controles alcanzando un 84% en el nivel de seguridad "En gran medida logrado" la mejora de la seguridad de información de la Universidad Peruana del Norte.[1]

García & Salas, elaboro la tesis titulada "Análisis e implementación de la seguridad de la información del centro de datos de la Universidad Nacional de la Amazonia Peruana bajo la norma ISO 27002" tuvo como propósito identificar las vulnerabilidades a las que está expuesta la información por la falta de aplicación de controles de seguridad, la problemática identificada en los últimos años ha presentado incidencias de seguridad de la información que fueron generando molestias a los usuarios y han sido causa de interrupciones de las actividades que se desarrollaron dentro del Centro de Datos de la universidad, por lo cual gracias a la información recolectada basada en el análisis de la norma ISO/IEC 27002 se pretende dar a conocer lineamientos de seguridad para prevenir y mitigar vulnerabilidades existentes. La metodología propuesta alineada a la ISO/IEC 27002. Utilizada para el proceso de la investigación son 4 fases: a) Definición, b) Aplicación, c) Monitoreo, d) Mejora. Por consiguiente, el tipo de investigación es de tipo descriptiva ya que se detalla las actividades que se desarrollaron en los procesos de manejo del objeto de estudio. En conclusión, el

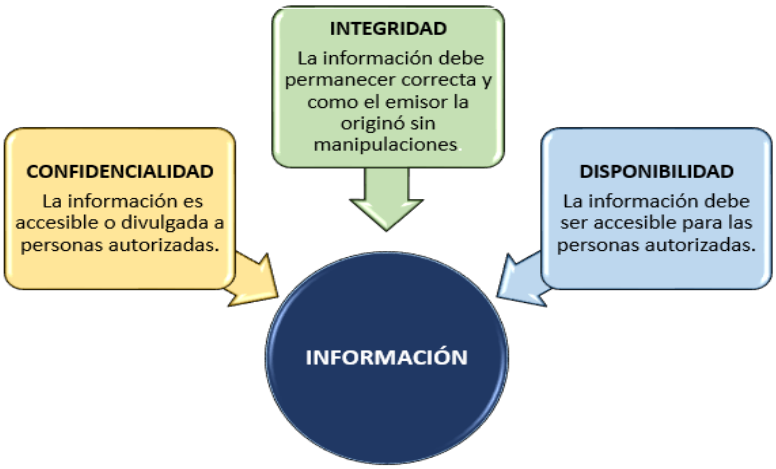
análisis realizado demostró que los activos de la información están críticos y la situación actual de la Oficina General de Informática refleja un alto índices de riesgos la cual exponen a la información a daños.[10]

2.2. MARCO TEÓRICO.

En este apartado se aborda el estado del arte de las dos variables de estudio. En primer lugar, se describe el marco en el cual se desarrollan los controles de seguridad del dominio 14 la Adquisición, desarrollo y mantenimiento de los sistemas de la ISO 27002:2015. Luego, se aborda la segunda variable, siendo la seguridad de la información en el proceso de desarrollo de un sistema. Finalmente, se describe el campo de estudio en el cual se desarrolló la presente investigación, la empresa BITNESS CORP. S.A.C.

2.2.1. SEGURIDAD DE LA INFORMACIÓN

INCIBE, refiere en el libro titulado “Gestión de Riesgos: Una guía de aproximación para el empresario” señala la importancia de la información en sus procesos productivos. La revolución ha asignado un papel importante al Internet como medio de comunicación, por ello las empresas que gestionan los riesgos de sus procesos productivos deben asignar recursos para la gestión de riesgos asociados a su información e infraestructura. En la gestión de riesgos de seguridad de la información el activo a proteger es la información de la compañía. Incluyendo información digital como aquella contenida en papel. La gestión se ocupa del ciclo de vida de la información, considerando todas sus etapas. La información es el activo principal, también: infraestructura informática, equipos auxiliares, redes de comunicaciones, instalaciones y personas. La información tiene tres principales pilares que se aprecian en la Ilustración 1:



:

Ilustración 1: Pilares de la Información
Fuente: INCIBE

Las amenazas pueden ser:

De origen natural: Inundaciones, terremotos, incendios, fallos de la infraestructura auxiliar, fallos de suministro eléctrico, refrigeración, entre otros.

Fallos de los sistemas informáticos y de comunicaciones: Fallos en las aplicaciones, hardware o equipos de transmisiones.

Error humano: Errores accidentales o deliberados de las personas que interactúan con la información como: acciones no autorizadas, uso de hardware o software no autorizado, funcionamiento incorrecto por abuso o robo de derechos de acceso, información comprometida por robos, entre otros.

Las vulnerabilidades de los sistemas de información, dependen de los activos, sean hardware, software, redes, personal, infraestructura entre otros. Por ejemplo: el equipamiento informático susceptible a variaciones de temperatura o humedad. Los sistemas operativos que, por su estructura, configuración, mantenimiento son vulnerables a ataques. Las localizaciones que son propensas a desastres naturales, las aplicaciones informáticas que por su diseño son inseguras. La mayoría de veces los factores son difíciles de erradicar y las organizaciones tienen que reducir el impacto de sus amenazas.[11]

Cámara de Comercio de Cali, realizó el manual titulado “Manual de Seguridad de la Información”, refiere que los principios de la seguridad de la información se basan en la

confidencialidad, la integridad, la disponibilidad y la auditabilidad. La confidencialidad es aquella que vela por la privacidad de la información, quiere decir que es accesible a aquellos usuarios autorizados. La integridad que garantiza que la información no ha sido alterada interna o externamente. La disponibilidad que garantiza la continuidad operativa y los respaldos necesarios para la continuidad del negocio. La auditabilidad que garantiza que todas las transacciones puedan ser auditadas por los usuarios autorizados. Además, también habla acerca de los lineamientos de la seguridad de la información, siendo estas las prácticas y reglas que manejan, protegen y distribuyen la información, son la guía general para la toma de decisiones. Son de carácter general y están diseñadas para durar en el largo plazo. Como normas de seguridad de la información se tiene a enunciados detallados de las políticas y establecen lo que se puede hacer en términos de seguridad información. Como normas establecidas se maneja el código de usuario único, quiere decir que cada usuario tiene un código de identificación para el acceso a las plataformas aplicaciones que use, no se comparte ni revela el código de usuario, además se requiere de un proceso de autenticación del usuario para acceder a cualquier recurso de tecnología informática. A su vez existen responsables que administran los códigos de usuario y son los únicos que crean, eliminan o inhabilitan los códigos. Las copias de respaldo de software se realizan de forma completa para garantizar la recuperación mediante comandos y/o procedimientos de restauración. La Cámara de Comercio de Cali dispone de un firewall que proporciona un software de IDS (Intrusion Detection System) que detecta virus y bloqueo de correos no deseados, administra los incidentes de seguridad de información. [12]

2.2.2. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Ministerio de Tecnología de la Información y Comunicación, elaboró el artículo "Controles de seguridad y privacidad de la información" refiere que la información debe ser protegida ya que forma parte de los activos de la organización, las políticas de seguridad y privacidad de la información garantizan minimizar los riesgos de daños, amenazas y un eficiente cumplimiento de objetivos. Toda institución debe tener como objetivo establecer, implementar, operar, monitorear, revisar, mantener y mejorar el sistema de gestión de seguridad de la información dentro de la institución. Un control es aquel que debe ser implementado para dar cumplimiento a la política definida. El listado de controles se utiliza para la declaración de aplicabilidad, en la cual cada control será justificado.[13]

Frayssinet, realizó la publicación “Taller de implementación de la norma ISO 27001” refiere que la seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones para resguardar y proteger la información manteniendo las dimensiones de la confidencialidad, disponibilidad e integridad. Esta abarca todo tipo de información sea impresa, escrita a mano, grabada con asistencia técnica, transmitida por correo electrónico, incluida en un sitio web, entre otros. Se establece el control en los métodos para gestionar, estos incluyen políticas, procedimientos, directrices y prácticas o estructuras organizativas. El objetivo del control es describir lo que se quiere lograr como resultado de los controles de aplicación. Existen tres tipos de controles, son los controles preventivos, controles de investigación y los controles correctivos. Los controles correctivos evitan la repetición de anomalías ya sea implementando planes de emergencia, concienciación, pruebas, procedimientos, actividades, entre otros.[14]

2.2.3. ISO 27002: 2013

Fuentes, ejecuta la tesis titulada “Auditoria al sistema de gestión de la seguridad de la información del proceso de gestión de incidentes de clientes de ANS Comunicaciones, con base en la norma técnica colombiana NTC-ISO/IEC 27002” refiere que las normas ISO son reconocidas por su contenido, que busca las mejoras que permiten a las empresas mejorar sus sistemas de información protegidos contra las amenazas que enfrentan las tecnologías de información. La norma que verifica el estado de su Sistema General de Seguridad de Información y brinda directrices de la norma ISO 27002: 2013, proporciona recomendaciones para mejorar las prácticas en gestión de la seguridad de la información.

Es un estándar global que incorpora un amplio conjunto de controles de seguridad que se adaptan a la organización. La identificación de los controles requiere de planificación y apoyo de los empleados tanto como de los accionistas, proveedores y externos. La norma ISO establece los tres requisitos de seguridad de la Ilustración 2.[15]

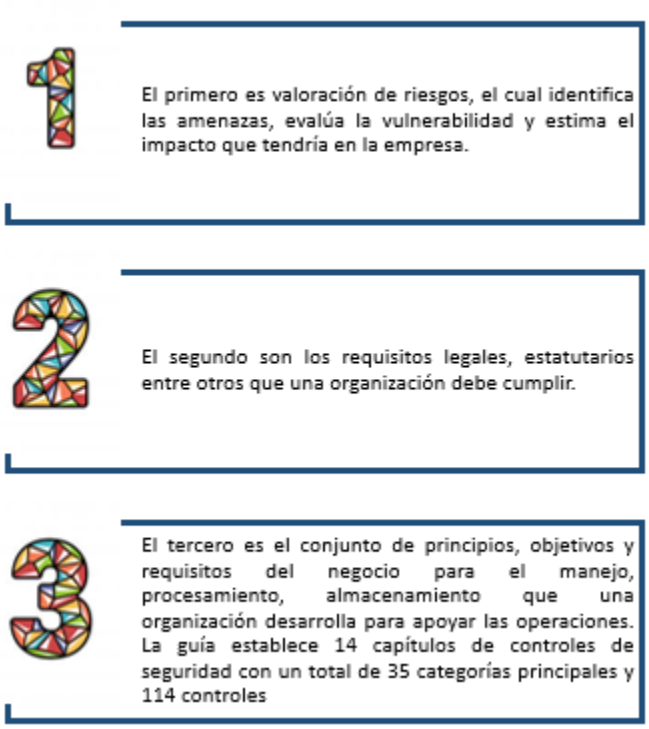


Ilustración 2: Requisitos de Seguridad de la Norma ISO 27002:2013
Fuente: Fuentes

2.2.4. SEGURIDAD EN LAS ETAPAS DEL PROCESO DE DESARROLLO DE SISTEMAS

Oficina de Seguridad para las Redes Informáticas, elaboro el proyecto "Metodología para la Gestión de la Seguridad Informática" menciona que para diseñar e implementar un sistema se debe conocer plenamente el objeto sobre el cual se diseñara. Se considera apropiado precisar los elementos que identifiquen especificaciones acerca del lugar donde se implantara el sistema. La caracterización del sistema informático incluye la protección, valoración y clasificación de los bienes informáticos. Se deben precisar datos de la información, los elementos de la entidad y otras instituciones considerando el carácter y nivel de clasificación. Se deben establecer las características del entorno donde se instalan los equipos como los puntos de acceso, la ubicación de las tecnologías de información, software instalado, nivel de clasificación de la información que se procesa, entre otros aspectos necesarios. Es de gran ayuda identificar los bienes informáticos a proteger, se puede agrupar como la refleja la Ilustración 3:

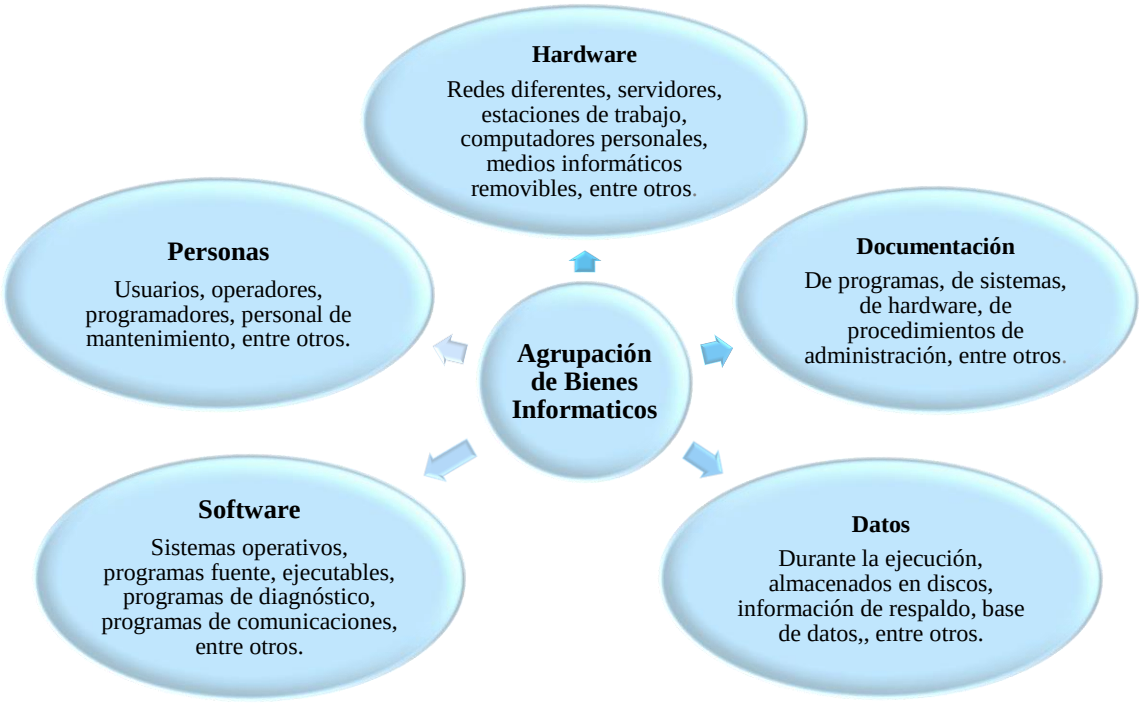


Ilustración 3: Agrupación de Bienes Informáticos
Fuente: Oficina de Seguridad para las Redes Informáticas

Al identificar los bienes informáticos que se deben proteger, se determina su importancia y clasificación dentro del sistema informático. También, es necesario identificar las amenazas de los bienes y estimar el daño (Impacto) que pueden producir. Cada bien informático debe ser protegido en base a los objetivos de seguridad tales como la confidencialidad, integridad y disponibilidad. Las amenazas comunes son la pérdida de información, corrupción o modificación de información, la sustracción, alteración o perdida de equipos o componentes, divulgación de información y/o interrupción de servicios.[16]

Barzanallana, elabora el libro “Introducción a la seguridad Informática” menciona que la seguridad es la ausencia de riesgo y se define como el estado de bienestar que percibe y disfruta el ser humano. Las empresas están abriendo sus sistemas de información a sus socios o proveedores, por ello se debe conocer los recursos de la empresa a proteger, controlar el acceso y los derechos a los usuarios de los sistemas informáticos. El “nomadismo”, que consiste en permitir al personal conectarse desde cualquier lugar, el personal transporta parte del sistema de información fuera de la infraestructura de la empresa. La seguridad informática refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento garantizando su confidencialidad, integridad y disponibilidad.

- Confidencialidad: Datos solo legibles y modificados por personas autorizadas.
- Integridad: Datos completos, sin modificar y los cambios son reproducibles (se conoce el autor y el momento del cambio).
- Disponibilidad: Acceso de datos garantizado. Evitar fallos del sistema y proveer el acceso adecuado.
- Otros aspectos:
- No repudio: Garantiza que una transacción no puede ser negada.
- Autenticación: Asegura que las personas autorizadas tengan acceso a los recursos.
- La seguridad global tiene en cuenta los siguientes aspectos:
- Sensibilizar: A los usuarios sobre los problemas de seguridad.
- Seguridad Lógica: Seguridad a nivel de datos (datos empresariales, aplicaciones o sistemas operativos).
- Seguridad de las telecomunicaciones: Tecnologías de red, servidores corporativos, redes de acceso, etc.
- Seguridad física: Seguridad a nivel de infraestructura física: salas seguras, lugares abiertos al público, zonas comunes de la empresa, puestos de trabajo, entre otros.
- La seguridad de los sistemas informáticos garantiza los derechos de acceso a los datos y recursos mediante mecanismos de autenticación y control que garanticen que los usuarios solo tienen los derechos que se les concede. La seguridad informática no debe impedir a los usuarios desarrollar los usos necesarios y la utilización del sistema de información con confianza. Se debe definir una política de seguridad que se desarrolle en las etapas:
- Identificar las necesidades de seguridad, riesgos informáticos y las posibles consecuencias.
- Desarrollar reglas y procedimientos a implementar en la organización.
- Supervisar y detectar vulnerabilidades en el sistema de información.
- Definir las acciones a tomar y el contacto si se detecta una amenaza.
- La política de seguridad son las orientaciones seguidas por la organización. Debe desarrollarse como una gestión de la organización ya que afecta a todos los usuarios del sistema.

- La seguridad informática de la empresa se basa en el conocimiento de las normas por parte de los empleados, gracias a campañas de formación y sensibilización dirigidas a los usuarios y cumple con:
- Un sistema de seguridad físico y lógico adaptado a las necesidades de la empresa y los usuarios.
- Un procedimiento de gestión de actualizaciones.
- Una estrategia de copias de seguridad correctamente planificada.
- Un plan de recuperación de incidentes.
- Un sistema documentado y actualizado.[17]

Venegas, en su artículo "Seguridad para minimizar riesgo en el desarrollo del software" refiere que, en la actualidad, debido al procesamiento de todo tipo de información, la conectividad son características que han incrementado la importancia del software, de la misma manera los riesgos a los que está expuesto la información que se maneja por cualquier software. Por eso se hace necesario tener en cuenta la seguridad en cada una de las etapas del ciclo de vida del desarrollo del software. La importancia de incluir seguridad durante todo el desarrollo del ciclo de vida del software debería ser la misma que la de garantizar la calidad en el software, el inconveniente es que las organizaciones se preocupan por la seguridad de las aplicaciones solo cuando se ha implementado. Existen diferentes modelos de ciclo de vida de desarrollo del software, cuyo principal objetivo es cumplir con el requerimiento funcional y no funcional solicitados, actualmente los requisitos de seguridad son de gran importancia debido al aumento de ataques maliciosos no solo a la infraestructura tecnológica sino también al software.

Incorporar seguridad en cada una de las etapas del proceso de desarrollo del software, garantiza las propiedades principales de la seguridad del software de la Ilustración 4: [18]

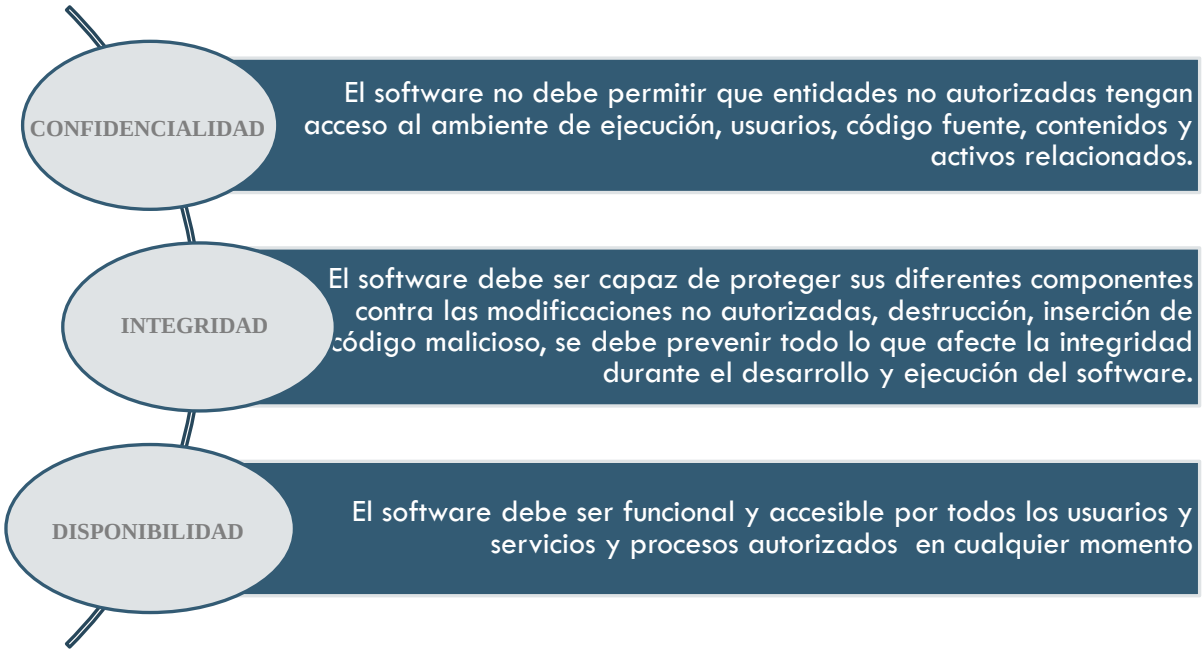


Ilustración 4: Propiedades principales de Seguridad del Software
Fuente: Venegas

Silega, en el artículo de "Requisitos de seguridad para la aplicación web", menciona que en los procesos de desarrollo de software actuales incrementa el riesgo de vulnerabilidades en un sistema de software. El aseguramiento de la información y de los sistemas que poseen dicha información es un objetivo crucial para las organizaciones. Debido a ello la gestión de la Seguridad informática es un tema que abarca desde el inicio del desarrollo del software evita que los mecanismos de seguridad se ajusten dentro de un diseño ya existente, lo que provocaría vulnerabilidades del software, incremento de costo y tiempo en solucionarlo. Un dilema común de los ingenieros de software es que durante el desarrollo de software es la falta de requisitos de seguridad que permitan el seguimiento desde etapas tempranas. La Seguridad Informática se podría resumir en cinco principios fundamental, los tres primeros también relacionados en la ISO 27002:2013:

- Integridad: garantiza que los datos no sean modificados desde su creación sin autorización y que ningún intruso pueda capturar y modificar los datos en tránsito.
- Confidencialidad: garantiza que la información, almacenada en el sistema informático o transmitido por la red, solamente va a estar disponible para aquellas personas autorizadas a accederla.

- Disponibilidad: garantiza el correcto funcionamiento de los sistemas de información y su disponibilidad en todo momento para los usuarios autorizados.
- No repudio: garantiza la participación de las partes en una comunicación. El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.
- Autenticación o Autenticidad: asegura que sólo los individuos autorizados tengan acceso a los recursos.

Ante la amenaza de ataques informáticos, las organizaciones deben demostrar que realizan una gestión competente y efectiva de la seguridad de los recursos y datos que gestionan. Este aspecto hace necesario el uso de estándares o normas que le orienten de forma estructurada, sistemática y coherente cómo proceder ante una situación de este tipo. A continuación los estándares: La ISO 17799, la familia de normas ISO 27000, 27001,27002, OWASP.[19]

2.2.5. SEGURIDAD EN EL PRODUCTO (SISTEMA)

Brito, elabora el artículo de nombre "Metodología para desarrollar software seguro" menciona que la seguridad ha dejado de ser un requerimiento no funcional, para implantarse como parte de la calidad del software o elemento primordial de cualquier aplicación. En ese sentido en la actualidad los hackers y grupos criminales evolucionan a diario y se han convertido experto en explotar las vulnerabilidades de las aplicaciones. Ante esta problemática ha sido necesaria de la implementación de diversas metodologías para el desarrollo del software, la eliminación de vulnerabilidades y la inclusión de la seguridad como elemento básico.

Cabe mencionar que las metodologías tradicionales, tienden a enfocarse básicamente en mejorar la calidad en el software, reducir el número de defectos y cumplir con las funcionalidades específicas que requiere el cliente. Pero también es necesario entregar un producto que garantice tener cierto nivel de seguridad, para ello hay metodologías que contemplan durante su proceso, un conjunto de actividades específicas para remover vulnerabilidades detectadas en el diseño o en el código, la aplicación de pruebas que aportan datos para la aplicación del estado de seguridad entre otras actividades para mejorar la seguridad del software. El presente artículo nos brindara la información de dos metodologías

que están enfocadas al desarrollo del software seguro: a) Correctness by Construction (CbyC) y Security Development Lifecycle (SDL). Las cuales representan mejor seguridad en el producto final.[20]

Ochoa, en su tesis "Seguridad del Software y Criterios de Evaluación" menciona que el software es un elemento lógico del sistema. La calidad de un software se adquiere mediante un buen diseño. Los defectos no detectados hacen que el programa falle en las primeras etapas, una vez corregido el índice de fallos disminuye y se estabiliza. La mejor característica de cualquier producto de software es la homogeneidad o estandarización de la interfaz, aspecto o forma de empleo. Esto significa para los usuarios mayor facilidad de manejo, mayor eficiencia y ahorro de tiempo. Los problemas que afectan el desarrollo del software son:

- La planificación y estimación de los costes (Imprecisas).
- La productividad de la comunidad del software no corresponde a la demanda de servicios.
- La calidad del software es inaceptable.
- El software tiene como base automatizar un proceso que se realice manualmente, añadiéndole rapidez, seguridad y exactitud, características que incrementan la calidad en los resultados, humanizan el trabajo y aumentan la cultura informática.[21]

Hernández, en su tesis "Seguridad y Privacidad en los Sistemas Informáticos" menciona que la informatización de la sociedad ha proporcionado mejoras y a la vez nuevos problemas. Muchas entidades contienen en sus ficheros de datos información personal cuya difusión puede perjudicar gravemente a la personar involucrada. La seguridad de la información depositada en un sistema no se pierda o sea alterada es un aspecto importante al igual que a esta información solo se acceda cuando sea necesario o con las autorizaciones pertinentes. La información dentro de los sistemas informáticos es vital y por lo tanto debe ser protegida. El número de incidentes que afectan a la seguridad de un sistema informático ha crecido exponencialmente y su coste es cada vez mayor. Un sistema es seguro si se puede confiar en él y se comporta de acuerdo a lo esperado. La seguridad es un conjunto de soluciones técnicas, métodos, planes, entre otros con el objetivo de que la información sea protegida. La seguridad comprende aspectos como:

- Confidencialidad: Solo el usuario autorizado puede acceder a la información.
- Integridad: La información no puede ser eliminada o modificada sin permiso.
- Disponibilidad: La información tiene que estar disponible cuando sea necesario.
- Consistencia: Las operaciones que se realizan sobre la información se comportan de acuerdo a lo esperado.
- Control: Regular y controlar el acceso a la información de la empresa.[22]

Asociación Española de Normalización, en su revista "Calidad del Producto de Software" menciona que las empresas dedicadas al desarrollo de software ha experimentado una fuerte demanda de productos en el sector. Para esta tipo de empresas la calidad del software es fundamental como diferenciador de conpetitividad y de imagen frente a sus clientes. Según la información de The CHAOS Manifesto del Standish Group en 2013 que solo el 39% de proyectos de desarrollo finalizaron en el tiempo establecido, recursos planificados y con una calidad aceptable. En este contexto la calidad del software estan cobrando cada vez mas importancia. El modelo de calidad del producto de software según la IDO/IEC 25010 son: Funcionalidad, Rendimiento, Usabilidad, Fiabilidad, Seguridad, Mantenibilidad, Portabilidad y Compatibilidad. Estas caracteristicas y subcaracteristicas de calidad sirven para la evaluación del producto de software. Los motivos para que una organización pueda interezarse en evaluar su producto según la ISO/IEC 25000 se incluyen:

- Asegurar que el producto software desarrollado respeta los niveles necesarios para las características de seguridad (confidencialidad, integridad, autenticidad, no-repudio, etc.).

Evaluar y controlar el rendimiento del producto software desarrollado, asegurando que podrá generar los resultados teniendo en cuenta las restricciones de tiempo y recursos establecidas.

Detectar los defectos en el producto software y proceder a su eliminación antes de la entrega, lo que supone un ahorro de costes en la fase de mantenimiento posterior.[23]

2.2.6. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se describe los controles de seguridad de la ISO 27002: 2015 que se consideran en la investigación:

La ISO 27002: 2015 está compuesta por 14 dominio, 35 objetivos de control y 114 controles, el dominio que alberga los controles de seguridad elegidos es el dominio 14 cuyo nombre es Adquisición, desarrollo y mantenimiento de los sistemas de información, de este dominio se identificaron 3 objetivos de control y 7 controles acorde a la situación de la empresa BITNESS CORP. S.A.C., los cuales se mencionan en las siguientes líneas:

14.1. Requisitos de seguridad de sistemas de información

Garantizar que la seguridad de la información sea integral en el ciclo de vida de los sistemas de información y las redes públicas.

14.1.1 Análisis de requisitos y especificaciones de seguridad de la información

Los requisitos de la seguridad de la información deben incluirse en los nuevos sistemas de información o en las mejoras a los sistemas existentes. Se identifican los requisitos de seguridad de la información mediante diversos métodos. Los resultados de la identificación deben ser documentados y revisados por los interesados. Los requisitos y controles deben reflejar la información de la empresa. Identificar y gestionar los requisitos de seguridad de la información y los procesos asociados debe realizarse en las primeras etapas. La seguridad de la información considera la identificación de los usuarios, la aprobación y autorización de acceso, información de usuarios, necesidades de protección para los activos también el registro y monitorización de transacciones, impuestos.

14.2 Seguridad en el desarrollo y en los procesos de soporte

Garantizar la seguridad de información diseñada e implementada en el ciclo de vida de desarrollo de sistemas de información.

14.2.1 Política de desarrollo seguro

Establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas. Como requisito se tiene el desarrollo seguro para los servicios, arquitectura, software entre otros. Considera la seguridad del entorno de desarrollo, seguridad en el ciclo de vida del software, seguridad en la metodología de desarrollo, guías de desarrollo, puntos de verificación de seguridad, repositorios seguros, control de versiones, seguridad de aplicaciones, gestión de vulnerabilidades.

14.2.2 Procedimiento de control de cambios en sistemas

Control de cambios formales en el ciclo de vida. Los procedimientos formales se deben documentar y hacer cumplir para asegurar la integridad del sistema, aplicaciones y productos. Un proceso formal consta de documentación, especificaciones, pruebas, control de calidad y gestión de implantación, evaluación de riesgo, análisis de impactos de cambios y especificación de controles de seguridad necesarios. Los procesos de control de cambios deben incluir un registro de los niveles de autorización, control de cambios, revisión de los procedimientos de seguridad, identificar el software (información, entidades de base de datos, hardware), aprobación formal de propuestas, gestión de cambios, documentación, gestión de versiones, registro de solicitudes entre otros.

14.2.6 Entorno de desarrollo seguro

Las organizaciones deben establecer y proteger el entorno adecuadamente en lo cual se incluye las personas, los procesos y la tecnología de desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.

14.2.8 Pruebas funcionales de seguridad de sistemas

Se deben realizar pruebas de seguridad funcional exhaustivas durante el desarrollo de los sistemas ya sea nuevos o los actualizados, incluyendo la preparación de un programa detallado de actividades y datos de prueba junto a los resultados esperados. Las pruebas inicialmente deberían ser realizadas por el equipo de desarrollo.

14.2.9 Pruebas de aceptación de sistemas

Se deben establecer programas de pruebas de aceptación y criterios para los nuevos sistemas de información, actualizaciones y nuevas versiones. En la cual deberían incluir las pruebas de requisitos de seguridad de la información y de que se han aplicado las prácticas de desarrollo seguro del sistema. Las organizaciones deberían utilizar herramientas automatizadas, como herramientas de análisis de códigos o escáneres de vulnerabilidades y verificar la solución de los efectos relacionados con la seguridad.

14.3. Datos de Prueba

Asegurar la protección de datos de prueba.

14.3.1 Protección de los datos de prueba

Los datos de prueba se deben seleccionar con cuidado y ser protegidos y controlados evitando el uso de datos reales que contengan datos de personas o cualquier otra información confidencial para las pruebas, si en caso se utiliza los datos confidenciales deberían protegerse mediante su retirada o su modificación.

Los controles identificados respecto a la mejora de la seguridad de la información en base a la norma ISO 27002: 2015, han sido aplicados mediante un instrumento en la empresa BITNESS CORP. S.A.C. se muestran en la Tabla 1:

Tabla 1:
Elección de controles de seguridad en base a la norma ISO 27002: 2015

Dominio		Objetivos de Control		Controles	
14	Adquisición, desarrollo y mantenimiento de los sistemas de información	14.1	Requisitos de Seguridad en Sistemas de Información	14.1.1	Análisis de requisitos y especificaciones de seguridad de información
		14.2	Seguridad en el desarrollo y en los procesos de soporte	14.2.1	Política de desarrollo seguro
				14.2.2	Procedimientos de control de cambios en sistemas
				14.2.6	Entorno de desarrollo seguro
				14.2.8	Pruebas funcionales de seguridad de sistemas
				14.2.9	Pruebas de aceptación de sistemas
		14.3	Datos de Prueba	14.3.1	Protección de los datos de prueba

Elaboración propia (2020)

2.3. MARCO CONCEPTUAL

2.3.1. SEGURIDAD

La definición de seguridad en los estados considera una relación causal entre el orden y la seguridad pública, y como fin de ésta la preservación de la integridad, derechos y libertades de las personas, pero hacen totalmente responsables a las dependencias policiales. En ese sentido, la introducción del concepto de seguridad interior en la normatividad estatal permitirá incorporar en la agenda a la alimentaria, a los recursos naturales y a la salud, entre otros, así como constituir estrategias de gobierno integrales para enfrentar problemas complejos como el crimen organizado o los desastres naturales que, si bien son responsabilidad de las instancias encargadas de la seguridad pública y de protección civil, requieren de la participación de varias dependencias gubernamentales.[24]

2.3.2. INFORMACIÓN

La información es un conjunto de datos acerca de algún suceso, hecho o fenómeno, que organizados en un contexto determinado tienen su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo".[25]

2.3.3. SOFTWARE

Se conoce como el equipamiento lógico de un sistema informático, que comprende todo el conjunto de componentes lógicos que hacen posible la realización de tareas específicas, asociados con la operación de un sistema de cómputo, la cual se clasifica en tres de software de sistema, software de aplicación y software de programación.[26]

2.3.4. VULNERABILIDAD

Hace referencia a la posibilidad de daño, finitud y condición mortal. La vulnerabilidad se ha asociado con las condiciones del medio (ambientales, sociales o de otro tipo) en que su vida se desarrolla, dando lugar a la necesidad de incorporar los aspectos socioculturales en la comprensión de este concepto. Por ello al decir poblaciones vulnerables, hace referencia a aquellos grupos de personas que, a consecuencia de las condiciones del medio en que viven, están en una situación de mayor susceptibilidad al daño.[27]

2.3.5. RIESGO

Es la posibilidad que se produzca un impacto determinado a un activo. Identificar amenazas, vulnerabilidades y riesgos sobre la plataforma tecnológica de una organización para implementar controles que aseguren un ambiente informático seguro.[28]

2.3.6. ISO 27002

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables y comúnmente aceptados en la seguridad de la información y que estas mismas son las que utiliza la ISO/IEC 27001 donde describe cómo implementar un Sistema de Gestión de Seguridad de la información que sirve para gestionar los controles y riesgos de la seguridad de la información dentro de una organización.[29]

2.3.7. POLÍTICAS DE SEGURIDAD

Controles para proporcionar directivas y consejos de gestión para mejorar la seguridad de los activos de información, para lo cual se debe disponer de los recursos necesarios para

garantizar el correcto desarrollo de los lineamientos planteados en cada política propuesta.[30]

2.3.8. SERVICIOS

Refiere un conjunto de actividades económicas heterogéneas. Las actividades de los servicios que pertenecen al sector terciario son las actividades que no producen bienes, entre ellas se encuentra la distribución, el transporte las comunicaciones, las instituciones financieras y los servicios a las empresas sociales y personales.[31]

2.3.9. AMENAZAS

Son eventos accidentales o intencionados que ocasionan diferentes daños en las cuales, al sistema informático, pérdidas de materiales o financiera entre otros. Existen diferentes tipos de amenazas: naturales (inundaciones, incendio, tormenta, fallo eléctrico, entre otros.), agentes externos (virus informáticos, ataques de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas.) y agentes internos (empleados descuidados con una formación inadecuada o descontentos, errores en la utilización de las herramientas y recursos del sistema.).[32]

2.3.10. ETAPAS DEL PROCESO DE DESARROLLO DE SOFTWARE

Todo sistema de información pasa por una serie de fases a lo largo de su vida. El ciclo de vida de un sistema de información comprende: Planificación, Análisis, Diseño, Implementación, Pruebas, Instalación o despliegue y Uso y mantenimiento. Estas etapas son un reflejo del proceso de resolución de cualquier tipo de problema. George Polya describió este proceso como: Comprender el problema (análisis), Plantear una posible solución, considerando soluciones alternativas(diseño), Llevar a cabo la solución planteada (Implementación) y Comprobar que el resultado obtenido es correcto (Pruebas). Las etapas adicionales son necesarias en el mundo real porque el desarrollo de un sistema conlleva costes.[33]

2.3.11. SISTEMA INFORMÁTICO

Un sistema se puede dividir en subsistemas. Toda empresa es un sistema, la teoría de la organización divide a la empresa en sistema: comercial, operaciones, financiero, personal y de información. El sistema de información se relaciona con el resto de sistemas y el entorno. Un sistema de información sirve para captar la información que se necesite y ponerla (con

las transformaciones necesarias) en aquellos miembros que la necesiten para la toma de decisiones. Es un conjunto de procesos que operando con un conjunto de datos estructurados recopila, elabora y distribuye la información necesaria para la operación y actividades de control correspondientes. Este hace posible el tratamiento automático de la información. Sus componentes son: Componente Físico (aparatos electrónicos y mecánicos que realizan cálculos y manejan información), Componente Lógico (aplicaciones y datos con los que trabajan los componentes físicos del sistema) y Componente Humano (usuarios que trabajan con los equipos sea elaborando apps).[34]

2.3.12. PROCESO

Es la secuencia de actividades que apuntan a un objetivo. La actividad es el conjunto de tareas necesarias para obtener un resultado. Se considera que un sistema es un conjunto de procesos cuya finalidad es la consecución de un objetivo. Existen diferentes niveles de proceso dependiendo del tamaño de la organización. Para definir un proceso se debe conocer el alcance y los límites del mismo. A su vez, se deben conocer los elementos del proceso tales como el dato de entrada o Input (Producto), la secuencia de actividades y la salida del proceso u Output (Destinado al usuario y/o cliente).[35]

2.3.13. PROCESO MISIONAL

Son procesos que se encargan de incorporar los requisitos y necesidades del cliente o destinatario de los bienes y servicios, y son encargados de lograr la satisfacción del mismo, estos procesos tienen que agregar valor y responden a las funciones sustantiva de la entidad.[36]

CAPÍTULO III:

MATERIALES Y MÉTODOS

3.1. METODOLOGÍA DE INVESTIGACIÓN.

3.1.1. NIVEL DE INVESTIGACIÓN.

Investigación Descriptiva y Explicativa

Hernández, da a conocer sobre los diferentes alcances de la investigación uno de ellos es la investigación descriptiva que se basa en especificar las propiedades, las características y los perfiles de personas o cualquier otro fenómeno que se someta a un análisis. Asimismo, también está el tipo de investigación correlacional que tiene como finalidad conocer la relación o grado de asociación que exista entre dos o más conceptos o variable en un contexto específico.[37]

La investigación de tipo descriptiva y explicativa, porque utilizando el instrumento de evaluación elaborado en base a la Norma ISO 27002: 2015 se pudo identificar y describir la situación de la seguridad del producto y la seguridad de las etapas del proceso de desarrollo de sistemas en la empresa BITNESS CORP. S.A.C. y en base a ello se establecieron mejoras.

3.1.2. TIPO DE INVESTIGACIÓN.

Investigación no experimental de tipo longitudinal

Hernández, menciona que el estudio no experimental se realiza sin la manipulación deliberada de variables y en los que sólo se observan los fenómenos en su ambiente natural para analizarlos, dicho esto en este libro se considera de la siguiente manera la clasificación del diseño no experimental en dos tipos: Transaccional y Longitudinal. Las cuales se diferencian por su dimensión temporal o el número de momentos o puntos en el tiempo en los cuales se recolectan datos.[37]

La investigación es no experimental ya que a través de la aplicación del instrumento de evaluación se obtuvo datos reales y no intencionados que se observan en el primer momento de la evaluación. Es importante mencionar que el tipo es longitudinal ya que se trabajó en dos tiempos uno que se dio como la situación actual de su nivel de seguridad de la información física y lógica basado en la Norma ISO 27002: 2015 y posterior a la implementación de los controles se conoció en cuanto ha mejorado.

3.1.3. ENFOQUE DE LA INVESTIGACIÓN.

El proceso de investigación posee medidas numéricas. La recolección de datos se basa en el proceso de observación, estos datos deben analizarse para responder las inquietudes de la investigación, ya que derivan en hipótesis que prueban la veracidad de la investigación. Se utilizan análisis estadísticos. Plantea un problema delimitado y concreto. La investigación cuantitativa sigue patrones predecibles y estructurados antes de iniciar la recolección de datos. La finalidad del enfoque cuantitativo es explicar y predecir fenómenos a partir del proceso, el resultado será un nuevo conocimiento.[38]

La presente investigación es cuantitativa ya que se clasifican datos y descripciones de la realidad social de la empresa BITNESS CORP. S.A.C. El producto de nuestra investigación cuantitativa es un informe en el que se muestra una serie de datos clasificados. Se han recogido, procesado y analizado datos cuantitativos o numéricos sobre variables determinadas, los datos mostrados en el informe final coinciden con las variables declaradas al principio.

3.1.4. DOMINIO DE INVESTIGACIÓN

La presente investigación está orientada a la línea de investigación **413. Gestión de Tecnología de Investigación** ya que se cumple con el objetivo específico de: Desarrollar investigaciones básicas, aplicadas y de innovación sobre tecnologías de información.

3.1.5. ETAPAS Y ACTIVIDADES DE LA INVESTIGACIÓN

La metodología de estudio está conformada por 4 fases en la cual se menciona determinadas actividades que deben cumplirse para conseguir un entregable por cada fase. En la Ilustración 5 se muestra la metodología de estudio que se estará realizando en todo el proceso de la investigación.

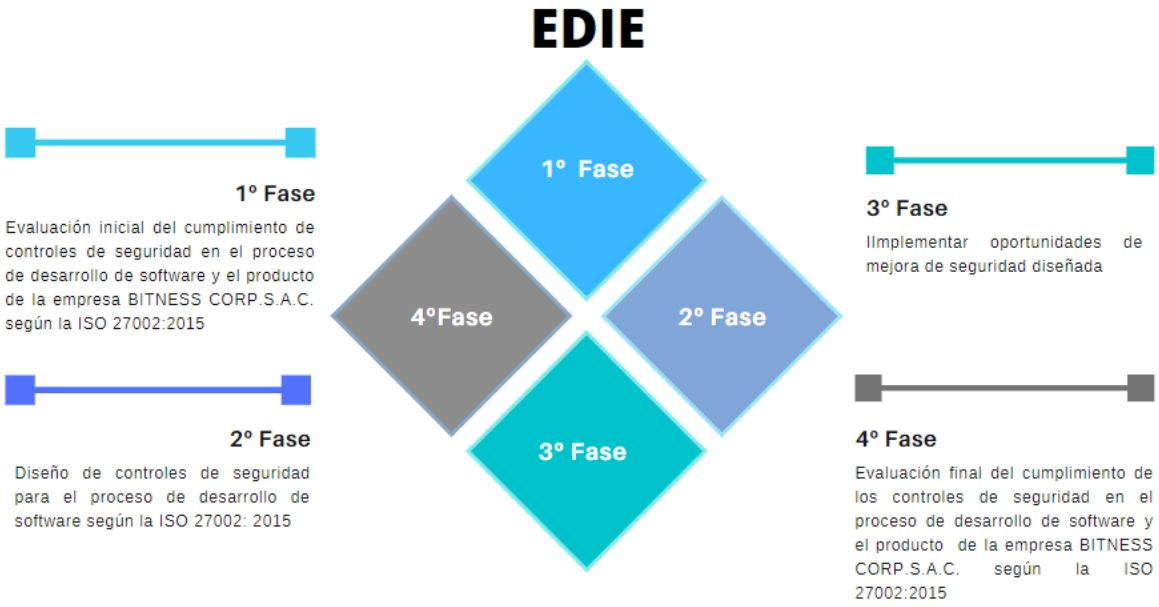


Ilustración 5: Fases de la investigación
Fuente: Elaboración propia (2020)

FASE 1: EVALUACIÓN INICIAL DEL CUMPLIMIENTO DE CONTROLES DE SEGURIDAD EN EL PROCESO DE DESARROLLO DE SOFTWARE Y EL PRODUCTO DE LA EMPRESA BITNEES CORP. S.A.C. SEGÚN LA ISO 27002: 2015.

Actividad 1.1. Elaborar el instrumento de evaluación

Esta actividad consiste en elaborar el instrumento de evaluación orientado a la seguridad de la información durante el desarrollo de sistemas y el producto, tal como se describe en el dominio 14. Adquisición, desarrollo y mantenimiento de los sistemas de información de la norma ISO 27002: 2015.

Actividad 1.2. Validar el instrumento de evaluación

Esta actividad consiste en la validación del instrumento por juicio de expertos. Se considera la participación mínima de 02 profesionales expertos, estos deben ser profesionales del área de tecnología que tengan conocimientos en el área de seguridad de la información. Se utilizan formatos de validación para la ejecución de esta actividad.

Actividad 1.3. Realizar evaluación inicial del proceso de desarrollo de software

Esta actividad consiste en aplicar el instrumento de evaluación validado, para obtener la data que permite hacer el cálculo del nivel de cumplimento de seguridad de la información en el proceso de desarrollo de sistemas y el producto.

Actividad 1.4. Identificar oportunidades de mejora

Con los resultados obtenidos de la actividad anterior, se plantean oportunidades de mejora. Las oportunidades de mejora deben suplir el nivel de seguridad de la información de la empresa BITNESS CORP. S.A.C.

FASE 2: DISEÑO DE CONTROLES DE SEGURIDAD PARA EL PROCESO DE DESARROLLO DE SOFTWARE SEGÚN LA ISO 27002: 2015

Actividad 2.1. Priorizar las oportunidades de mejora

En esta actividad se priorizan las oportunidades de mejora identificadas en la actividad anterior en base a criterios de evaluación. Se debe considerar una valuación del puntaje. El resultado de la evaluación considera factible las oportunidades de mejora que obtienen una puntuación sobresaliente.

Actividad 2.2 Diseñar propuestas de controles de seguridad identificados y priorizados

En esta actividad se procede a diseñar oportunidades de mejora priorizadas. Para ello se debe realizar investigaciones aplicando el conocimiento con el objetivo de mejorar el nivel de la seguridad de la información durante el proceso de desarrollo y el producto.

Actividad 2.3 Aprobar propuestas diseñadas de oportunidades de mejora

Esta actividad consiste en la presentación formal de las oportunidades de mejora a la empresa BITNESS CORP. S.A.C. Se realiza la firma del acta de aceptación y la entrega de la documentación correspondiente.

FASE 3: IMPLEMENTAR OPORTUNIDADES DE MEJORA DE SEGURIDAD DISEÑADA

Actividad 3.1. Programar la implementación de las oportunidades de mejora diseñados

Se establecen fechas para la implementación de las oportunidades de mejora diseñadas, conforme a la disponibilidad de la empresa BITNESS CORP. S.A.C.

Actividad 3.2. Implementar oportunidades de mejora de seguridad diseñadas

En esta actividad se realiza la ejecución de las oportunidades de mejora, de acuerdo a la situación actual de la empresa BITNESS CORP. S.A.C.

FASE 4: EVALUACIÓN FINAL DEL CUMPLIMIENTO DE LOS CONTROLES DE SEGURIDAD EN EL PROCESO DE DESARROLLO DE SOFTWARE Y EL PRODUCTO DE LA EMPRESA BITNESS CORP.S.A.C., SEGÚN LA ISO 27002:2015

Actividad 4.1 Realizar evaluación final

Esta actividad consiste en aplicar el instrumento de evaluación tras la ejecución de las oportunidades de mejora.

Actividad 4.2 Calcular resultados de la mejora

Esta actividad consiste en obtener la data que permite hacer el cálculo del nivel de cumplimento de seguridad de la información en el proceso de desarrollo de sistemas y el producto.

3.2. HIPÓTESIS.

3.2.1. HIPÓTESIS GENERAL.

La seguridad de la información en el proceso de desarrollo de sistemas y del producto en la empresa BITNESS CORP. S.A.C., mejora significativamente con la implementación de controles de seguridad basado en la norma ISO 27002:2015, 2020.

3.2.2. HIPÓTESIS ESPECÍFICAS.

- La seguridad de la información en el proceso de desarrollo de sistemas en la empresa BITNESS CORP. S.A.C., mejora significativamente con la implementación de controles de seguridad basado en la norma ISO 27002:2015, 2020.
- La seguridad de la información del producto en la empresa BITNESS CORP. S.A.C., mejora significativamente con la implementación de controles de seguridad basado en la norma ISO 27002:2015, 2020.

3.3. OPERACIONALIZACIÓN DE VARIABLES:

Tabla 2:
Operacionalización de variables

Variables	Dimensiones	Indicadores
Variable Independiente: Controles de Seguridad del dominio 14 de la ISO 27002: 2015	Requisitos de Seguridad en Sistemas de Información	
	Seguridad en el desarrollo y en los procesos de soporte	
	Seguridad en los datos de prueba	
Variable Dependiente: Seguridad de la Información en el proceso de desarrollo de sistemas	Producto (Sistema)	N° de controles de la seguridad de la información orientados a la protección de los requisitos de seguridad del producto.
		N° de controles de la seguridad de la información orientados a la protección de los requisitos de seguridad en el proceso de desarrollo.
	Etapas del proceso de desarrollo de sistemas	N° de controles de la seguridad de la información orientados a la protección de la información generada por el control de cambios en el proceso de desarrollo.
		N° de controles de seguridad orientados a la protección de la confidenciliadad de la información por medio de contratos de confidencialidad.

Elaboración propia (2020)

3.3.1. VARIABLES DEPENDIENTE E INDEPENDIENTE.

Variable Dependiente

Seguridad de la Información en el proceso de desarrollo de sistemas.

Variable Independiente

Controles de la Seguridad del dominio 14 de la ISO 27002: 2015.

3.3.2. DEFINICIÓN DE LA(S) VARIABLE(S).

Seguridad de la Información en el proceso de desarrollo de sistemas: Se encarga de garantizar la confidencialidad, integridad y disponibilidad de la información (Software

personas, hardware, entre otros) desde la concepción de un sistema hasta su culminación. Nos habla de los riesgos, amenazas, análisis, buenas prácticas y normas que deben poseer los procesos y tecnología para elevar el nivel de confianza de la información.

Controles de la Seguridad del dominio 14 de la ISO 27002: 2015: Consiste en mantener la seguridad de la información de forma integral de los sistemas de información durante todo el proceso de desarrollo y del producto. Cabe mencionar que la norma ISO 27002: 2015 consta de una estructura: Dominio de control, objetivos de control y controles.

3.3.3. OBTENCIÓN DE LA INFORMACIÓN

Para desarrollar el análisis de seguridad de la información se utilizará los siguientes mecanismos de recolección de información:

- Instrumento de evaluación
- Entrevistas virtuales

3.3.4. TRATAMIENTO DE LA INFORMACIÓN.

La presente investigación se realiza mediante el nivel de cumplimiento de los controles de seguridad que se aplica durante las etapas del desarrollo del software, una vez obtenida la información se registra, y posteriormente se analiza el nivel de cumplimiento en la etapa inicial, asimismo ya identificado e implementado los controles de seguridad se vuelve a aplicar el instrumento para comparar y evidenciar la mejora del nivel de seguridad de la información en la empresa BITNESS CORP. S.A.C. Cabe mencionar que con los datos o la información que se trabaja de la empresa están debidamente protegidos utilizando dispositivos de almacenamiento seguros.

3.3.5 PRESENTACIÓN DE LA INFORMACIÓN.

Los resultados de la investigación se visualizan mediante los gráficos estadísticos mostrando ahí el nivel de seguridad de la información inicial y el nivel de la seguridad de la información final es cuando se han implementado ciertos controles.

CAPÍTULO IV:

CARACTERIZACIÓN DEL LUGAR OBJETO DE ESTUDIO

4.1. RESEÑA HISTÓRICA: BITNESS CORP. S.A.C.

Nace el 18 de febrero del 2018, formada por la unión de dos egresados de la Universidad Peruana Unión siendo el Ing. de Sistemas Andrés Rosas y el Ing. Civil Samuel. Fue una meta trazada en las aulas de estudio. Ambos ingenieros querían tener una empresa y no descansaron hasta lograrlo. El nombre nació de la unión de dos palabras By y Business. A lo largo de estos años hubo mucho trabajo y la entrega de los ingenieros fue total, Andrés encargado de operaciones y Samuel encargado del área de ventas. Andrés refiere “Siempre hemos tenido trabajo y tendremos porque un sistema es necesario en todas las empresas”, destacando la importancia de los ingenieros de sistemas actualmente.

4.2. MISIÓN

Comprometidos con el éxito y crecimiento de nuestros clientes brindando soluciones tecnológicas en entornos digitales, con el asesoramiento de primer nivel enfocado en el rubro de cada sector empresarial.

4.3. VISIÓN

Ser reconocidos como una empresa líder e innovadora, brindando un servicio y asesoramiento continuo en el mundo digital.

4.4. ORGANIGRAMA DE BITNESS CORP. S.A.C.

En la Ilustración 6 se aprecia el organigrama funcional de la empresa BITNESS CORP. S.A.C., el cual nos proporcionó el Gerente de Operaciones.

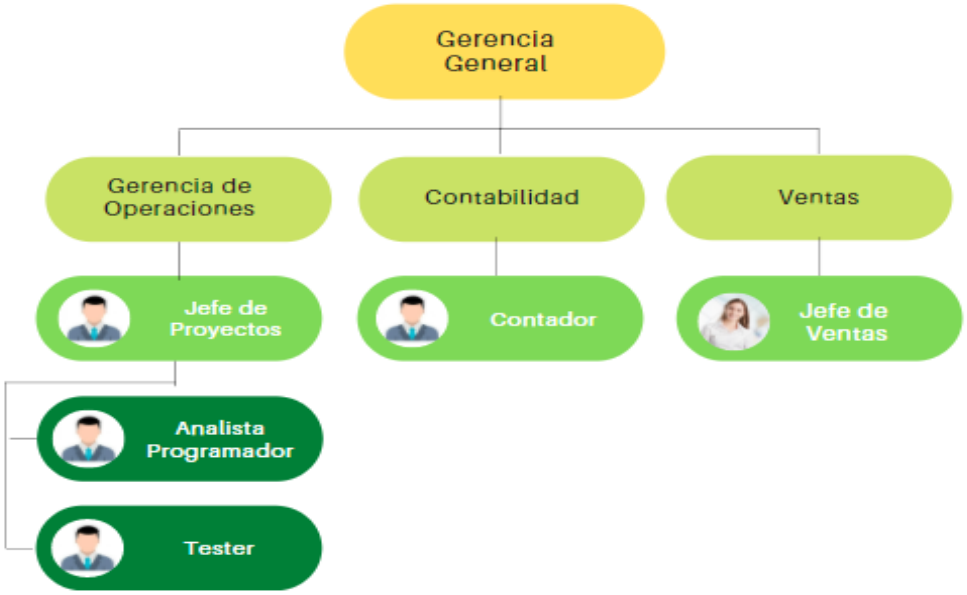


Ilustración 6: Organigrama de BITNESS CORP. S.A.C.
Fuente: Elaboración propia (2020)

4.5. VALORES

En la Ilustración 7 se muestra los valores que ejercen en la empresa BITNESS CORP. S.A.C.

Ilustración 7: Valores de BITNESS CORP. S.A.C.
Fuente: Elaboración propia (2020)

4.6. PROYECTOS

La empresa BITNESS CORP. S.A.C. viene realizando proyectos desde su fundación (Año 2018), por lo cual cuenta con un banco de proyectos. En el primer año de creación la

empresa desarrolló entre 6 a 8 proyectos de software. En el año 2019 la empresa realizó entre 8 a 12 proyectos de software. En el presente año, se encuentra realizando proyectos de software hasta el momento cuenta con una cantidad estimada menor a 20 proyectos de software. En la Ilustración 8 se aprecia el crecimiento de la empresa desde sus inicios hasta el presente año.

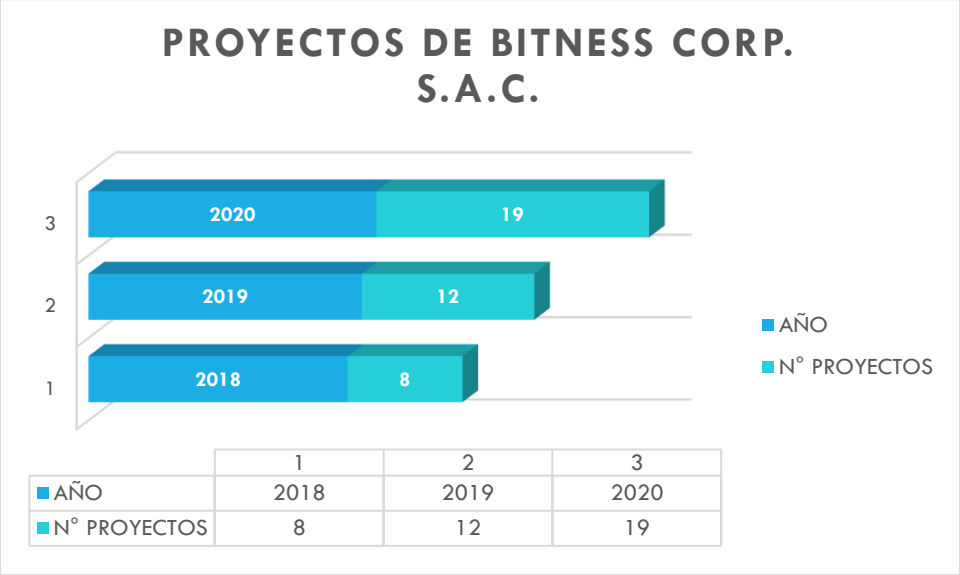


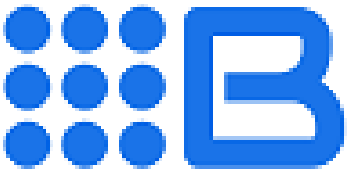
Ilustración 8:Crecimiento anual de proyectos en BITNESS CORP. S.A.C.
Fuente: Elaboración propia (2020)

BITNESS CORP. S.A.C. cuenta con tres proyectos representativos:

Ilustración 9: Proyectos de BITNESS CORP. S.A.C.
Fuente: Elaboración propia (2020)

4.7. LOGO

La empresa BITNESS CORP. S.A.C. realiza la descripción de su logo de la siguiente manera:



La letra “B”: Refiere al nombre de la empresa.
El color azul: Simboliza a la tecnología.
Los círculos: Representa a la conexión global de tecnologías, también está representado así por el icono de aplicaciones.

4.8. PLATAFORMAS DE COMUNICACIÓN

La empresa BITNESS CORP. S.A.C. está presente en distintas redes sociales. Sin embargo, para establecer un contacto ya sea para el desarrollo de un software entre otros, utiliza con mayor frecuencia el correo corporativo.

bitnesscorp.com
contacto@bitnesscorp.com
andresrosas@bitnesscorp.com
https://www.instagram.com/bitnesscorp/
https://www.youtube.com/channel/UCA6tCWWOJf9EC6pwW6ZmfiQ

CAPÍTULO V:

INGENIERÍA DE LA PROPUESTA

La metodología está alineada a la norma ISO/IEC 27002:2015 y corresponde al análisis del nivel de seguridad de la información para el producto y durante el desarrollo del producto. Inició con la solicitud del permiso a BITNESS CORP. S.A.C. para realizar la investigación. Al recibir la autorización, por parte de la empresa, accedimos a la información necesaria para la investigación. Se realizó una primera reunión para el estudio del negocio en la cual se tomó conocimiento de la creación, organigrama y el proceso de trabajo de la empresa. Luego de ello se identificó la problemática la cual es esencial para la investigación realizada. Asimismo, detallaremos las cinco fases son sus respectivas actividades.

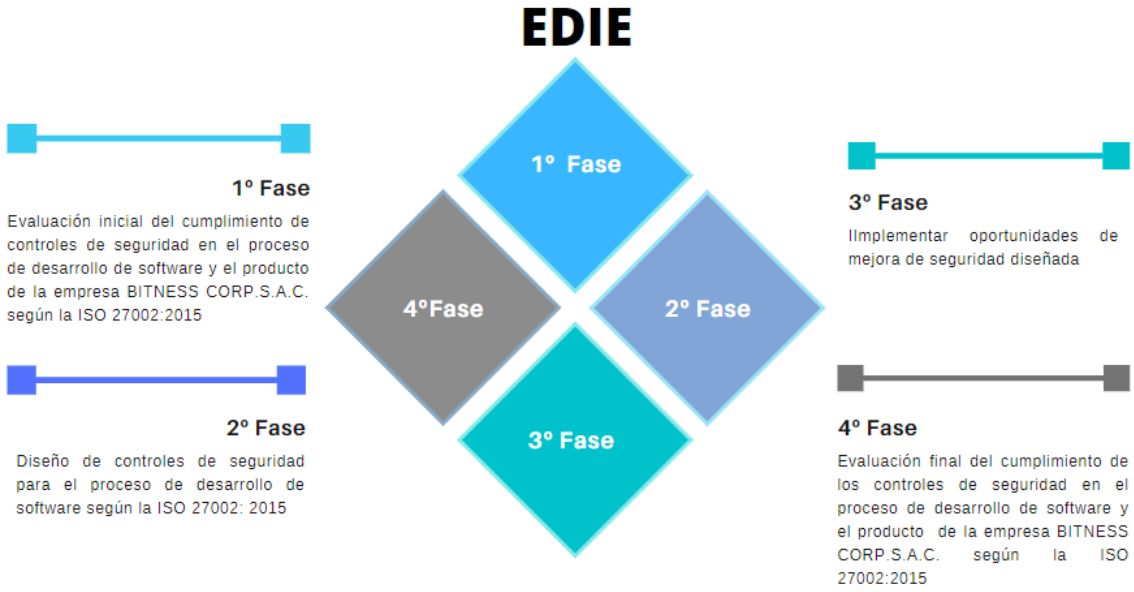


Ilustración 10: Fases de la Investigación
Fuente: Elaboración propia (2020)

5.1. FASES - DESARROLLO DE LA INVESTIGACIÓN

FASE 1: EVALUACIÓN INICIAL DEL CUMPLIMIENTO DE CONTROLES DE SEGURIDAD EN EL PROCESO DE DESARROLLO DE SOFTWARE Y EL PRODUCTO DE LA EMPRESA BITNEES CORP. S.A.C. SEGÚN LA ISO 27002: 2015.

Actividad 1.1. Elaborar el instrumento de evaluación

El instrumento de evaluación se desarrolló en base a los controles de seguridad de la ISO 27002: 2015, en el dominio 14 Adquisición, desarrollo y mantenimiento de los sistemas

con los objetivos de control 14.1 Requisitos de seguridad en sistemas de información, 14.2 Seguridad en el desarrollo y procesos de soporte y 14.3 Datos de prueba, como se muestra en la tabla 3.

Tabla 3:
Controles de Seguridad de la ISO 27002: 2015 para la construcción del instrumento de evaluación

Dominio		Objetivos de Control		Controles	
14	Adquisición, desarrollo y mantenimiento de los sistemas de información	14.1	Requisitos de Seguridad en Sistemas de Información	14.1.1	Análisis de requisitos y especificaciones de seguridad de información
		14.2	Seguridad en el desarrollo y en los procesos de soporte	14.2.1	Política de desarrollo seguro
				14.2.2	Procedimientos de control de cambios en sistemas
				14.2.6	Entorno de desarrollo seguro
				14.2.8	Pruebas funcionales de seguridad de sistemas
				14.2.9	Pruebas de aceptación de sistemas
		14.3	Datos de Prueba	14.3.1	Protección de los datos de prueba

Elaboración propia (2020)

El instrumento se describe en el (Anexo 1). A cada control se le otorgó un peso de acuerdo a su complejidad de implementación y al conocimiento de las tesistas sobre el tema de seguridad de la información.

Los controles 14.1.1 Análisis de requisitos y especificaciones de seguridad de información, 14.2.1 Política de desarrollo seguro, 14.2.2 Procedimientos de control de cambios en sistemas y 14.2.6 Entorno de desarrollo seguro, se les otorgó un peso alto debido a que se ejecutan desde la etapa temprana hasta la culminación, incluyendo proceso, tecnología y persona durante el proceso de desarrollo de sistemas y el producto.

Los controles 14.2.8 Pruebas funcionales de seguridad de sistemas, 14.2.9 Pruebas de aceptación de sistemas y 14.3.1 Protección de los datos de prueba, se asignó un peso menor a causa de que son evaluaciones que respaldan la seguridad en el proceso de desarrollo de sistemas y el producto.

Tal como se aprecia en la Ilustración 11:

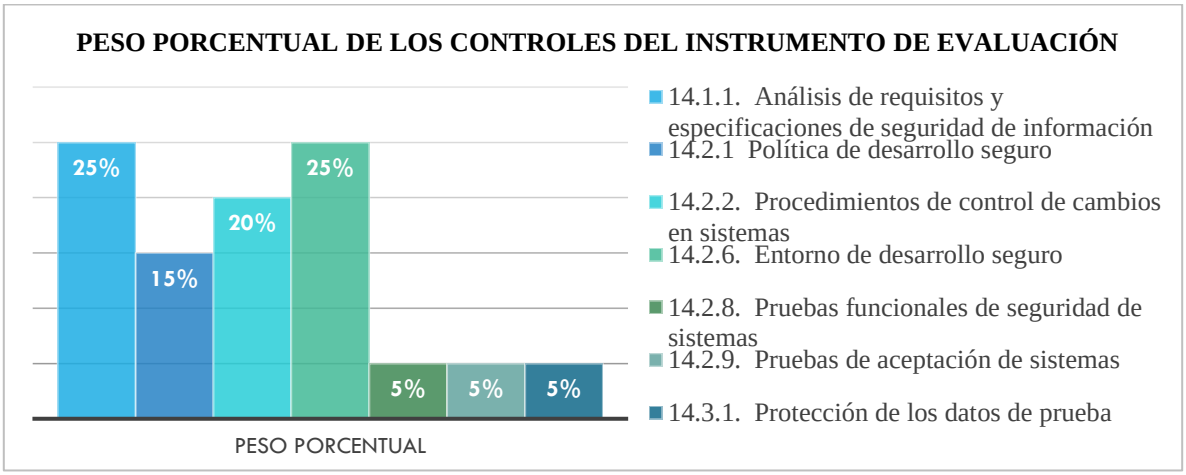


Ilustración 11: Peso porcentual de los controles del Instrumento de Evaluación
Fuente: Elaboración propia (2020)

El instrumento de evaluación tiene un nivel de calificación basado en la propuesta del PAM de COBIT 5, calificado en base a los criterios de puntuación. La tabla 4 muestra los porcentajes y la descripción de cada nivel de calificación.

Tabla 4:
Criterios de Puntuación

Nivel de Calificación	Porcentaje	Descripción del Porcentaje
No Logrado (0% al 20%)	0% 20%	No posee ninguna evidencia y manifiesta desconocimiento de ello. Tiene conocimiento de ello y lo practica a criterio personal.
Parcialmente Logrado (21% al 49%)	40%	Tiene conocimiento de ello y se capacita para ponerlo en práctica. (Maneja en un nivel básico, muy general).
Ampliamente Logrado (50% al 79%)	60%	Cumplimiento parcial del control sin generar evidencia alguna.
Completamente Logrado (80% al 100%)	80%	Cumplimiento del control sin generar evidencia alguna
	100%	Posee evidencia del cumplimiento del control y tiene un amplio conocimiento sobre ello.

Fuente: Elaboración propia (2020)

Actividad 1.2. Validar el instrumento de evaluación

El instrumento de evaluación se validó de acuerdo al conocimiento profesional de 02 expertos: el Mg. Sergio Omar Valladares Castillo y el Ing. Jenson Chambi Aguilar, pertenecientes a la escuela profesional de Ingeniería de Sistemas de la Universidad Peruana Unión. La presentación del instrumento de evaluación se dio de manera virtual, se envió un correo con 03 documentos: Carta de presentación (Anexo 2), Validación del instrumento de evaluación por juicio de experto (Anexo 3) y el Instrumento de evaluación (Anexo 1) para validar el instrumento de evaluación. Al término de una semana enviaron la validación del instrumento (Anexo 4 y 5), se obtuvo una valoración cuantitativa de 30 (Máximo puntaje) siendo favorable.

Actividad 1.3. Realizar evaluación inicial del proceso de desarrollo de software

Para aplicar el instrumento de evaluación se coordinó una reunión virtual con el Gerente de Operaciones, la persona responsable de evaluar y/o verificar el desarrollo del software hasta la entrega del producto. En la reunión virtual el Gerente de Operaciones respondió a todas las preguntas del instrumento de evaluación y se asignó una calificación en función a las respuestas que él daba. Dependiendo de la pregunta se solicitaron evidencias que respaldan el puntaje obtenido. Para la evaluación inicial del proceso de desarrollo de sistemas y el producto se aplicaron tres técnicas de obtención de datos: la entrevista, la observación y la encuesta. En el Anexo 6 se muestra el instrumento de evaluación utilizado con las respuestas brindadas por el Gerente de Operaciones.

Obtenido los datos del proceso se realizó el cálculo del nivel de cumplimiento de cada control de seguridad, se sumó el porcentaje obtenido en cada pregunta en base a los resultados. El porcentaje que se obtuvo por control indica el nivel de cumplimiento de los controles de la seguridad de la información y se expresa en porcentajes para asignar una calificación.

A su vez, se procedió a realizar fórmulas matemáticas para hallar el porcentaje logrado y no logrado por control. El cálculo que se aplicó para hallar el Porcentaje Logrado (PL) es el siguiente, donde:

P =Peso Porcentual del Control

A= Porcentaje obtenido tras la aplicación del instrumento (Acumulado)

$$PL = \frac{Px\ A}{100}$$

El porcentaje logrado en cada control permitió obtener también el porcentaje de lo que Falta Lograr (FL) en la empresa BITNESS CORP. S.A.C., para ello se realizó el siguiente cálculo matemático donde:

P =Peso Porcentual del Control

PL=Porcentaje logrado

$$FL = P - PL$$

En base a las fórmulas se obtuvo los resultados expuestos en la Ilustración 12.

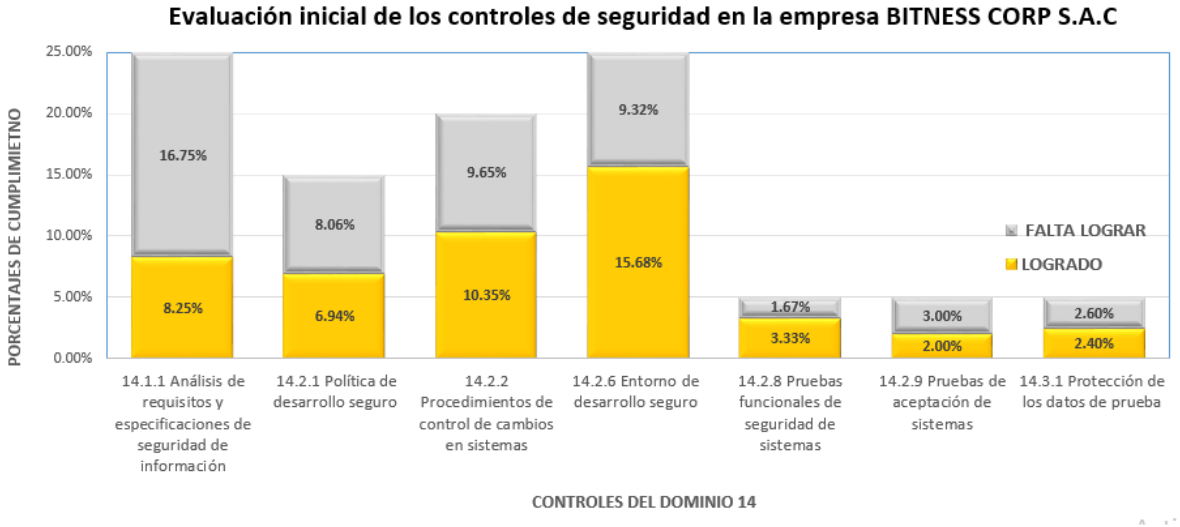


Ilustración 12: Nivel de cumplimiento inicial de los controles en BITNESS CORP. S.A.C.
Fuente: Elaboración propia (2020)

FASE 2: DISEÑO DE CONTROLES DE SEGURIDAD PARA EL PROCESO DE DESARROLLO DE SOFTWARE SEGÚN LA ISO 27002: 2015

Actividad 2.1. Priorizar las oportunidades de mejora (Propuestas de controles de seguridad)

Tras obtener el porcentaje de cada control, se evaluaron aquellos que poseían un alto porcentaje de incumplimiento (FL), siendo de prioridad debido al daño que podrían ocasionar a la empresa BITNESS CORP. S.A.C. Se analizó el riesgo de cada control mediante criterios como: el contexto de la empresa, el conocimiento de las tesistas, el porcentaje de lo que falta lograr que supera por mucho a lo logrado y la situación actual(pandemia). Respecto a ello se

procedió a resaltar de color negro en cursiva aquellos controles poseen un alto riesgo a los cuales se les proporcionara una oportunidad de mejora. Véase en la tabla 5:

Tabla 5:
Cumplimiento de los controles

Controles	Peso	Acumulado	Logrado	Falta Lograr
14.1.1. Análisis de requisitos y especificaciones de seguridad de información	25%	33.00%	8.25%	**16.75%**
14.2.1. Política de desarrollo seguro	15%	46.25%	6.94%	**8.06%**
14.2.2. Procedimientos de control de cambios en sistemas	20%	51.76%	10.35%	**9.65%**
14.2.6. Entorno de desarrollo seguro	25%	62.73%	15.68%	**9.32%**
14.2.8. Pruebas funcionales de seguridad de sistemas	5%	66.67%	3.33%	1.67%
14.2.9. Pruebas de aceptación de sistemas	5%	40.00%	2.00%	3.00%
14.3.1. Protección de los datos de prueba	5%	48.00%	2.40%	2.60%
TOTAL	100%		48.96%	51.04%

Fuente: Elaboración propia (2020)

Se identificó las preguntas de los controles seleccionados que reflejan un solo tema en este caso la "Identificación de requisitos de seguridad". En la Ilustración 13 se aprecia que las preguntas del control 14.1.1., enfocan a una oportunidad de mejora.

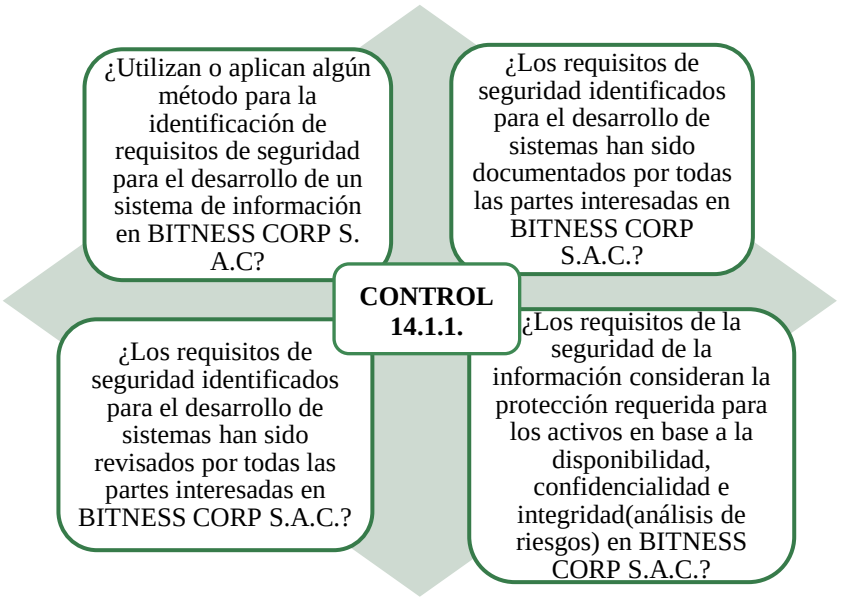


Ilustración 13: Cuestionario del control 14.1.1.
Fuente: Elaboración propia (2020)

Se aplicaron los conocimientos adquiridos y se propuso la oportunidad de mejora que eliminó las deficiencias evidenciadas en el instrumento de evaluación. En la Tabla 6 se observa las oportunidades de mejora que reflejan una solución a las preguntas mencionadas.

Tabla 6:
Oportunidad de mejora

Control	Preguntas	Oportunidades de Mejora
14.1.1	¿Utilizan o aplican algún método para la identificación de requisitos de seguridad para el desarrollo de un sistema de información en BITNESS CORP S. A.C? ¿Los requisitos de seguridad identificados para el desarrollo de sistemas han sido documentados por todas las partes interesadas en BITNESS CORP S.A.C.? ¿Los requisitos de seguridad identificados para el desarrollo de sistemas han sido revisados por todas las partes interesadas en BITNESS CORP S.A.C.? ¿Los requisitos de la seguridad de la información consideran la protección requerida para los activos en base a la disponibilidad, confidencialidad e integridad (análisis de riesgos) en BITNESS CORP S.A.C.?	***Definir un proceso o método para identificar requisitos de seguridad que tenga en cuenta los tres pilares de la información para el caso de los activos, esté debe ser documentado y revisado por las partes interesadas.*** ***Capacitar al personal respecto al método realizado.*** ***Seguimiento del cumplimiento del método brindado.***

Fuente: Elaboración propia (2020)

Se analizó la factibilidad de la implementación de las oportunidades de mejora en base a los 4 criterios de evaluación: “Pandemia, tiempo, costo y conocimiento”. La Tabla 7 muestra la descripción de los criterios de evaluación.

Tabla 7:
Criterios de Evaluación

Criterios de Evaluación	Descripción
Pandemia	Situación actual que restringe determinadas actividades como encuentros entre más de 7 personas.
Tiempo	Tanto la empresa como las tesistas disponen de un tiempo limitado para realizar la investigación.
Costo	El gasto que implica la ejecución de cada oportunidad de mejora ha sido evaluado, para que dicha oportunidad de mejora sea considerada como factible.
Conocimiento	Del equipo de investigación para el desarrollo e implementación de las oportunidades de mejora.

Fuente: Elaboración propia (2020)

Se realizó una valuación a las oportunidades de mejora, en la que se calificó acorde a los puntajes de la Ilustración 14:

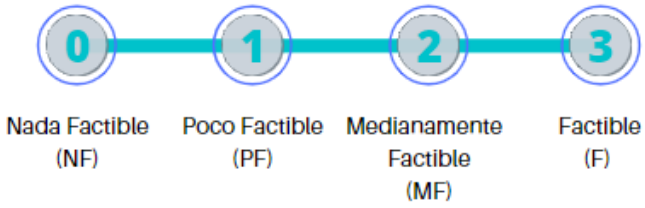


Ilustración 14: Descripción de puntajes
Fuente: Elaboración propia (2020)

Encontrada la calificación se consideró factibles aquellas oportunidades de mejora que obtuvieron una puntuación igual o mayor a 10, siendo estas las oportunidades de mejora escogidas, por ser factibles para desarrollar e implementar. En la Tabla 8 se observa las puntuaciones.

Las oportunidades de mejora priorizadas para implementar se encuentran en negritas siendo su valor es mayor o igual a 10.

Tabla 8:
Evaluación de oportunidades de mejora

Oportunidades de Mejora	Criterios de Evaluación				
	Pandemia	**Tiempo**	**Costo**	**Conocimiento**	**Resultado**
Definir un proceso o método para identificar requisitos de seguridad que tenga en cuenta los tres pilares de la información para el caso de los activos, esté debe ser documentado y revisado por las partes interesadas. *Capacitar al personal respecto al método realizado.* *Seguimiento del cumplimiento del método brindado.*	***2***	***3***	***3***	***2***	***10***
Realizar capacitaciones al personal de BITNES en temas de seguridad en los sistemas de información	2	2	1	1	6
Establecer un proceso que asegure el control de calidad de los productos.	***2***	***2***	***3***	***3***	***10***
Definir una política de seguridad para el desarrollo de aplicaciones seguras y capacitar al personal involucrado	2	2	1	1	6
Definir un proceso o método para el control de cambios en el desarrollo de sistemas, tanto para los sistemas realizados como para los sistemas nuevos, esté debe ser documentado y revisado por las partes interesadas. *Software de apoyo para realizar el control de cambios.*	***2***	***2***	***3***	***3***	***10***
Establecer un modelo de contrato de confidencialidad.	***3***	***3***	***3***	***3***	***12***
Establecer un control de acceso físico Brindar herramientas de apoyo para el acceso físico.	0	3	3	3	9

Fuente: Elaboración propia

Actividad 2.2. Diseñar propuestas de controles de seguridad identificados y priorizados.

Mediante la identificación de las oportunidades de mejora factibles se elaboraron tres procesos y un modelo de contrato de confidencialidad para su implementación en la empresa BITNESS CORP. S.A.C.

OM01: Proceso de Gestión de Requisitos de Seguridad para el desarrollo de sistemas

La primera oportunidad de mejora que se identificó para la empresa BITNESS CORP. S.A.C. es el proceso de la "Gestión de requisitos de seguridad para el desarrollo de sistemas", que comprende la gestión de requisitos de seguridad durante el desarrollo del sistema y del producto, para asegurar que el sistema cumpla con los requisitos de seguridad en base a confidencialidad, integridad y disponibilidad.

La presente oportunidad de mejora surge como respuesta al Instrumento de Evaluación aplicado en la empresa BITNESS CORP. S.A.C., ya que la empresa presentó deficiencias en el control 14.1.1. Análisis de requisitos y especificaciones de seguridad de información obteniendo un 16.75% en lo que falta lograr, por ello se analizó las preguntas del Instrumento de Evaluación para hallar la oportunidad de mejora que resolviera está deficiencia en la empresa BITNESS CORP. S. A.C. En la Tabla 9 se observan las preguntas aplicadas a la empresa junto a la oportunidad de mejora.

Tabla 9:
Preguntas del Instrumento de Evaluación y Oportunidad de Mejora

Preguntas	Oportunidad de Mejora
¿Utilizan o aplican algún método para la identificación de requisitos de seguridad para el desarrollo de un sistema de información en BITNESS CORP S. A.C?	Definir un proceso o método para identificar requisitos de seguridad que tenga en cuenta los tres pilares de la información para el caso de los activos, esté debe ser documentado y revisado por las partes interesadas.
¿Los requisitos de seguridad identificados para el desarrollo de sistemas han sido documentados por todas las partes interesadas en BITNESS CORP S.A.C.?	Capacitar al personal respecto al método realizado. Seguimiento del cumplimiento del método brindado.
¿Los requisitos de seguridad identificados para el desarrollo de sistemas han sido revisados por todas las partes interesadas en BITNESS CORP S.A.C.?	
¿Los requisitos de la seguridad de la información consideran la protección requerida para los activos en base a la disponibilidad, confidencialidad e integridad (análisis de riesgos) en BITNESS CORP S.A.C.?	

Fuente: Elaboración Propia (2020)

El proceso de “Gestión de Requisitos de Seguridad para el Sistema” inicia con la recepción del listado de requisitos del sistema, este listado indica todas las funcionalidades que debe tener el sistema a desarrollar, luego se pasa a clasificar estos requisitos en funcionales (características requeridas) y no funcionales (propiedades del sistema). Como parte del proceso se extraen los requisitos no funcionales para poder enfocarnos en los RNF de Seguridad los cuales se clasificarán en base a los pilares de la seguridad de la información que son la confidencialidad, integridad y disponibilidad, esto será llenado en un formato llamado Inventario de Requisitos de Seguridad. Al tener esta clasificación realizada se toma la decisión de que sea aprobado por el equipo que desea el sistema, si surgieran observaciones estas se analizan y se corrigen para la aprobación del Inventario de Requisitos de Seguridad. Una vez, aceptado el Inventario se documentan los requisitos de Seguridad del Producto en la Matriz de Trazabilidad la cual será informada a los miembros del equipo de desarrollo los cuales identificaran los requisitos de seguridad durante el proceso de desarrollo del sistema. Al identificar los requisitos de seguridad durante el proceso de desarrollo del sistema se realizará una validación, si existen observaciones se corregirán y se vuelven a presentar. Como parte final se define el acceso de información a los integrantes del equipo de desarrollo y se capacita acerca del sistema para el cumplimiento del proceso “Gestión de Requisitos de Seguridad para el Sistema”. Para comprender el proceso descrito observe la Ilustración 15, en la cual se aprecia el flujo del proceso.

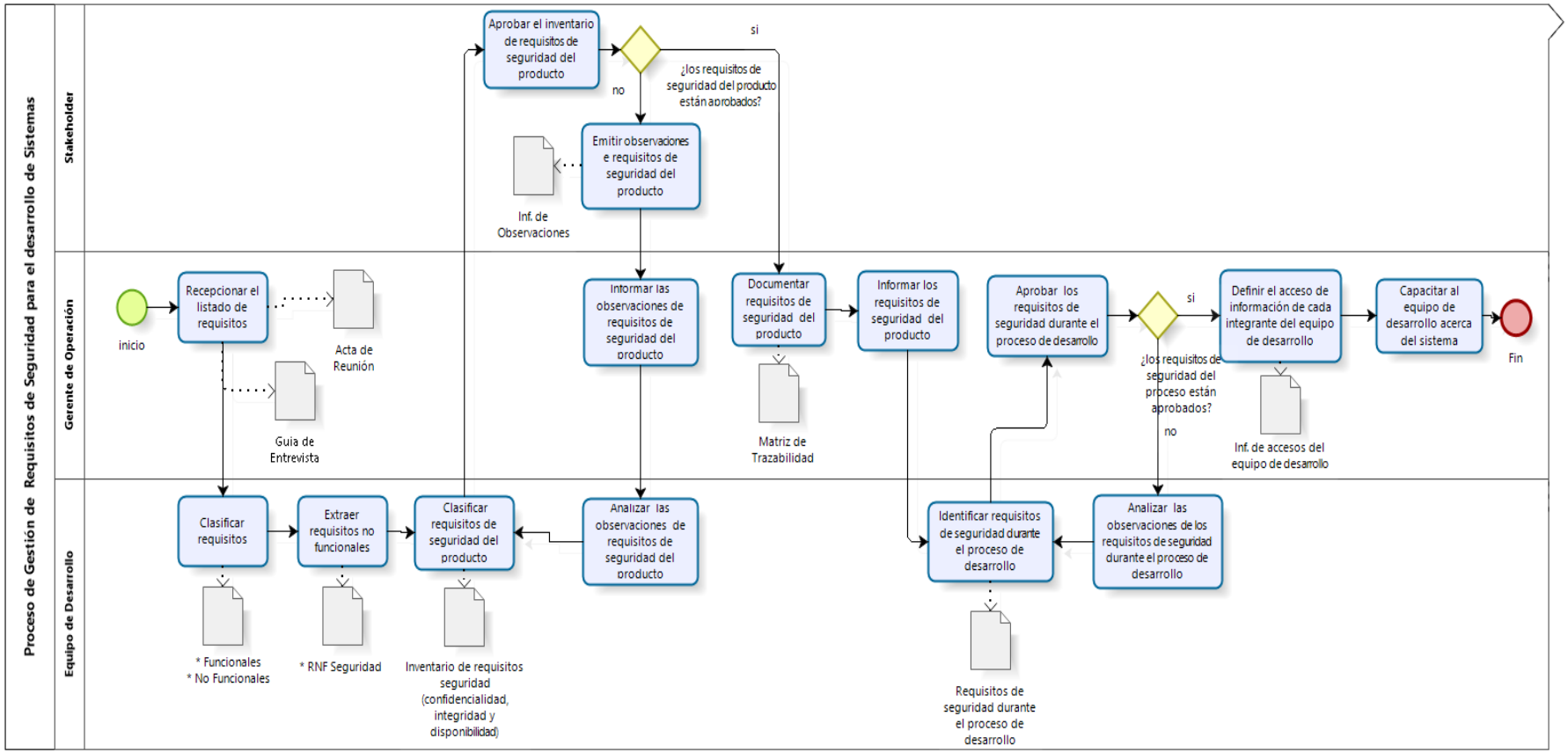


Ilustración 15: Proceso de Gestión de requisitos de seguridad para el desarrollo de sistemas
Fuente: Elaboración propia (2020)

En este proceso se consideró la participación activa de los siguientes roles:

Gerente de Operaciones: Es el rol que lidera al equipo de desarrollo en BITNESS CORP. S.A.C. y en el proceso es el encargado de Gestionar las reuniones con el stakeholder para obtener información y con el equipo de desarrollo para el desarrollo de este.

Equipo desarrollador: Son los expertos de desarrollo del sistema, su principal función es analizar y clasificar los requisitos de seguridad del producto, además de cumplirlos durante todas las etapas del desarrollo del producto.

Stakeholder: Es aquella persona u organización interesada en recibir un servicio o un producto de BITNESS CORP. S.A.C.

El presente proceso cuenta con ocho formatos, los cuales son fundamentales para el cumplimiento de la oportunidad de mejora y a su vez son considerados evidencias de control. La descripción de dichos formatos se observa en la Tabla 10.

Tabla 10:
Descripción de Formatos de la 1° Oportunidad de Mejora

Rol	Cód. de Formato	Nombre del Formato	Descripción
	F01-PM01	Guía de entrevista	Cuestionario guía que incluye preguntas generales a realizar a la empresa que solicita el servicio de BITNESS CORP. S.A.C. (Anexo 7)
Gerente de Operaciones	F02-PM01	Acta de reunión	Se plasman los acuerdos establecidos en cada reunión. (Anexo 8)
Equipo de Desarrollo	F03-PM01	Requisitos funcionales y no funcionales	Clasifica los requisitos funcionales de los no funcionales, esta división permite enfocarnos en los requisitos no funcionales, véase en el (Anexo 9)
Equipo de Desarrollo	F04-PM01	Requisitos no funcionales de seguridad	Se asigna un código y responsable a cada requisito no funcional de seguridad. (Anexo 10)
Equipo de Desarrollo	F05-PM01	Inventario de requisitos de seguridad (Confidencialidad, integridad y disponibilidad)	Se asigna a los requisitos no funcionales su tipo en base a la confidencialidad, integridad y disponibilidad. (Anexo 11)
Stakeholder	F06-PM01	Informe de observaciones	Es opcional ya que pueden existir observaciones del Stakeholder del Inventario tanto como puede ser aceptado sin observación alguna. (Anexo 12)
Gerente de Operaciones	F07-PM01	Matriz de Trazabilidad	Registro especifico de los requisitos incluyendo las instrucciones para realizar un óptimo llenado. (Anexo 13)
Gerente de Operaciones	F08-PM01	Requisito de seguridad durante el desarrollo	Clasifica los requisitos de seguridad durante las etapas del proceso de desarrollo: Elaboración, Ejecución y Transición. (Anexo14)
Gerente de Operaciones	F09-PM01	Informe de accesos del equipo de desarrollo	Brinda información de los accesos al sistema de manera que coincida con la información brindada a los empleados. (Anexo 15)

Fuente: Elaboración Propia (2020)

Todos los formatos realizados son pieza clave para un adecuado cumplimiento del proceso, estos pueden ser modificados de acuerdo al criterio de la empresa BITNESS CORP. S.A.C. La documentación fue enviada al correo corporativo del Gerente de Operaciones de

la empresa BITNESS CORP. S.A.C. Se observa en la Ilustración 15 el proceso de “Gestión de requisitos de seguridad para el desarrollo de sistemas”.

En el Anexo 16 se encuentra el manual del proceso, este cuenta con indicadores, evidencias de control y riesgos. Los indicadores nos permiten medir el cumplimiento del proceso, en este caso se identifican dos, el nivel de cumplimiento de las actividades del proceso y la calidad de los requisitos documentados los cuales son responsabilidad del Gerente de Operaciones. Y como evidencias de control se tiene todos los formatos realizados durante el proceso. Los riesgos que asume la empresa son el incumplimiento del cronograma y la disponibilidad del stakeholder, que son circunstancias fuera del alcance de la empresa.

OM02: Proceso de Adquisición formal del producto o servicio asegurando la calidad.

La segunda oportunidad de mejora es el proceso de "Adquisición formal del producto o servicio asegurando la calidad", que comprende desde la identificación de la necesidad del producto o servicio hasta la negociación de la adquisición del producto o servicio. Esta propuesta se elaboró en base a las preguntas que no se aplicaron en la empresa BITNESS CORP. S.A.C., del instrumento de evaluación, estas preguntas se muestran en la Tabla 11. Al mismo tiempo el diseño del proceso se desarrolló aplicando el conocimiento de los tesistas y una ardua investigación.

Tabla 11:
Las preguntas y la segunda propuesta de Oportunidad de Mejora

Preguntas	Oportunidad de Mejora
¿Existe un proceso de pruebas y adquisición formal para la adquisición de productos en BITNESS CORP S.A.C.? ¿Se evalúan o implementan las guías disponibles para la configuración de seguridad del producto adquirido alineado con el software y los servicios finales en BITNESS CORP S.A.C.?	Establecer un proceso que asegure el control de calidad de los productos
¿Se han definido criterios de aceptación para la adquisición de productos respecto a su funcionalidad para asegurar el cumplimiento de los requisitos de seguridad identificados en BITNESS CORP S.A.C.?	
¿Para la adquisición de un producto o servicios se realizan evaluaciones de acuerdo a los criterios de aceptación definidos en BITNESS CORP. S.A.C.?	

Fuente: Elaboración Propia (2020)

A continuación, la Ilustración 16 muestra el flujo de actividades del proceso mencionado.

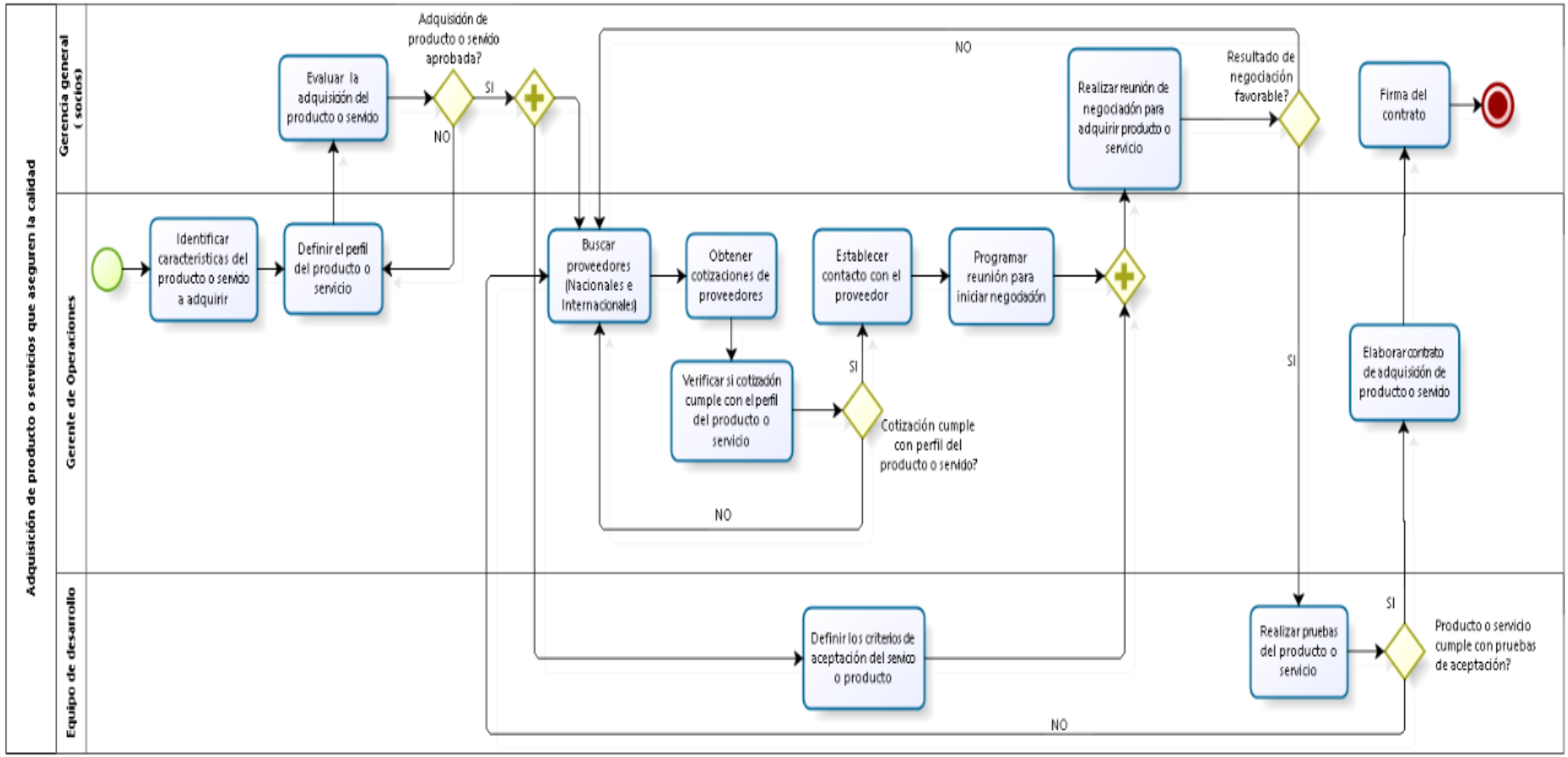


Ilustración 16: Proceso de Adquisición formal del producto o servicio asegurando la calidad
Fuente: Elaboración propia (2020)

La primera actividad que da inicio al proceso es la identificación de la necesidad del producto o servicio a adquirir, seguidamente se define el perfil del producto o servicio para que posteriormente se evalué la adquisición del producto o servicio mediante una decisión si se deniega la adquisición regresa a la actividad de definir el perfil del producto, por lo contrario si se acepta la adquisición entonces se ejecutan paralelamente dos actividades definir los criterios de aceptación del producto o servicio y la búsqueda de proveedores entre nacionales e internacionales paso seguido se procede a obtener las cotizaciones de los proveedores, para luego verificarlas si cumple o no con el perfil del producto o servicio si no cumple las cotizaciones con el perfil entonces se busca otros proveedores, de lo contrario si cumple se establece el contacto con el proveedor y se programa una reunión para precisar la negociación, si el resultado de la negociación no es favorable regresa a la búsqueda de otros proveedores y si es favorable se realizan las pruebas utilizando los criterios de aceptación definidas. Una vez obtenidas los resultados de las pruebas si no cumple con los criterios regresa a la búsqueda de otros proveedores, caso contrario si cumple entonces se elabora el contrato y firman ambas partes.

Además, para este proceso se consideró la participación activa de los siguientes roles:

Gerente de operaciones: Es la persona que inicia el proceso con la identificación de la necesidad del producto o servicio a adquirir y gestionar la adquisición de estos.

Gerencia General (socios): Es el área encargada de tomar las decisiones mediante una evaluación de la adquisición del producto o servicio.

Equipo de desarrollo: Son los expertos en el desarrollo de los sistemas, su principal función en el proceso es realizar los criterios de aceptación del producto y servicio que se va adquirir para posteriormente realizar las pruebas y verificar el cumplimiento de los criterios de aceptación para la adquisición del producto o servicio.

Cabe mencionar que en algunas actividades se diseñó formatos para una documentación eficaz y que sirva como una evidencia de control para el cumplimiento del proceso. La descripción de dichos formatos se observa en la Tabla 12.

Tabla 12:
Descripción de Formatos de la 2° Oportunidad de Mejora

Rol	Cód. de Formato	Nombre del Formato	Descripción
Gerente de Operaciones	F01-PM02	Características técnicas del producto o servicio	Se realiza para identificar de forma detallada qué características técnicas y generales se debe considerar al momento de adquirir un producto o servicio. (Anexo 17)
Gerente de Operaciones	F02-PM02	Perfil del producto	Se realiza en base a la información obtenida del F01 y quedara una información más consolidada de lo que se desea adquirir: producto o servicio. (Anexo 18)
Equipo de desarrollo	F03-PM02	Criterios de aceptación	Se realiza para evaluar el producto o servicio adquirir, utilizando la información del F01. (Anexo 19)
Gerencia General	F04-PM02	Periodo de prueba	Se realiza cuando se haya realizado la negociación. (Anexo 20)
Equipo de desarrollo	F05-PM02	Cronograma de pruebas	Realiza en base a la planificación de las pruebas y el acuerdo de negociación. (Anexo 21)
Equipo de desarrollo	F06-PM02	Informe de periodo de pruebas	Se realiza cuando se obtiene los resultados de la evaluación de los criterios de aceptación. (Anexo 22).

Fuente: Elaboración Propia (2020)

Sin embargo, estos formatos pueden ser modificados de acuerdo al criterio del personal responsable a ejecutar esta tarea de la empresa BITNESS CORP. S.A.C.

En el Anexo 23 se encuentra el manual del proceso, que contiene: el objetivo del proceso, el alcance, definiciones, bases legales y normativa, el diseño de diagrama de procesos, el procedimiento de las actividades con sus tareas detalladas, los indicadores que nos permiten medir el cumplimiento del proceso, en este caso se identifico uno que es el cumplimiento de las actividades el cual es responsabilidad del Gerente de operaciones, Y como evidencias de control se tiene todos los formatos realizados durante el proceso y se consideró los riesgo en caso hubiera se propone un plan de contingencia.

OM03: Proceso de Control de cambios.

La tercera oportunidad de mejora que se identificó para la empresa BITNESS CORP. S.A.C. es el proceso de "Control de Cambios", que comprende desde la solicitud de cambios hasta el cierre de cambio, para asegurar el control adecuado de los cambios y que estos no afecten a la empresa.

La presente oportunidad de mejora surge como respuesta al Instrumento de Evaluación aplicado en la empresa BITNESS CORP. S.A.C., ya que la empresa presentó deficiencias en el control 14.2.2. Procedimientos de control de cambios en sistemas obteniendo un 9.655% en lo que falta lograr, por ello se analizó las preguntas del Instrumento de Evaluación para hallar la oportunidad de mejora que resolviera está deficiencia en la empresa BITNESS CORP. S. A.C. En la Tabla 13 se observan las preguntas aplicadas a la empresa para elaborar la oportunidad de mejora junto a la oportunidad de mejora. Se diseño el proceso conforme al conocimiento de las tesistas e investigaciones.

Tabla 13:
Preguntas del Instrumento de Evaluación y la Tercera Oportunida de Mejora

Preguntas	Oportunidad de Mejora
¿La empresa BITNESS CORP. S.A.C realiza el control de cambios mediante el uso de procedimientos formales durante el ciclo de vida del desarrollo de software?	Definir un proceso o método para el control de cambios en el desarrollo de sistemas, tanto para los sistemas realizados como para los sistemas nuevos, esté debe ser documentado y revisado por las partes interesadas.
¿En la empresa BITNESS CORP. S.A.C se han documentado los procedimientos formales de control de cambios?	Software de apoyo para realizar el control de cambios.
¿En la empresa BITNESS CORP. S.A.C. cumple los procedimientos formales de control de cambios?	
¿La incorporación de sistemas nuevos y cambios importantes sigue un proceso formal de documentación, especificaciones, pruebas, control de calidad y gestión de implantación?	
¿El procedimiento de control de cambios incluye el mantenimiento de registros de auditoría de las solicitudes de cambio? ¿La empresa BITNESS CORP. S.A.C. realiza la monitorización de los cambios en el producto?	

Fuente: Elaboración Propia (2020)

A continuación, la Ilustración 17 muestra el flujo de actividades del proceso mencionado.

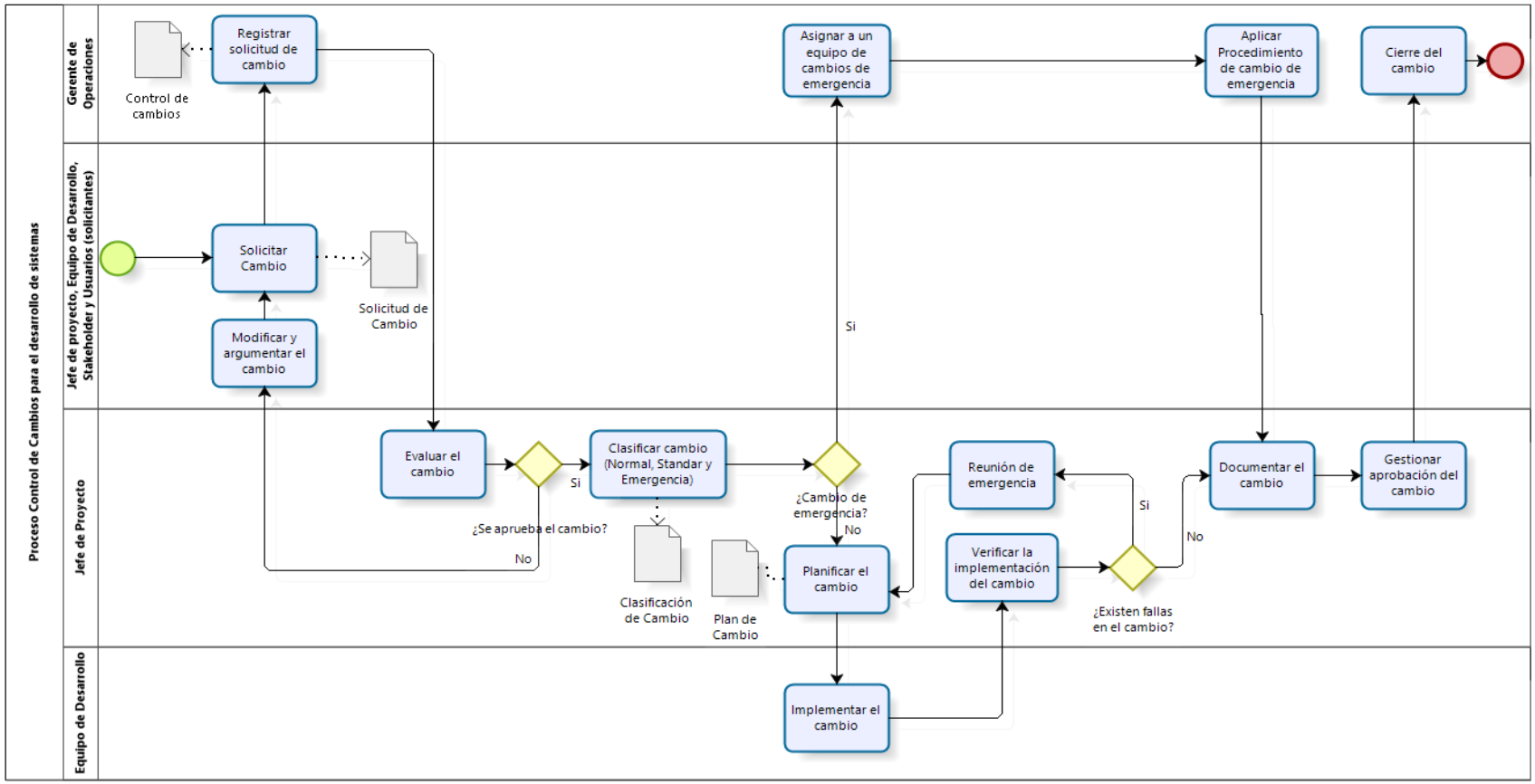


Ilustración 17:Proceso de Control de cambios para el desarrollo de sistemas
Fuente: Elaboración propia (2020)

El proceso de “Control de cambios”, da inicio con la solicitud del cambio donde se justifica la necesidad del cambio, después se procede a registrar la solicitud del cambio en un formato Excel que se le demonina Control de cambios, siguidamente se realiza la evaluación de la solicitud del cambio para deliberar si se aprueba dicha solicitud o no, si no se aprueba el solicitante tiene que modificar y argumentar bien el cambio para que nuevamente presente su solicitud, de lo contrario si se aprueba se clasifica el tipo de cambio: normal, estándar o de emergencia. Si el cambio es normal o estándar entonces se realiza el plan de cambio, de manera que se pueda implementar el cambio. Una vez implementado el cambio se procede a verificar la implementación y se toma una decisión si existen fallas en la implementación de cambio, se convoca a una reunión de emergencia y nuevamente se planifica el cambio, si no existen fallan se continua con la documentación del cambio, se gestiona la aprobación y por ultimo el cierre de cambio. Sin embargo si el cambio es de emergencia el procedimiento cambia se asigna a un equipo consultos de cambios de emergencia se analiza el cambio y se aplica los procedimientos de cambio de emergencia hasta encontrar una solución optima. Ya encontrada la solución se documenta, se gestiona su aprobación del cambio y se realiza el cierre de cambio.

En este proceso se consideró la participación activa de los siguientes roles:

Solicitante de cambio: Es la persona que solicita y registra el cambio, puede ser un usuario o integrante del Equipo de Desarrollo.

Gerente de Operaciones: Es encargado del equipo de desarrollo en BITNESS CORP. S.A.C. y en el proceso es el encargado de registrar los cambios del sistema y actuar ante un cambio de emergencia.

Jefe del proyecto: Es el líder del proyecto, en el proceso es el que realiza la mayor cantidad de actividades ya que cuenta con la función de clasificar el cambio, planificarlo, verificarlo entre otras actividades importantes en el control de cambios.

Equipo de Desarrollo: Son los expertos en el desarrollo de los sistemas, su principal función en el proceso es implementar el cambio.

Cabe mencionar que en algunas actividades se diseñó formatos para una documentación eficaz y que sirva como una evidencia de control para el cumplimiento del proceso. La descripción de dichos formatos se observa en la Tabla 14.

Tabla 14:
Descripción de Formatos de la 3° Oportunidad de Mejora

Rol	Cód. de Formato	Nombre del Formato	Descripción
Solicitante	F01-PM03	Solicitud de cambio	Se realiza para describir la naturaleza del cambio, justificar el motivo del cambio y los modulos que afectarián si no se da la solución(Anexo 24)
Gerente de Operaciones	F02-PM03	Control de cambios	Se realiza en base a la información obtenida del F01, es un registro de toda la información que se obtendrá al realizar el cumplimiento de todas las actividades. (Anexo 25)
Jefe de proyecto	F03-PM03	Clasificación de cambio	Se realiza para identificar y prioricar el tipo de cambio a la que se atenderá. (Anexo 26)
Equipo de desarrollo	F06-PM03	Plan de cambio	Se realiza cuando se identifica el cambio ya sea normal o estándar, donde se describirán las tareas a realizar para una solución óptima. (Anexo 27).

Fuente: Elaboración Propia (2020)

Todos los formatos realizados es fundamental para un adecuado cumplimiento del proceso, estos pueden ser modificados de acuerdo al criterio de la empresa BITNESS CORP. S.A.C. La documentación fue enviada al correo corporativo del Gerente de Operaciones de la empresa BITNESS CORP. S.A.C.

En el Anexo 28 se encuentra el manual del proceso, este cuenta con indicadores, evidencias de control y riesgos. Los indicadores nos permiten medir el cumplimiento del proceso, en este caso se identifican tres, el nivel de cumplimiento de las actividades del proceso, Números de cambios promamados / implementados y Número de cambios exitosos / ejecutados los cuales son responsabilidad del Gerente de Operaciones. Y como evidencias de control se tiene todos los formatos realizados durante el proceso. El riesgo que asume la empresa es el incumplimiento de control de cambios ya que por circunstancias eventuales no se registre correctamente la información del proceso de cambio.

OM04: Contrato de Confidencialidad.

La cuarta oportunidad de mejora es un documento de Contrato de Confidencialidad que permite el acuerdo de las partes para la protección de la información brindada por la empresa y a la no divulgación del Equipo de desarrollo, el formato se encuentra en el Anexo 29.

Actividad 2.3. Aprobar propuestas diseñadas de oportunidades de mejora

Para la presentación y aprobación formal de las oportunidades de mejora se establecieron fechas de reunión, en las cuales se procedió a explicar las oportunidades de mejora con su respectiva documentación y se respondieron todas las inquietudes al Gerente de Operaciones.

La primera oportunidad de mejora "**Proceso de Gestión de Requisitos de Seguridad para el desarrollo de sistemas",** se presentó al Gerente de Operaciones de la BITNESS CORP. S.A.C., el 07 de septiembre de 2020. Esta presentación incluyó la documentación del proceso y sus respectivos formatos. Al finalizar la presentación se realizó la firma del Acta de aceptación y aprobación de la oportunidad de mejora que se encuentra en el Anexo 30 y se realizó la entrega de la documentación correspondiente.

La segunda oportunidad de mejora "**Proceso de Adquisición formal del producto o servicio asegurando la calidad.",** se presentó al Gerente de Operaciones de la BITNESS CORP. S.A.C., el 03 de diciembre de 2020. Esta presentación incluyó la documentación del proceso y sus respectivos formatos. Al finalizar la presentación se realizó la firma del Acta de aceptación y aprobación de la oportunidad de mejora que se encuentra en el Anexo 31 y se realizó la entrega de la documentación correspondiente.

La tercera oportunidad de mejora "**Proceso de Control de cambios.",** se presentó al Gerente de Operaciones de la BITNESS CORP. S.A.C., el 13 de Enero de 2021. Esta presentación incluyó la documentación del proceso y sus respectivos formatos. Al finalizar la presentación se realizó la firma del Acta de aceptación y aprobación de la oportunidad de

mejora que se encuentra en el Anexo 32 y se realizó la entrega de la documentación correspondiente.

Al finalizar cada presentación se realizó la firma del Acta de aceptación (Anexo 33) de cada oportunidad de mejora y la entrega de la documentación correspondiente.

FASE 3: IMPLEMENTAR OPORTUNIDADES DE MEJORA DE SEGURIDAD DISEÑADA

Actividad 3.1. Programar la implementación de las oportunidades de mejora diseñados

Se establecieron fechas para la implementación de las oportunidades de mejora diseñadas, conforme a la disponibilidad de la empresa BITNESS CORP. S.A.C, según se observa en la Tabla 15:

Tabla 15:
Programación de Oportunidades de Mejora

N°	Oportunidad de Mejora	Fecha	Asistentes
1	Proceso de Gestión de Requisitos de Seguridad para el desarrollo de sistemas	13/01/2021	Dirección General Gerente de Operaciones Analista Programadores
2	Proceso de Adquisición formal del producto o servicio asegurando la calidad.	Observación	
3	Proceso de Control de cambios.	Observación	
4	Contrato de confidencialidad.	20/02/2021	

Fuente: Elaboración Propia (2020)

Como se observa en la Tabla 15, para las OM02y OM03 no se defienieron fechas, los motivos se describen a continuación:

OM02: Proceso de Adquisición formal de producto o servicio asegurando la calidad

Tras una evaluación para la implementación de la segunda oportunidad de mejora "Proceso de Adquisición formal de producto o servicio asegurando la calidad", con la participación del Gerente de Operaciones se concluye que la coyuntura actual (Pandemia), es causa importante para la adquisición de un producto o servicio en la empresa BITNESS CORP.S.A.C. y además no cuenta con un presupuesto asignado de adquisición.

OM03: Proceso de Control de Cambios

Tras una evaluación para la implementación de la tercera oportunidad de mejora "Proceso de Control de Cambios", con la participación del Gerente de Operaciones se concluye que no es posible aplicar la tercera oportunidad de mejora, ya que actualmente, los proyectos que están trabajando no cumplen con las características necesarias para la implementación del proceso en la empresa BITNESS CORP.S.A.C.

Actividad 3.2. Implementar oportunidades de mejora de seguridad diseñadas

Para la implementación de las oportunidades de mejora se procedió a realizar una reunión con el Gerente de Operaciones de la empresa BITNESS CORP. S.A.C. En dicha reunión, se acordó la implementación de la OM01 por medio de una simulación con datos reales, debido a la coyuntura de la pandemia del COVID 19.

OM01: Proceso de Gestión de Requisitos de Seguridad para el desarrollo de sistemas

Según la fecha acordada, 13 de enero de 2021, se realizó la reunión con el Gerente de Operaciones de BITNESS CORP S.A.C. para dar inicio a la implementación del "**Proceso de Gestión de Requisitos de Seguridad para el desarrollo de sistemas".** En dicha reunión se acordó trabajar con un proyecto de desarrollo de software correspondiente a la empresa Miguelito. Se dio la difusión del proceso para la aplicación de los formatos.

El representante de la empresa Miguelito S.A.C y el Gerente de Operaciones de BITNESS CORP., se reúnen para la identificación de requisitos del sistemas, en la cual el Gerente de Operaciones hace uso de la Guia de Entrevista **formato F01–PM01** Anexo 34 , Para concretar la reunión el Gerente de operación registra lo acordado en el Acta de Reunión **formato F02–PM01** Anexo 35. firmada por los asistentes, esto se da en la segunda reunión.

En la Tercera reunión El Gerente de Operaciones se reúne con el Equipo de Desarrollo y el equipo de seguimiento (Tesistas) para dar continuidad a la implementación del proceso. Se realizó el análisis de la clasificación de los requisitos funcionales y no funcionales utilizando el **formato F03–PM01** Anexo 36**.** Luego se revisó y analizó la documentación de los requisitos no funcionales para documentarlos en el formato de Requisitos no Funcionales de seguridad **F04–PM01** Anexo 37**.** Una vez que se obtuvó el documento de requerimientos no funcionales de seguridad se clasificó los requisitos de seguridad del producto en base a

los tres pilares de integridad, confidencialidad y disponibilidad, esta información se detalló en el **Inventario de Requisitos de Seguridad del Producto** formato **F05–PM01** Anexo 38**.** Para consolidar la información obtenida de los formatos ya aplicados se elaboró la **Matriz de Trazabilidad** en el **formato F07-PM01** Anexo 39**.** En cada etapa del proceso de desarrollo se identificaron requisitos de seguridad, se consideró, como etapas de desarrollo: Elaboración, Ejecución y Transición, las cuales se describieron en el formato **F08–PM01** Anexo 40 **de Requisitos de seguridad durante el proceso de desarrollo.** Después de la identificación de los requisitos de seguridad del proceso de desarrollo se delimitaron los accesos por roles en el formato **F09-PM** Anexo 41 **Informe de accesos del Equipo de Desarrollo.** Todas las actividades fueron realizadas para asegurar un desarrollo de calidad.

Ilustración 18: Etapas de la implementación del "Proceso de Gestión de Requisitos de Seguridad para el desarrollo de sistemas"..
Fuente: Elaboración Propia (2021)

OM04: Implementación del Contrato de Confidencialidad

El 20 de febrero de 2021, se implementó la cuarta oportunidad de mejora "**Contrato de Confidencialidad."** para el proyecto Miguelito, previa coordinación con el Gerente de operaciones se realizó una reunión con el Equipo de desarrollo para explicar la importancia

de la firma del contrato de confidencialidad en los proyectos de desarrollo de software de acuerdo a la ISO 27002:2015 este contrato busca proteger la información que entrega el cliente, como la información que se genera en el desarrollo del proyecto. Los miembros del Equipo de desarrollo que firmaron el contrato del proyecto de Miguelito fueron el Analista y el Jefe de Proyecto comprometiéndose a no divulgar la información de la Corporación Miguelito S.A.C., estos contratos se pueden visualizar en el Anexo 42.

FASE 4: EVALUACIÓN FINAL DEL CUMPLIMIENTO DE LOS CONTROLES DE SEGURIDAD EN EL PROCESO DE DESARROLLO DE SOFTWARE Y EL PRODUCTO DE LA EMPRESA BITNESS CORP.S.A.C., SEGÚN LA ISO 27002:2015

Actividad 4.1 Realizar evaluación final

Para aplicar el instrumento de evaluación se coordinó una reunión virtual con fecha del 21 de febrero del 2021 con el Gerente de Operaciones, la persona responsable de evaluar y/o verificar el desarrollo del software hasta la entrega del producto. En la reunión virtual el Gerente de Operaciones respondió a todas las preguntas del instrumento de evaluación y se asignó una calificación en función a las respuestas que él daba. Dependiendo de la pregunta se solicitaron evidencias que respaldan el puntaje obtenido. Para la evaluación final del proceso de desarrollo de sistemas y el producto tras haber implementado los procesos y el contrato de confidencialidad se aplicaron tres técnicas de obtención de datos: la entrevista, la observación y la encuesta. En el Anexo 43 se muestra el instrumento de evaluación utilizado con las respuestas brindadas por el Gerente de Operaciones.

Actividad 4.2 Calcular resultados de la mejora

Esta actividad consiste en obtener la data que permite hacer el cálculo del nivel de cumplimento de seguridad de la información en el proceso de desarrollo de sistemas y el producto.

Obtenidos los resultados de la aplicación del instrumento para la evalución final, se realizó el cálculo del nivel de cumplimiento de cada control de seguridad, se sumó el porcentaje obtenido en cada pregunta en base a los resultados. El porcentaje que se obtuvo

por control indica el nivel de cumplimiento de los controles de seguridad de la información y se expresa en porcentajes para asignar una calificación.

Los resultados reflejan mejoras significativas por cada control de seguridad evaluado, lo que se visualiza en la Ilustración 18:

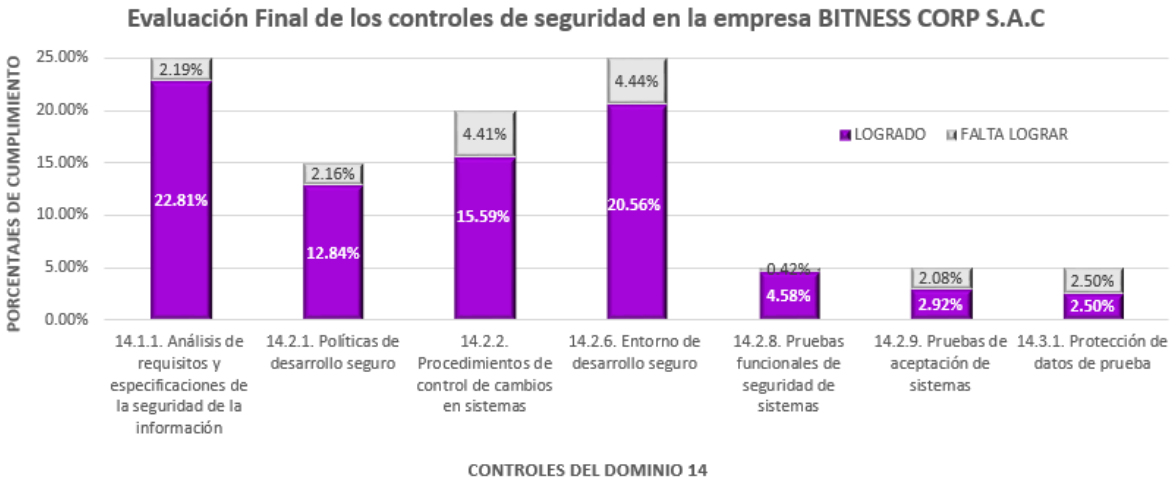


Ilustración 19: Evaluación Final de los Controles de Seguridad en la Empresa BITNESS CORP. S.A.C.
Fuente: Elaboración Propia (2021)

La Ilustración 18 refleja que el control 14.1.1. Análisis de Requisitos y especificaciones de la seguridad de la información alcanzó un 22.81% de un valor esperado de 25% siendo el control con mayor cumplimiento del nivel de seguridad esperado en la empresa BITNESS CORP. S.A.C. Para este control de seguridad se implementó el "Proceso de Gestión de Requisitos de seguridad para el desarrollo de sistemas" y el documento de "Contrato de Confidencialidad" y se diseño el "Proceso de Adquisición formal de producto o servicio asegurando la calidad".

El control de seguridad 14.2.1. Políticas de desarrollo seguro alcanzó un 12.84% de un valor esperado de 15%. La oportunidad de mejora asociada a este control es el "Proceso de Gestión de Requisitos de seguridad para el desarrollo de sistemas", este proceso está implementado.

El control de seguridad 14.2.2. Procedimientos de control de cambios en sistemas alcanzó un 15.59% de un valor esperado del 20%. La oportunidad de mejora asociada a este control es el “Proceso de Control de Cambios”.

El control de seguridad 14.2.6. Entorno de desarrollo seguro alcanzó un 20.56% de un valor esperado del 25%. Las oportunidades de mejora implementadas referentes a este control son el “Proceso de Gestión de Requisitos de seguridad para el desarrollo de sistemas” y el documento de“Contrato de Confidencialidad”.

El control de seguridad 14.2.8. Pruebas funcionales de seguridad de sistemas alcanzó un 3.75% de un valor esperado del 5%. En este control de seguridad de información no se logro implementar oportunidades de mejora debido a los criterios de evaluación (Pandemia, Tiempo, Costo y Conocimiento).

El control de seguridad 14.2.9. Pruebas de aceptación de sistemas alcanzó un 2.92% de un valor esperado del 5%. En este control de seguridad de información no se logro implementar oportunidades de mejora debido a los criterios de evaluación (Pandemia, Tiempo, Costo y Conocimiento).

El control de seguridad 14.3.1. Protección de datos de prueba alcanzó un 2.50% de un nivel esperado del 5%. Este control de seguridad refiere a la cuarta oportunidad de mejora de documento de “Contrato de Confidencialidad” implementado en la empresa BITNESS CORP. S.A.C.

Es importante saber que se dearrolló una capacitación informativa sobre aquellas oportunidades de mejora que no se llegaron a implementar. En la cual se detalló el uso de la documentación correspondiente.

CAPÍTULO VI:

RESULTADOS Y DISCUSIÓN DE LA INVESTIGACIÓN

6.1. ANALISIS DE RESULTADOS

En la evaluación inicial los resultados obtenidos se muestran en la Tabla 16, cuyos porcentajes logrados alcanzan el 48.95% encontrándose en la escala de calificación en el nivel Parcialmente Logrado, estos resultados reflejan que en la empresa BITNESS CORP. S.A.C. tiene conocimiento de los controles de seguridad en un nivel básico.

Tabla 16:
Evaluación Inicial del Cumplimiento de los Controles de Seguridad

Control de Seguridad	**Nivel de Cumplimiento Esperado**	**Evaluación Inicial**	
		Logrado	**No logrado**
14.1.1. Análisis de requisitos y especificaciones de la seguridad de la información	25%	8.25%	16.75%
14.2.1. Políticas de desarrollo seguro	15%	6.94%	8.06%
14.2.2. Procedimientos de control de cambios en sistemas	20%	10.35%	9.65%
14.2.6. Entorno de desarrollo seguro	25%	15.68%	9.32%
14.2.8. Pruebas funcionales de seguridad de sistemas	5%	3.33%	1.67%
14.2.9. Pruebas de aceptación de sistemas	5%	2%	3%
14.3.1. Protección de datos de prueba	5%	2.4%	2.6%
Total	100%	48.95%	51.05%

Fuente: Elaboración Propia (2020)

A continuación, se presenta en la Tabla 17, los resultados de la evaluación posterior a la implementación de las oportunidades de mejora. En la evaluación final los resultados obtenidos alcanzan el 81.80% encontrándose en la escala de calificación en el nivel Completamente Logrado, reflejando que en la empresa BITNESS CORP. S.A.C. tiene evidencia(documentación) de los controles implementados además de tener un mayor conocimiento acerca de los controles de seguridad.

Tabla 17:
Evaluación Final del Cumplimiento de los Controles de Seguridad

Control de Seguridad	Nivel de Cumplimiento Esperado	Evaluación Final	
		Logrado	**No Logrado**
14.1.1. Análisis de requisitos y especificaciones de la seguridad de la información	25%	22.81%	2.19%
14.2.1. Políticas de desarrollo seguro	15%	12.84%	2.16%
14.2.2. Procedimientos de control de cambios en sistemas	20%	15.59%	4.41%
14.2.6. Entorno de desarrollo seguro	25%	20.56%	4.44%
14.2.8. Pruebas funcionales de seguridad de sistemas	5%	4.58%	0.42%
14.2.9. Pruebas de aceptación de sistemas	5%	2.92%	2.08%
14.3.1. Protección de datos de prueba	5%	2.50%	2.50%
Total	100%	81.80%	18.20%

Fuente: Elaboración Propia (2020)

6.2. ANALISIS POR CONTROLES

Las mejoras que se hicieron para el control 14.1.1. Análisis de requisitos y especificaciones de la seguridad de la información reflejan un 8.25% en la evaluación inicial y un incremento en la evaluación final del 22.81% en el nivel de seguridad, de un porcentaje esperado del 25%.

Este incremento se dió gracias a la implementación del “Proceso de Gestión de Requisitos de seguridad para el desarrollo de sistemas”, desarrollando la identificación de requisitos de seguridad, documentándolos, revisándolos y siendo difundidos al personal de la empresa BITNESS CORP. S.A.C. Ademas, se documento la delimitación de acceso de los usuarios en base a sus deberes y responsabilidades. El documento de “Contrato de Confidencialidad” se implementó en el control para la protección de la información recibida para el desarrollo de sistemas. Tambien se diseño el “Proceso de Adquisición formal de producto o servicio asegurando la calidad” el cual define los criterios de aceptación para el producto o servicio a adquirir asegurando el cumplimiento de requisitos de seguridad.

La Ilustración 20 muestra la comparación del porcentaje alcanzado en la Evaluación Inicial y Final.

Ilustración 20: Nivel de Cumplimiento del Control de Seguridad 14.1.1. en la Empresa BITNESS CORP. S.A.C.
Fuente: Elaboración Propia (2021)

Las mejoras que se hicieron para el control 14.2.1. Políticas de Desarrollo Seguro reflejan un 6.94% en la evaluación inicial y un incremento en la evaluación final del 12.84% en el nivel de seguridad, de un porcentaje esperado del 15%.

Este incremento se dió gracias a la implementación del "Proceso de Gestión de Requisitos de seguridad para el desarrollo de sistemas", estableciendo reglas en las etapas de desarrollo de sistemas y del producto, también el diseño del proceso permitió aplicar políticas de desarrollo seguro, asimismo repositorios seguros y control de versiones.

La Ilustración 21 muestra la comparación del porcentaje alcanzado en la Evaluación Inicial y Final.

Ilustración 21:Nivel de Cumplimiento del Control de Seguridad 14.2.1. en la Empresa BITNESS CORP. S.A.C.
Fuente: Elaboración Propia (2021)

Las mejoras que se hicieron para el control 14.2.2. Procedemientos de Control de Cambios reflejan un 10.35% en la evaluación inicial y un incremento en la evaluación final del 15.59% en el nivel de seguridad, de un porcentaje esperado del 20%.

Este incremento se dió gracias al diseño del "Proceso de Control de cambios", este realiza un procedimiento formal documentado de control de cambios durante el ciclo de vida del desarrollo del software incluyendo una evaluación de riesgos, pruebas, y gestión de la implementación. El procedimiento de control de cambios incluye la identificación del software (información, base de datos, hardware) que requieren un cambio y a los usuarios autorizados para el desarrollo del cambio, actualiza la documentación del sistema manteniendo un control de cambios de versiones y solicitudes de cambio, estas tareas se realizan mediante la secuencia de las actividades del proceso incluyendo la aprobación de las propuestas detalladas antes de la ejecución del trabajo.

La Ilustración 22 muestra la comparación del porcentaje alcanzado en la Evaluación Inicial y Final

Ilustración 22:Nivel de Cumplimiento del Control de Seguridad 14.2.2. en la Empresa BITNESS CORP. S.A.C.
Fuente: Elaboración Propia (2021)

Las mejoras que se hicieron para el control 14.2.6. Desarrollo de Entorno Seguro reflejan un 15.68% en la evaluación inicial y un incremento en la evaluación final del 20.56% en el nivel de seguridad, de un porcentaje esperado del 25%.

Este incremento se dió gracias a la implementación del "Proceso de Gestión de Requisitos de seguridad para el desarrollo de sistemas", que implica el cumplimiento de los requisitos de seguridad en cada etapa de desarrollo de sistemas por parte del equipo de desarrollo. Además, establece sanciones a aquellos miembros del equipo de desarrollo que no cumplen el documento de "Contrato de Confidencialidad" el cual se implementó para la protección de la información recibida para el desarrollo de sistemas.

La Ilustración 23 muestra la comparación del porcentaje alcanzado en la Evaluación Inicial y Final.

Ilustración 23: Nivel de Cumplimiento del Control de Seguridad 14.2.6. en la Empresa BITNESS CORP. S.A.C.
Fuente: Elaboración Propia (2021)

Las mejoras que se hicieron para el control 14.2.8. Pruebas Funcionales de Seguridad de Sistemas reflejan un 3.33% en la evaluación inicial y un incremento en la evaluación final del 4.58% en el nivel de seguridad, de un porcentaje esperado del 5%.

Este incremento se dió gracias a que la empresa BITNESS CORP. S.A.C.implemetó pruebas de aceptación independientes para el desarrollo interno y externo. Para este control no se desarrollo la oportunidad de mejora debido a los criterios de evaluación definidos (Pandemia, Tiempo, Costo y Conocimiento).

La Ilustración 24 muestra la comparación del porcentaje alcanzado en la Evaluación Inicial y Final.

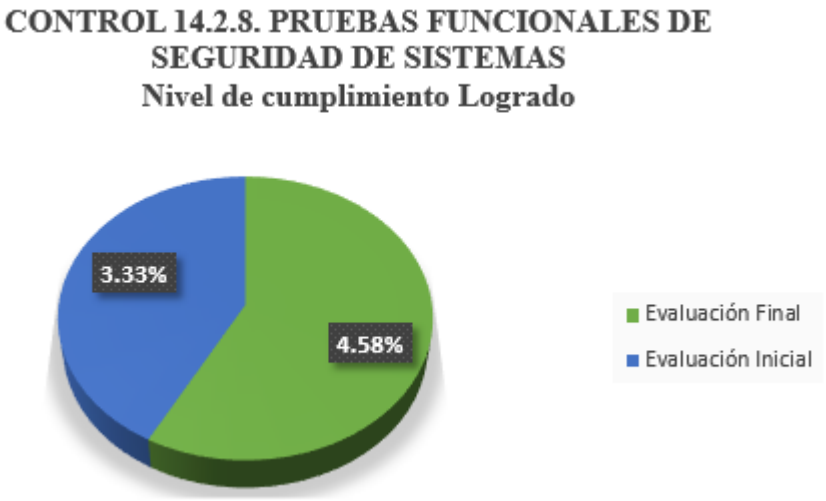


Ilustración 24: Nivel de Cumplimiento del Control de Seguridad 14.2.8. en la Empresa BITNESS CORP. S.A.C.
Fuente: Elaboración Propia (2021)

Las mejoras que se hicieron para el control 14.2.9. Pruebas de Aceptación de Sistemas reflejan un 2.00% en la evaluación inicial y un incremento en la evaluación final del 2.92% en el nivel de seguridad, de un porcentaje esperado del 5%.

Este incremento se dió gracias a las pruebas de aceptación que BITNESS CORP. S.A.C incluyó en las practicas de desarrollo seguro de sistemas y en los componentes recibidos. Para este control no se desarrollo la oportunidad de mejora debido a los criterios de evaluación definidos (Pandemia, Tiempo, Costo y Conocimiento).

La Ilustración 25 muestra la comparación del porcentaje alcanzado en la Evaluación Inicial y Final.

Ilustración 25: Nivel de Cumplimiento del Control de Seguridad 14.2.9. en la Empresa BITNESS CORP. S.A.C.
Fuente: Elaboración Propia (2021)

Las mejoras que se hicieron para el control 14.3.1. Pruebas de protección de datos reflejan un 2.40% en la evaluación inicial y un incremento en la evaluación final del 2.50% en el nivel de seguridad, de un porcentaje esperado del 5%.

Este incremento se dió gracias a la implementación del documento "Contrato de Confidencialidad" para evitar el uso de datos reales o divulgar información confidencial para las pruebas, en caso de que se use datos reales o información confidencial esta debe cumplir con las obligaciones de confidencialidad definidas en este documento.

La Ilustración 26 muestra la comparación del porcentaje alcanzado en la Evaluación Inicial y Final.

Ilustración 26: Nivel de Cumplimiento del Control de Seguridad 14.3.1. en la Empresa BITNESS CORP. S.A.C.
Fuente: Elaboración Propia (2021)

En la Ilustración 27 se visualiza el estado de la evaluación inicial y final de la empresa BITNESS CORP. S.A.C. con respecto al nivel de seguridad de la información. La implementación de los controles de seguridad incidió positivamente en el nivel de seguridad de la empresa alcanzando en la evaluación final el resultado de 81.80% encontrándose en el nivel de calificación Completamente Logrado.

Ilustración 27: Nivel de Seguridad en la empresa BITNESS CORP. S.A.C.
Fuente: Elaboración Propia (2021)

CAPÍTULO VII

CONCLUSIONES Y RECOMENDACIONES

7.1. CONCLUSIONES

La presente investigación llega a las siguientes conclusiones:

1. Los controles de la seguridad de la información implementados en esta investigación fueron la base fundamental para determinar la mejora del nivel seguridad en el proceso de desarrollo de sistemas y del producto. La evaluación inicial del proceso en estudio, tuvo una resultado del 48.95%, eso ubica al nivel de seguridad del proceso como Parcialmente Logrado. Se alcanzó un 81.80% de cumplimiento en los controles de seguridad, lo que evidencia un incremento del 32.85% del nivel seguridad de la información luego de implementar las oportunidades de mejora diseñadas, esto uiere decir ue durante la implementación el Gerente de Operaciones se comprometio a cumplir cada una de las actividades del proceso implementado, se capacito al personal de la empresa BITNESS CORP. S. a. C. Finalmente el personal participo en el desarrollo de las actividades de las oportunidades de mejora.
2. Para la seguridad de la información en el proceso de desarrollo de sistemas se consideraron los controles 14.1.1. Analisis de requisitos y especificaciones de seguridad de la información, 14.2.1. Politicas de desarrollo seguro, 14.2.2. Procedimientos de control de cambios de sistemas y 14.2.6. Entorno de desarrollo seguro. Luego de realizadas las mejoras en estos controles de seguridad, se puede evidenciar una mejora del nivel de seguridad en un 14.66% para el control 14.1.1. Analisis de requisitos y especificaciones de seguridad de la información, en un 5.90% para el control 14.2.1. Politicas de desarrollo seguro, en un 5.24% para el control 14.2.2. Procedimientos de control de cambios de sistemas y en un 4.88% para el control 14.2.6. Entorno de desarrollo de seguro. Los resultados de la evaluación inicial se puede ver en la Tabla 16 y la evaluación final de cada control se pueden ver en la Tabla 17.

3. Para la seguridad de la información del producto se consideraron los controles 14.1.1. Analisis Analisis de requisitos y especificaciones de seguridad de la información, 14.2.6. Entorno de desarrollo de seguro y el control 14.3.1. Protección de datos de prueba. Luego

de realizadas las mejoras en estos controles de seguridad, se puede evidenciar una mejora del nivel de seguridad en un 14.66% para el control 14.1.1. Analisis de requisitos y especificaciones de seguridad de la información, en un 4.88% para el control 14.2.6. Entorno de desarrollo de seguro y en un 0.10% para el control 14.3.1. Protección de datos de prueba. Los resultados de la evaluación inicial se puede ver en la Tabla 16 y la evaluación final de cada control se pueden ver en la Tabla 17.

4. La evaluación inicial permitió conocer las carencias respecto a la seguridad de la información durante el proceso de desarrollo y del producto de la empresa BITNESS CORP. S.A.C las cuales, en términos generales son: requisitos de sistemas no documentados, inexistencia de un control de cambios, procesos no definidos en la empresa. En base a esas carencias se diseñaron e implementaron las mejoras necesarias y factibles para mejorar el nivel de seguridad de la información en el proceso en estudio obteniendo como resultado una mejora significativa al alcanzar un 81.80%.
5. Para el desarrollo de cada una de las propuestas de mejora se propusieron: manuales, formatos, diagramas para una correcta operación de los procesos. Estos procesos se desarrollaron de forma iterativa con el Gerente de Operaciones.

RECOMENDACIONES

1. Se requiere el compromiso de todo el personal de BITNESS CORP. S.A.C. para continuar con el cumplimiento de los procesos y utilización de los documentos implementados con la finalidad de lograr un mejor nivel de seguridad y asi alcanzar el nivel de calificación Completamente Logrado.
2. Se recomienda seguir con las capacitaciones brindadas al personal, en temas relacionados a la seguridad de la información para una óptima gestión en la empresa BITNESS CORP. S.A.C.
3. El documento de requisitos no funcionales y el documento de requisitos funcionales durante el proceso de desarrollo, constituyen un elemento fundamental para el desarrollo de un sistema. La especificación de requisitos, es crítica para asegurar que el futuro sistema, satisfaga efectivamente las necesidades del cliente. Sin embargo, obtener un conjunto de requisitos de calidad, es una tarea compleja y demanda tiempo. Por lo tanto, si se inicia el desarrollo de un proyecto, a partir de requisitos que ya hayan sido

especificados para proyectos similares o en similares negocios, existe mayor tiempo y probabilidad de mejorar la calidad y completitud de los requisitos para el nuevo sistema.

4. Para garantizar el cumplimiento de las oportunidades de mejora se recomienda a la empresa BITNESS CORP. S.A.C. realizar evaluaciones al equipo de desarrollo que permitan saber si se realizan los procesos de acuerdo a lo establecido.

REFERENCIAS

[1] Gavidia y Torres, «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», *Univ. Peru. Unión*, p. 250, 2018.

[2] KASPERSKY, «Boletín de seguridad», *KASPERSKY*, 2019.

[3] ESET, «ESET SECURITY REPORT Latinoamerica 2019», *ESET*, 2019.

[4] B. Bermúdez, «Análisis en seguridad informática y seguridad de la información basado en la Norma ISO/IEC 27001- sistemas de gestión de deguridad de la información dirigido a una Empresa de Servicios Financieros.», *Univ. Politénica Sales.*, p. 180, 2015.

[5] Guzmán, «Metodología para la seguridad de tecnologías de información y comunicaciones en la Clínica Ortega», *Univ. Nac. del Cent. del Perú*, p. 139, 2015.

[6] Contero, «Diseño de una política de seguridad de la información basada en la Norma ISO 27002:2013, para el sistema de botones de seguridad del Ministerio del Interior», *Univ. Int. SEK Ser Mejor.*, vol. 22, pp. 1-8, 2019.

[7] Sota; Mechan, «Implementación de controles y cumplimiento de requisitos de la ISO / IEC 27001 : 2013 para la seguridad», *Univ. San Martin Porres*, 2018.

[8] Romo y Valarezo, «Analisis e implementacio de la norma ISO 27002 para el departamento de sistemas de la Universidad Politecnica Salesiana sede Guayaquil», *Univ. Politénica Sales.*, p. 183, 2012.

[9] Huacanés, «Implementación de la norma ISO-IEC 27002:2013, sección "Control de acceso" para las aplicaciones informáticas de la Aseguradora del Sur», *Univ. las Américas*, 2016.

[10] García y Salas, «Análisis e Implementación de la seguridad de la información del centro de datos de la Universidad Nacional de la Amazonía Peruana bajo la NORMA ISO 27002.», *Univ. Nac. la Amaz. Peru.*, vol. 53, n.º 9, pp. 1689-1699, 2017.

[11] INCIBE, *Gestión de Riesgos*. 2015.

[12] CCC, «Manual de seguridad de la información», *Cámara Comer. Calí*, pp. 1-36, 2016.

[13] MinTIC, «Controles de Seguridad y Privacidad de la Información», *Minist. Tecnol. la iIformción y las Comun. Colomb.*, n.º 8, p. 18, 2016.

[14] Frayssinet, «Taller de Implementación de la norma ISO 27001», *Of. Nac. Gob.*

Electrónico e Informática, p. 97, 2011.

[15] Fuentes, «Auditoria al sistema de gestion de la seguridad de la información del proceso de gestión de incidentes de clientes de ANS comunicaciones, con base en la norma técnica colombiana NTC-ISO/IEC 27002», 2019.

[16] OSRI, «Metodología para la gestión de la seguridad informática», *Of. Segur. para las Redes Informaticas*, pp. 1-68, 2018.

[17] Barzanallana, «Introducción a la Seguridad Informática», *Apl. Criptográficas Java*, p. 361, 2016.

[18] Vanegas, «Seguridad para minimizar riesgos en el desarrollo del software», *Univ. Pilot. Colomb.*, pp. 1-7, 2015.

[19] B. Silega, «Requisitos de Seguridad para aplicaciones web», *Rev. Cuba. Ciencias Informáticas*, vol. 12, pp. 205-221, 2018.

[20] Brito, «Metodologías para desarrollar software seguro», *ReCIBE. Rev. electrónica Comput. Informática, Biomédica y Electrónica*, vol. 2, n.º 3, p. V, 2013.

[21] Ochoa, «Seguridad del software y criterios de evaluación», *Univ. San Carlos Guatemala*, n.º 1, pp. 147-173, 2003.

[22] Hernández, «Seguridad y privacidad en los sistemas informáticos», pp. 1-9, 1999.

[23] ISO/IEC, «Calidad del producto software», *ISO/IEC 25000*, pp. 30-35, 2013.

[24] Montero, «El concepto de seguridad en el nuevo paradigma de la normatividad mexicana», *Tecnológico de Monterrey*, vol. 25, n.º 58, 2013.

[25] Thompson, «Definición de Información», *Defin. Inf.*, p. 3, 2008.

[26] Cerón, «Hadware y Software», *Univ. Autónoma del Estado Hidalgo*, 2014.

[27] Feito, «Vulnerabilidad», *Univ. Rey Juan Carlos*, vol. 28, n.º 3, pp. viii-xi, 2017.

[28] Castro y Rojas, «Riesgos, Amenazas y Vulnerabilidades de los sistemas de información geográfica», 2013.

[29] Oliván, «Guía de controles de ciberseguridad para la protección integral de la pyme», *Máster Interuniv. en Segur. las Tecnol. la Inf. y las Comun. MISTIC*, 2017.

[30] Barbosa, Cano, Gonzalez, y Jurado, «Politica de Seguridad», *Univ. Virtual Int.*, 2013.

[31] González, Gómez, y Domínguez, «Los servicios: concepto, clasificación y problemas de medición», *Ekon. Rev. vasca Econ.*, n.º 13, pp. 10-19, 1989.

[32] Sain, «¿ Qué es la seguridad Informática?», *Security*, n.º 2018, pp. 5-5, 2018.

[33] Berzal, «El ciclo de vida de un sistema de información».

[34] Guiral; Lapiedra; Devece, *Introducción a la gestión de sistemas de información en la empresa*. 2011.

[35] Gonzalez, «Documentación de los procesos misionales de un sistema de gestión de la calidad basado en los requisitos de la norma ISO 9001:2015 en una empresa del sector tecnologia», *Fund. Univ. América*, 2017.

[36] S. de G. Pública, «Metodología para la implementación de la gestión por procesos en las entidades de la administración pública.», vol. 1, n.º 2, pp. 1-43, 2013.

[37] Hernández, *Metodologia de la investigación*. 2014.

[38] Otero, «Enfoques de investigación», *Univ. del Atlántico*, n.º August, 2018.

ANEXOS

Anexo 1.Instrumento de evaluación

UNIVERSIDAD PERUANA UNIÓN
FACULTAD DE INGENIERÍA Y ARQUITECTURA
EP INGENIERÍA DE SISTEMAS

INSTRUMENTO DE EVALUACIÓN DE LOS CONTROLES DE SEGURIDAD EN EL PROCESO DE DESARROLLO

INTRODUCCIÓN

El presente documento tiene como objetivo medir los controles de seguridad en el proceso de desarrollo de sistemas de información de la empresa BITNESS CORP S.A.C. Las preguntas se elaboraron en función al dominio 14 de la ISO 27002:2015.

Dominio 14: Adquisición, desarrollo y mantenimiento de los sistemas de información					
14.1 Requisitos de seguridad de sistemas de información					
14.1.1 Análisis de requisitos y especificaciones de seguridad de información					
N°	**PREGUNTA**	**NL 0– 20%**	**PL 21 – 49%**	**AL 50– 79%**	**CL 80 – 100%**
1.	La empresa BITNESS CORP. S.A.C. tiene requisitos de seguridad de información identificados para el desarrollo de sistemas de información?				
2.	¿Utilizan o aplican algún método para la identificación de requisitos de seguridad para el desarrollo de un sistema de información en BITNESS CORP S. A.C?				
3.	¿Los requisitos de seguridad identificados para el desarrollo de sistemas han sido documentados por todas las partes interesadas en BITNESS CORP S.A.C.?				
4.	¿Los requisitos de seguridad identificados para el desarrollo de sistemas han sido revisados por todas las partes interesadas en BITNESS CORP S.A.C.?				
5.	¿Los requisitos y controles de seguridad de la información recibidos para el desarrollo de aplicaciones o sistemas reciben un nivel adecuado de protección de acuerdo a su importancia en la organización?				
6.	¿Los requisitos de seguridad de la información y los procesos asociados se integran desde las primeras etapas del proyecto de sistemas de información?				
7.	¿Los requisitos de la seguridad de la información consideran el nivel de confianza de la identidad declarada por los usuarios para obtener los requisitos de autentificación?				
8.	¿Los requisitos de la seguridad de la información consideran la aprobación y autorización de acceso para los usuarios(usuarios de negocio, usuarios con privilegios o usuarios técnicos)?				
9.	¿Los requisitos de la seguridad de la información consideran la información de los usuarios privilegiados y técnicos respecto a sus deberes y responsabilidades en BITNESS CORP S.A.C.?				
10.	¿Los requisitos de la seguridad de la información consideran la protección requerida para los activos en base a la disponibilidad, confidencialidad e integridad(análisis de riesgos) en BITNESS CORP S.A.C.?				
11.	¿Los requisitos de la seguridad de la información consideran los procesos de negocio (registro de transacciones, supervisión y monitoreo, requisitos de no repudio entre otros) en BITNESS CORP S.A.C.?				
12.	¿La empresa BITNESS CORP S.A.C. consideran los requisitos impuestos por otros controles de seguridad como interfaces para el registro, monitorización sistemas, detección de fugas de datos entre otros?				

13.	¿La empresa BITNESS CORP. S.A.C ofrece seguridad para evitar actividades fraudulentas a aquellas empresas que solicitan sistemas de información que contengan datos sensibles como transacciones?				
14.	¿Existe un proceso de pruebas y adquisición formal para la adquisición de productos en BITNESS CORP S.A.C.?				
15.	¿Los contratos con los proveedores de productos o servicios cumplen con los requisitos de seguridad identificados en BITNESS CORP S.A.C.?				
16.	¿Se consideran los riesgos que se introducen al adquirir un producto o servicio que no satisface los requisitos especificados en BITNESS CORP S.A.C.?				
17.	¿Se evalúan o implementan las guías disponibles para la configuración de seguridad del producto adquirido alineado con el software y los servicios finales en BITNESS CORP S.A.C.?				
18.	¿Se han definido criterios de aceptación para la adquisición de productos respecto a su funcionalidad para asegurar el cumplimiento de los requisitos de seguridad identificados en BITNESS CORP S.A.C.?				
19.	¿Para la adquisición de un producto o servicios se realizan evaluaciones de acuerdo a los criterios de aceptación definidos en BITNESS CORP. S.A.C.?				
20.	¿Las funciones adicionales de los productos o servicios adquiridos son revisadas para asegurar que no presenten nuevos riesgos inaceptables en BITNESS CORP S.A.C.?				
14.2 Seguridad en el desarrollo y en los procesos de soporte					
14.2.1 Política de desarrollo seguro					
N°	**PREGUNTA**	**NL 0– 20%**	**PL 21 – 49%**	**AL 50 – 79%**	**CL 80 – 100%**
1.	¿La empresa BITNESS CORP. S.A.C. tiene establecido reglas dentro de la organización para el desarrollo de aplicaciones y sistemas?				
2.	¿La empresa BITNESS CORP. S.A.C. aplica políticas de desarrollo seguro en el entorno de desarrollo (personas, proceso y tecnología)?				
3..	¿ La empresa BITNESS CORP. S.A.C.aplica políticas de desarrollo seguro en el ciclo de vida de desarrollo de software?				
4.	¿ La empresa BITNESS CORP. S.A.C. cuenta con una metodología de desarrollo del software?				
5.	¿ La empresa BITNESS CORP. S.A.C.aplica políticas de desarrollo seguro en la metodología de desarrollo del software?				
6.	¿La empresa BITNESS CORP. S.A.C. aplica guías de desarrollo seguro para cada lenguaje de programación utilizado.?				
7.	¿La política de desarrollo seguro en BITNESS CORP. S.A.C considera requisitos de seguridad en la fase de diseño?				
8.	¿La política de desarrollo seguro en BITNESS CORP. S.A.C consideran puntos de verificación en los hitos del proyecto (Entregables o indicadores de progreso)?				
9.	¿La política de desarrollo seguro en BITNESS CORP. S.A.C consideran los repositorios seguros?				
10.	¿La política de desarrollo seguro en BITNESS CORP. S.A.C.considera el control de versiones ?				
11.	¿La política de desarrollo seguro en BITNESS CORP. S.A.C. considera el conocimiento sobre seguridad de aplicaciones.?				
12.	¿La política de desarrollo seguro considera la capacidad de los desarrolladores de evitar, encontrar y reparar vulnerabilidades en BITNESS CORP. S.A.C.?				
13.	¿La empresa BITNESS CORP. S.A.C. utiliza técnicas de programación segura.(para los nuevos desarrollos o situaciones de reutilización de códigos)?				
14	¿La empresa BITNESS CORP. S.A.C. considera las indicaciones correspondientes para el uso de las técnicas de programación segura?				
15.	¿Los desarrolladores están formados en el uso de las técnicas de programación segura ?				
16.	La empresa BITNESS CORP. S.A.C exige que la parte externa (desarrolladores externos) cumplan con las normas de desarrollo seguro?				
14.2.2 Procedimientos de control de cambios en sistemas					
N°	**PREGUNTA**	**NL 0– 20%**	**PL 21 – 49%**	**AL 50 – 79%**	**CL 80 – 100%**

1.	¿La empresa BITNESS CORP. S.A.C realiza el control de cambios mediante el uso de procedimientos formales durante el ciclo de vida del desarrollo de software?				
2.	¿En la empresa BITNESS CORP. S.A.C se han documentado los procedimientos formales de control de cambios?				
3.	¿La empresa BITNESS CORP. S.A.C. cumple los procedimientos formales de control de cambios?				
4.	¿La incorporación de sistemas nuevos y cambios importantes sigue un proceso formal de documentación, especificaciones, pruebas, control de calidad y gestión de implantación?				
5.	¿Para el proceso de control de cambios se incluye una evaluación de riesgos?				
6.	¿El proceso de control de cambios asegura que los procedimientos de seguridad y controles existentes no sean accesibles a los programadores de apoyo y que estos accedan a las partes necesarias de su trabajo?				
7.	Los procedimientos de control de cambios deberían incluir, pero no limitarse a: a) el mantenimiento de un registro de los niveles de autorización aprobados;				
8	¿El procedimiento de control de cambios asegura que los cambios son enviados a los usuarios autorizados?				
9.	¿Los procedimiento de control de cambios deben incluir la revisión de los controles y procedimientos de integridad asegurando que estos no se vean comprometidos por los cambios?				
10.	¿El procedimiento de control de cambios incluye la identificación de todo el software,la información, las entidades de base de datos y el hardware que requiere cambios?				
11.	¿El procedimiento de control de cambios incluye la identificación y comprobación de la seguridad del código crítico?				
12.	¿El procedimiento de control de cambios incluye la aprobación formal de las propuestas detalladas antes de que comience el trabajo?				
13.	¿El procedimiento de control de cambios incluye la aceptación de los cambios de los usuarios autorizados antes de su implementación?				
14.	¿El procedimiento de control de cambios actualiza la documentación del sistema al finalizar cada cambio y elimina la documentación obsoleta?				
15.	¿El procedimiento de control de cambios incluye el mantenimiento de un control de versiones para las actuaciones del software?				
16.	¿El procedimiento de control de cambios incluye el mantenimiento de registros de auditoría de las solicitudes de cambio?				
17.	¿El procedimiento de control de cambios incluye la implantación de los cambios en el momento adecuado sin perturbar los procesos de negocio involucrados?				

14.2.6 Entorno de desarrollo seguro

N°	PREGUNTA	NL 0– 20%	PL 21 – 49%	AL 50 – 79%	CL 80 – 100%
1.	¿Las personas que forman parte del equipo de desarrollo cumplen con los requisitos de seguridad establecidos?				
2.	¿Los procesos de cada etapa de desarrollo cumplen con los requisitos de seguridad establecidos?				
3.	¿Las tecnologías(computadoras, servidores, software, código) que se usan para el desarrollo de sistemas cumplen con los requisitos de seguridad establecidos?				
4.	¿Los requisitos funcionales(datos de entrada) que ingresan como información están protegidos(como por ejemplo en un repositorio)?				
5.	¿Los datos procesados están almacenados en dispositivos seguros?				
6.	¿La empresa BITNESS CORP. S.A.C realiza copias de seguridad de los datos procesados?				
7.	¿La empresa BITNESS CORP. S.A.C transmite la información de manera protegida(mediante correos electrónicos, usb,archivos compartidos, entre otros)?				
8.	¿La empresa BITNESS CORP. S.A.C aplica los requisitos de seguridad externos e internos?				
9.	¿Los controles de seguridad de la organización apoyan el desarrollo del sistema?				
10.	¿El personal de BITNESS CORP. S.A.C. cumple con los requisitos de seguridad(no realizan copias indebidas, no sacan la información fuera del entorno de desarrollo)?				

11.	¿Existe algún documento de confidencialidad para la contratación de personal externo?				
12.	¿Existen sanciones en caso de no cumplir el contrato de confidencialidad?				
13.	¿La empresa BITNESS CORP. S.A.C. segrega la información cuidadosamente de acuerdo al trabajo que ejerce cada personal?				
14.	¿La empresa BITNESS CORP. S.A.C. maneja un control de acceso físico(ambiente de trabajo, oficinas)?				
15.	¿La empresa BITNESS CORP. S.A.C. maneja un control de acceso lógico(acceso a los servidores, acceso a cuentas de usuario)?				
16.	¿La empresa BITNESS CORP. S.A.C. realiza la monitorización de los cambios en el producto?				
17.	¿La empresa BITNESS CORP. S.A.C. realiza la monitorización de los cambios durante el proceso de desarrollo(código)?				
18.	¿La empresa BITNESS CORP. S.A.C. realiza copias de seguridad fuera de las instalaciones?				
19	¿La empresa BITNESS CORP. S.A.C. almacena de manera segura sus copias de respaldo?				
20.	¿La empresa BITNESS CORP. S.A.C. tiene identificado al personal que accede a las copias de respaldo?				
21.	¿La empresa BITNESS CORP. S.A.C realiza una gestión adecuada para la presentación de avances(entregables)?				
22.	¿La empresa BITNESS CORP. S.A.C cumple con las medidas de seguridad para la presentación de avances(entregables)?				
14.2.8 Pruebas funcionales de seguridad de sistemas		**100%**			
N°	**PREGUNTA**	**NL 0– 20%**	**PL 21 – 49%**	**AL 50 – 79%**	**CL 80 – 100%**
1.	¿Realizan pruebas y verificaciones exhaustivas en el proceso de desarrollo de sistemas nuevos y los actualizados.?				
2.	¿Las pruebas y verificaciones exhaustivas son realizadas por el equipo de desarrollo?				
3.	¿Se realizan pruebas de aceptación independientes(para desarrollos internos y desarrollos externalizados)?				
14.2.9 Pruebas de aceptación de sistemas					
N°	**PREGUNTA**	**NL 0– 20%**	**PL 21 – 49%**	**AL 50 – 79%**	**CL 80 – 100%**
1.	¿La empresa BITNESS CORP. S.A.C. establece programas de pruebas de aceptación?				
2.	¿Las pruebas de aceptación del sistema incluyen las pruebas de los requisitos de seguridad de la información?				
3.	¿Las pruebas de aceptación del sistema incluyen las prácticas de desarrollo seguro del sistema?				
4.	¿Se realizan pruebas a los componentes recibidos?				
5.	¿La empresa BITNESS CORP. S.A.C. utiliza herramientas automatizadas(herramientas de análisis de código o los escáneres de vulnerabilidad) para la seguridad?				
6.	¿La empresa BITNESS CORP. S.A.C. realiza pruebas realistas que eviten la introducción de vulnerabilidades en la organización?				
14.3.1 Protección de los datos de prueba					
N°	**PREGUNTA**	**NL 0– 20%**	**PL 20 – 49%**	**AL 50 – 79%**	**CL 80 – 100%**
1.	¿En la empresa BITNESS CORP. S.A.C. evita el uso de datos reales o la información confidencial para las pruebas?				
2.	¿En caso la empresa BITNESS CORP. S.A.C use datos o información confidencial está es protegia mediante su retirada o modificación?				

3.	¿Los procedimientos de control de acceso de BITNESS CORP. S.A.C se aplican a las sistema de pruebas?				
4.	¿La empresa BITNESS CORP. S.A.C realiza un control de acceso cada vez que la información de operación se copia a un entorno de prueba?				
5.	¿En la empresa BITNESS CORP. S.A.C la copia y uso de información operacional es registrada para futuras auditorias?				

Anexo 2.Carta de Presentación

Lima, 14 de Junio del 2020

Señor

Presente.

Asunto: VALIDACIÓN DE INSTRUMENTO DE EVALUACIÓN POR JUICIO DE EXPERTOS

Nos es muy grato dirigimos a usted para expresarle nuestros saludos y así mismo hacer de su conocimiento que somos bachilleres en Ingeniería de Sistemas egresadas de la Universidad Peruana Unión, y a la vez manifestarle que, conocedores de su trayectoria académica y profesional, solicitamos su atención al elegirlo como JUEZ EXPERTO para revisar el contenido del instrumento que pretendemos utilizar en la Investigación que estamos realizando para optar el título profesional de Ingenieros de Sistemas.

El título de la investigación es "Seguridad en el desarrollo de sistemas según la ISO 27002 2015 en la empresa BITNESS CORP S.A.C" y el objetivo del instrumento es medir la variable que determina el nivel de seguridad de la información en el proceso de desarrollo de sistemas en la empresa BITNESS CORP S.A.C.

Con la finalidad de determinar la validez de su contenido, solicitamos utilizar el Formato de Validación de Instrumento de Evaluación por Juicio de Expertos adjunto, de acuerdo a su amplia experiencia y conocimientos.

Agradecemos anticipadamente su colaboración y estamos seguros que su opinión y criterio de experto servirán para los fines propuestos.

Atentamente,

P.D. Adjuntamos el Instrumento de Evaluación.

Bach. Gaby M. Alvarado L.

Bach. Miryam R. Sánchez T

Anexo 3.Validación del instrumento de evaluación por juicio de experto

UNIVERSIDAD PERUANA UNIÓN
FACULTAD DE INGENIERÍA Y ARQUITECTURA
EP INGENIERÍA DE SISTEMAS

FORMATO DE VALIDACIÓN DE INSTRUMENTO DE EVALUACIÓN POR JUICIO DE EXPERTOS

I. DATOS DEL EXPERTO

I.1. Apellidos y nombres: _____

I.2. Grado Académico: ( ) Bachiller, ( ) Maestro/Magíster ( ) Doctor

I.3. Profesión: _____

I.4. Institución donde labora: _____

I.5. Cargo que desempeña: _____

II. DATOS DEL TEMA DE INVESTIGACIÓN

II.1. Titulo de la investigación

"Seguridad en el desarrollo de sistemas según la ISO 27002 2015 en la empresa BITNESS CORP S.A.C"

II.2.Objetivo de la investigación

Determinar la mejora de la seguridad de la información en el proceso de desarrollo de sistemas con la implementación de controles de seguridad de la ISO 27002:2015 en la empresa BITNESS CORP. S.A.C., 2020.

II.3.Variable:

VARIABLES	DEFINICIÓN
Controles de Seguridad del dominio 14 de la ISO 27002:2015	Basados en la ISO 27002:2015.
Seguridad de la Información en el proceso de desarrollo de sistemas	Seguridad en las Etapas del proceso de desarrollo de un sistema y seguridad en el producto(sistema).

III. INSTRUMENTO DE VALIDACIÓN

Instrucciones:

Determinar si el instrumento de evaluación para la investigación descrita reúne las características adecuadas y pertinente, indicando el nivel alcanzado en los Criterios de Evaluación del Instrumentos: Excelente, Muy bueno, Bueno, Regular o Deficiente. Coloque un aspa (X) en el casillero correspondiente.

CRITERIOS DE EVALUACIÓN DEL INSTRUMENTO			NIVELES DE EVALUACIÓN				
N°	INDICADOR	DESCRIPCIÓN	Excelente 5	Muy bueno 4	Bueno 3	Regular 2	Deficiente 1
1	CLARIDAD	Están formulados con lenguaje apropiado que facilita su comprensión					
2	OBJETIVIDAD	Están expresados en términos observables, medibles					
3	CONSISTENCIA	Existe una organización lógica en los contenidos en relación con la teoría					
4	COHERENCIA	Existe relación de los contenidos con los indicadores de la variable					
5	PERTINENCIA	Las categorías de respuestas y sus valores son apropiados					
6	SUFICIENCIA	Son suficientes la cantidad y calidad de ítems presentados en el instrumento					
		SUMATORIA PARCIAL					
		SUMATORIA TOTAL					

(Sumatoria total entre: 20 y 30 = Favorable, 10 y 19 = Debe mejorar, 1 y 9 = No favorable)

IV. RESULTADOS DE LA VALIDACIÓN

Valoración total cuantitativa: _____

Opinión: ( ) Favorable( ) Debe mejorar ( ) No favorable

Observaciones:

_____

Firma

Anexo 4.Validación del Instrumento de Evaluación por el Ing. Jenson Chambi

UNIVERSIDAD PERUANA UNIÓN
FACULTAD DE INGENIERÍA Y ARQUITECTURA
EP INGENIERÍA DE SISTEMAS

FORMATO DE VALIDACIÓN DE INSTRUMENTO DE EVALUACIÓN POR JUICIO DE EXPERTOS

I. DATOS DEL EXPERTO

I.1. Apellidos y nombres: **Chambi Aguilar Jenson Daniel**

I.2. Grado Académico: (X) Bachiller, ( ) Maestro/Magister ( ) Doctor **I.3.** Profesión:

Ingeniero de Sistemas

I.4. Institución donde labora: Universidad Peruana Unión

I.5. Cargo que desempeña: Desarrollador, Analista, Docente

II. DATOS DEL TEMA DE INVESTIGACIÓN

II.1. Titulo de la investigación

"Seguridad en el desarrollo de sistemas según la ISO 27002 2015 en la empresa BITNESS CORP S.A.C"

II.2.Objetivo de la investigación

Determinar la mejora de la seguridad de la información en el proceso de desarrollo de sistemas con la implementación de controles de seguridad de la ISO 27002:2015 en la empresa BITNESS CORP. S.A.C., 2020.

II.3.Variable:

VARIABLES	DEFINICIÓN
Controles de Seguridad del dominio 14 de la ISO 27002:2015	Basados en la ISO 27002:2015.
Seguridad de la Información en el proceso de desarrollo de sistemas	Seguridad en las Etapas del proceso de desarrollo de un sistema y seguridad en el producto(sistema).

III. INSTRUMENTO DE VALIDACIÓN

Instrucciones:

Determinar si el instrumento de evaluación para la investigación descrita reúne las características adecuadas y pertinente, indicando el nivel alcanzado en los Criterios de Evaluación del Instrumentos: Excelente, Muy bueno, Bueno, Regular o Deficiente. Coloque un aspa (X) en el casillero correspondiente.

CRITERIOS DE EVALUACIÓN DEL INSTRUMENTO			NIVELES DE EVALUACIÓN				
N°	INDICADOR	DESCRIPCIÓN	Excelente 5	Muy bueno 4	Bueno 3	Regular 2	Deficiente 1
1	CLARIDAD	Están formulados con lenguaje apropiado que facilita su comprensión	X				
2	OBJETIVIDAD	Están expresados en términos observables, medibles		X			
3	CONSISTENCIA	Existe una organización lógica en los contenidos en relación con la teoría	X				
4	COHERENCIA	Existe relación de los contenidos con los indicadores de la variable	X				
5	PERTINENCIA	Las categorías de respuestas y sus valores son apropiados	X				
6	SUFICIENCIA	Son suficientes la cantidad y calidad de ítems presentados en el instrumento	X				
		SUMATORIA PARCIAL	25	4			
		SUMATORIA TOTAL	29				

(Sumatoria total entre: 20 y 30 = Favorable, 10 y 19 = Debe mejorar, 1 y 9 = No favorable)

IV. RESULTADOS DE LA VALIDACIÓN

Valoración total cuantitativa: Veintinueve

Opinión: (X) Favorable ( ) Debe mejorar ( ) No favorable

Observaciones:

Firma

Anexo 5. Validación del Instrumento de Evaluación por el Ing. Sergio Valladares

UNIVERSIDAD PERUANA UNIÓN
FACULTAD DE INGENIERÍA Y ARQUITECTURA
EP INGENIERÍA DE SISTEMAS

FORMATO DE VALIDACIÓN DE INSTRUMENTO DE EVALUACIÓN POR JUICIO DE EXPERTOS

I. DATOS DEL EXPERTO Valladares Castillo Sergio

I.1. Apellidos y nombres: _____

I.2. Grado Académico: ( ) Bachiller, (X) Maestro/Magíster ( ) Doctor

I.3. Profesión: Ingeniería de Sistemas

I.4. Institución donde labora: UPeU

I.5. Cargo que desempeña: Docente

II. DATOS DEL TEMA DE INVESTIGACIÓN

II.1. Titulo de la investigación

"Seguridad en el desarrollo de sistemas según la ISO 27002 2015 en la empresa BITNESS CORP S.A.C"

II.2.Objetivo de la investigación

Determinar la mejora de la seguridad de la información en el proceso de desarrollo de sistemas con la implementación de controles de seguridad de la ISO 27002:2015 en la empresa BITNESS CORP. S.A.C., 2020.

II.3.Variable:

VARIABLES	DEFINICIÓN
Controles de Seguridad del dominio 14 de la ISO 27002:2015	Basados en la ISO 27002:2015.
Seguridad de la Información en el proceso de desarrollo de sistemas	Seguridad en las Etapas del proceso de desarrollo de un sistema y seguridad en el producto(sistema).

III. INSTRUMENTO DE VALIDACIÓN

Instrucciones:

Determinar si el instrumento de evaluación para la investigación descrita reúne las características adecuadas y pertinente, indicando el nivel alcanzado en los Criterios de Evaluación del Instrumentos: Excelente, Muy bueno, Bueno, Regular o Deficiente. Coloque un aspa (X) en el casillero correspondiente.

CRITERIOS DE EVALUACIÓN DEL INSTRUMENTO			NIVELES DE EVALUACIÓN				
N°	INDICADOR	DESCRIPCIÓN	Excelente 5	Muy bueno 4	Bueno 3	Regular 2	Deficiente 1
1	CLARIDAD	Están formulados con lenguaje apropiado que facilita su comprensión	X				
2	OBJETIVIDAD	Están expresados en términos observables, medibles	X				
3	CONSISTENCIA	Existe una organización lógica en los contenidos en relación con la teoría	X				
4	COHERENCIA	Existe relación de los contenidos con los indicadores de la variable	X				
5	PERTINENCIA	Las categorías de respuestas y sus valores son apropiados	X				
6	SUFICIENCIA	Son suficientes la cantidad y calidad de ítems presentados en el instrumento	X				
		SUMATORIA PARCIAL					
		SUMATORIA TOTAL	30				

(Sumatoria total entre: 20 y 30 = Favorable, 10 y 19 = Debe mejorar, 1 y 9 = No favorable)

IV. RESULTADOS DE LA VALIDACIÓN

Valoración total cuantitativa: 30

Opinión: (X) Favorable( ) Debe mejorar ( ) No favorable

Observaciones:

_____

_____

_____

Firma

Anexo 6. Instrumento de Evaluación Aplicado

UNIVERSIDAD PERUANA UNIÓN
FACULTAD DE INGENIERÍA Y ARQUITECTURA
EP INGENIERÍA DE SISTEMAS

INSTRUMENTO DE EVALUACIÓN DE LOS CONTROLES DE SEGURIDAD EN EL PROCESO DE DESARROLLO

INTRODUCCIÓN

El presente documento tiene como objetivo medir los controles de seguridad en el proceso de desarrollo de sistemas de información de la empresa BITNESS CORP S.A.C. Las preguntas se elaboraron en función al dominio 14 de la ISO 27002:2015.

	PESO	ACUMULADO	LOGRADO	LO QUE FALTA LOGRAR
14.1.1.Análisis de requisitos y especificaciones de seguridad de información	25%	33.00%	8.25%	16.75%
14.2.1. Política de desarrollo seguro	15%	46.25%	6.94%	8.06%
14.2.2. Procedimientos de control de cambios en sistemas	20%	51.76%	10.35%	9.65%a
14.2.6.Entorno de desarrollo seguro	25%	62.73%	15.68%	9.32%
14.2.8. Pruebas funcionales de seguridad de sistemas	5%	66.67%	3.33%	1.67%
14.2.9. Pruebas de aceptación de sistemas	5%	40.00%	2.00%	3.00%
14.3.1. Protección de los datos de prueba	5%	48.00%	2.40%	2.60%
TOTAL	100%		48.96%	51.04%

ANÁLISIS DE PORCENTAJE

PORCENTAJE	DESCRIPCIÓN DEL PORCENTAJE
0%	No posee ninguna evidencia y manifiesta desconocimiento de ello.
20%	Tiene conocimiento de ello y lo practica a criterio personal.
40%	Tiene conocimiento de ello y se capacita para ponerlo en práctica.(Lo maneja en un nivel básico, muy general).

60%	Cumplimiento parcial del control sin generar evidencia alguna.
80%	Cumplimiento del control pero sin generar evidencia.
100%	Posee evidencia del cumplimiento del control y tiene un amplio conocimiento sobre ello.

Dominio 14: Adquisición, desarrollo y mantenimiento de los sistemas de información					
14.1 Requisitos de seguridad de sistemas de información					
14.1.1 Análisis de requisitos y especificaciones de seguridad de información					
N°	**PREGUNTA**	**NL 0 – 20%**	**PL 21 – 49%**	**AL 50– 79%**	**CL 80 – 100%**
1.	La empresa BITNESS CORP. S.A.C. tiene requisitos de seguridad de información identificados para el desarrollo de sistemas de información?		X40%		
2.	¿Utilizan o aplican algún método para la identificación de requisitos de seguridad para el desarrollo de un sistema de información en BITNESS CORP S. A.C?	X 0%			
3.	¿Los requisitos de seguridad identificados para el desarrollo de sistemas han sido documentados por todas las partes interesadas en BITNESS CORP S.A.C.?	X0%			
4.	¿Los requisitos de seguridad identificados para el desarrollo de sistemas han sido revisados por todas las partes interesadas en BITNESS CORP S.A.C.?	X0%			
5.	¿Los requisitos y controles de seguridad de la información recibidos para el desarrollo de aplicaciones o sistemas reciben un nivel adecuado de protección de acuerdo a su importancia en la organización?			X60%	
6.	¿Los requisitos de seguridad de la información y los procesos asociados se integran desde las primeras etapas del proyecto de sistemas de información?				X80%
7.	¿Los requisitos de la seguridad de la información consideran el nivel de confianza de la identidad declarada por los usuarios para obtener los requisitos de autentificación?				X80%
8.	¿Los requisitos de la seguridad de la información consideran la aprobación y autorización de acceso para los usuarios(usuarios de negocio, usuarios con privilegios o usuarios técnicos)?				X 80%
9.	¿Los requisitos de la seguridad de la información consideran la información de los usuarios privilegiados y técnicos respecto a sus deberes y responsabilidades en BITNESS CORP S.A.C.?			X 60%	
10.	¿Los requisitos de la seguridad de la información consideran la protección requerida para los activos en base a la disponibilidad, confidencialidad e integridad(análisis de riesgos) en BITNESS CORP S.A.C.?	X20%			
11.	¿Los requisitos de la seguridad de la información consideran los procesos de negocio (registro de transacciones, supervisión y monitoreo, requisitos de no repudio entre otros) en BITNESS CORP S.A.C.?				X100%
12.	¿La empresa BITNESS CORP S.A.C. consideran los requisitos impuestos por otros controles de seguridad como interfaces para el registro, monitorización sistemas, detección de fugas de datos entre otros?	X0%			
13.	¿La empresa BITNESS CORP. S.A.C ofrece seguridad para evitar actividades fraudulentas a aquellas empresas que solicitan sistemas de información que contengan datos sensibles como transacciones?	X0%			
14.	¿Existe un proceso de pruebas y adquisición formal para la adquisición de productos en BITNESS CORP S.A.C.?	x0%			
15.	¿Los contratos con los proveedores de productos o servicios cumplen con los requisitos de seguridad identificados en BITNESS CORP S.A.C.?		x40%		
16.	¿Se consideran los riesgos que se introducen al adquirir un producto o servicio que no satisface los requisitos especificados en BITNESS CORP S.A.C.?		x40%		
17.	¿Se evalúan o implementan las guías disponibles para la configuración de seguridad del producto adquirido alineado con el software y los servicios finales en BITNESS CORP S.A.C.?	x0%			

18.	¿Se han definido criterios de aceptación para la adquisición de productos respecto a su funcionalidad para asegurar el cumplimiento de los requisitos de seguridad identificados en BITNESS CORP S.A.C.?	X0%			
19.	¿Para la adquisición de un producto o servicios se realizan evaluaciones de acuerdo a los criterios de aceptación definidos en BITNESS CORP. S.A.C.?	x0%			
20.	¿Las funciones adicionales de los productos o servicios adquiridos son revisadas para asegurar que no presenten nuevos riesgos inaceptables en BITNESS CORP S.A.C.?			x60%	
SUMA TOTAL = 660 PORCENTAJE= 660/20=33%		20	120	180	340
14.2 Seguridad en el desarrollo y en los procesos de soporte					
14.2.1 Política de desarrollo seguro					
N°	**PREGUNTA**	**NL 0 – 20%**	**PL 21 – 49%**	**AL 50– 79%**	**CL 80 – 100%**
1.	¿La empresa BITNESS CORP. S.A.C. tiene establecido reglas dentro de la organización para el desarrollo de aplicaciones y sistemas?		X40%		
2.	¿La empresa BITNESS CORP. S.A.C. aplica políticas de desarrollo seguro en el entorno de desarrollo (personas, proceso y tecnología)?		x40%		
3..	¿ La empresa BITNESS CORP. S.A.C. aplica políticas de desarrollo seguro en el ciclo de vida de desarrollo de software?		x40%		
4.	¿ La empresa BITNESS CORP. S.A.C. cuenta con una metodología de desarrollo del software?		x40%		
5.	¿ La empresa BITNESS CORP. S.A.C. aplica políticas de desarrollo seguro en la metodología de desarrollo del software?		x40%		
6.	¿La empresa BITNESS CORP. S.A.C. aplica guías de desarrollo seguro para cada lenguaje de programación utilizado.?		40%		
7.	¿La política de desarrollo seguro en BITNESS CORP. S.A.C considera requisitos de seguridad en la fase de diseño?		40%		
8.	¿La política de desarrollo seguro en BITNESS CORP. S.A.C consideran puntos de verificación en los hitos del proyecto (entregables o indicadores de progreso)?			x60%	
9.	¿La política de desarrollo seguro en BITNESS CORP. S.A.C consideran los repositorios seguros?				X100%
10.	¿La política de desarrollo seguro en BITNESS CORP. S.A.C.considera el control de versiones ?				X100%
11.	¿La política de desarrollo seguro en BITNESS CORP. S.A.C. considera el conocimiento sobre seguridad de aplicaciones.?	X0%			
12.	¿La política de desarrollo seguro considera la capacidad de los desarrolladores de evitar, encontrar y reparar vulnerabilidades en BITNESS CORP. S.A.C.?	X20%			
13.	¿La empresa BITNESS CORP. S.A.C. utiliza técnicas de programación segura.(para los nuevos desarrollos o situciones de reutilización de códigos)?			x60	
14	¿La empresa BITNESS CORP. S.A.C. considera las indicaciones correspondientes para el uso de las técnicas de programación segura?			x60	
15.	¿Los desarrolladores están formados en el uso de las técnicas de programación segura ?			x60%	
16.	La empresa BITNESS CORP. S.A.C exige que la parte externa (desarrolladores externos) cumplan con las normas de desarrollo seguro?	x0%			
SUMA TOTAL = 740 PORCENTAJE= 740/16=46.25%		20	280	240	200
14.2.2 Procedimientos de control de cambios en sistemas					
N°	**PREGUNTA**	**NL 0 – 20%**	**PL 21 – 49%**	**AL 50– 79%**	**CL 80 – 100%**
1.	¿La empresa BITNESS CORP. S.A.C realiza el control de cambios mediante el uso de procedimientos formales durante el ciclo de vida del desarrollo de software?	x0%			
2.	¿En la empresa BITNESS CORP. S.A.C se han documentado los procedimientos formales de control de cambios?	x0%			
3.	¿La empresa BITNESS CORP. S.A.C. cumple los procedimientos formales de control de cambios?	x0%			
4.	¿La incorporación de sistemas nuevos y cambios importantes sigue un proceso formal de documentación, especificaciones, pruebas, control de calidad y gestión de implantación?	x0%			

5.	¿Para el proceso de control de cambios se incluye una evaluación de riesgos?		x40%		
6.	¿El proceso de control de cambios asegura que los procedimientos de seguridad y controles existentes no sean accesibles a los programadores de apoyo y que estos accedan a las partes necesarias de su trabajo?				x100%
7.	Los procedimientos de control de cambios deberían incluir, pero no limitarse a: a) el mantenimiento de un registro de los niveles de autorización aprobados;				x100%
8	¿El procedimiento de control de cambios asegura que los cambios son enviados a los usuarios autorizados?				x80%
9.	¿Los procedimiento de control de cambios deben incluir la revisión de los controles y procedimientos de integridad asegurando que estos no se vean comprometidos por los cambios?				x100
10.	¿El procedimiento de control de cambios incluye la identificación de todo el software,la información, las entidades de base de datos y el hardware que requiere cambios?		x40%		
11.	¿El procedimiento de control de cambios incluye la identificación y comprobación de la seguridad del código crítico?				x80%
12.	¿El procedimiento de control de cambios incluye la aprobación formal de las propuestas detalladas antes de que comience el trabajo?			x60%	
13.	¿El procedimiento de control de cambios incluye la aceptación de los cambios de los usuarios autorizados antes de su implementación?				x80%
14.	¿El procedimiento de control de cambios actualiza la documentación del sistema al finalizar cada cambio y elimina la documentación obsoleta?		x40		
15.	¿El procedimiento de control de cambios incluye el mantenimiento de un control de versiones para las actuaciones del software?				x100%
16.	¿El procedimiento de control de cambios incluye el mantenimiento de registros de auditoría de las solicitudes de cambio?	x0%			
17.	¿El procedimiento de control de cambios incluye la implantación de los cambios en el momento adecuado sin perturbar los procesos de negocio involucrados?			x60%	
SUMA TOTAL = 880 PORCENTAJE= 880/17=51.76%		0	120	120	640

14.2.6 Entorno de desarrollo seguro

N°	PREGUNTA	NL 0 – 20%	PL 21 – 49%	AL 50– 79%	CL 80 – 100%
1.	¿Las personas que forman parte del equipo de desarrollo cumplen con los requisitos de seguridad establecidos?		40%		
2.	¿Los procesos de cada etapa de desarrollo cumplen con los requisitos de seguridad establecidos?		40%		
3.	¿Las tecnologías(computadoras, servidores, software, código) que se usan para el desarrollo de sistemas cumplen con los requisitos de seguridad establecidos?		40%		
4.	¿Los requisitos funcionales(datos de entrada) que ingresan como información están protegidos(como por ejemplo en un repositorio)?				100%
5.	¿Los datos procesados están almacenados en dispositivos seguros?				100%
6.	¿La empresa BITNESS CORP. S.A.C realiza copias de seguridad de los datos procesados?				100%
7.	¿La empresa BITNESS CORP. S.A.C transmite la información de manera protegida(mediante correos electrónicos, usb,archivos compartidos, entre otros)?		40%		
8.	¿La empresa BITNESS CORP. S.A.C aplica los requisitos de seguridad externos e internos?		40%		
9.	¿Los controles de seguridad de la organización apoyan el desarrollo del sistema?		40%		
10.	¿El personal de BITNESS CORP. S.A.C. cumple con los requisitos de seguridad(no realizan copias indebidas, no sacan la información fuera del entorno de desarrollo)?				x 100
11.	¿Existe algún documento de confidencialidad para la contratación de personal externo?	x0			
12.	¿Existen sanciones en caso de no cumplir el contrato de confidencialidad?	x0			
13.	¿La empresa BITNESS CORP. S.A.C. segrega la información cuidadosamente de acuerdo al trabajo que ejerce cada personal?				x100
14.	¿La empresa BITNESS CORP. S.A.C. maneja un control de acceso físico(ambiente de trabajo, oficinas)?	x0			

15.	¿La empresa BITNESS CORP. S.A.C. maneja un control de acceso lógico(acceso a los servidores, acceso a cuentas de usuario)?				x100
16.	¿La empresa BITNESS CORP. S.A.C. realiza la monitorización de los cambios en el producto?	x0			
17.	¿La empresa BITNESS CORP. S.A.C. realiza la monitorización de los cambios durante el proceso de desarrollo(código)?				x100
18.	¿La empresa BITNESS CORP. S.A.C. realiza copias de seguridad fuera de las instalaciones?				100
19	¿La empresa BITNESS CORP. S.A.C. almacena de manera segura sus copias de respaldo?				100
20.	¿La empresa BITNESS CORP. S.A.C. tiene identificado al personal que accede a las copias de respaldo?				100%
21.	¿La empresa BITNESS CORP. S.A.C realiza una gestión adecuada para la presentación de avances(entregables)?		40%		
22.	¿La empresa BITNESS CORP. S.A.C cumple con las medidas de seguridad para la presentación de avances(entregables)?				100%

14.2.8 Pruebas funcionales de seguridad de sistemas

N°	PREGUNTA	NL 20%	PL – 49%	AL - 79%	CL - 100%
1.	¿Realizan pruebas y verificaciones exhaustivas en el proceso de desarrollo de sistemas nuevos y los actualizados.?				100
2.	¿Las pruebas y verificaciones exhaustivas son realizadas por el equipo de desarrollo?				100
3.	¿Se realizan pruebas de aceptación independientes(para desarrollos internos y desarrollos externalizados)?	0%			

14.2.9 Pruebas de aceptación de sistemas

N°	PREGUNTA	NL 0 – 20%	PL 21 – 49%	AL 50– 79%	CL 80 – 100%
1.	¿La empresa BITNESS CORP. S.A.C. establece programas de pruebas de aceptación?				100%
2.	¿Las pruebas de aceptación del sistema incluyen las pruebas de los requisitos de seguridad de la información?				100
3.	¿Las pruebas de aceptación del sistema incluyen las prácticas de desarrollo seguro del sistema?		40%		
4.	¿Se realizan pruebas a los componentes recibidos?	0%			
5.	¿La empresa BITNESS CORP. S.A.C. utiliza herramientas automatizadas(herramientas de análisis de código o los escáneres de vulnerabilidad) para la seguridad?	0%			
6.	¿La empresa BITNESS CORP. S.A.C. realiza pruebas realistas que eviten la introducción de vulnerabilidades en la organización?	0%			

14.3.1 Protección de los datos de prueba

N°	PREGUNTA	NL 0 – 20%	PL 21 – 49%	AL 50– 79%	CL 80 – 100%
1.	¿En la empresa BITNESS CORP. S.A.C. evita el uso de datos reales o la información confidencial para las pruebas?				100%
2.	¿En caso la empresa BITNESS CORP. S.A.C use datos o información confidencial está es protegia mediante su retirada o modificación?		40%		
3.	¿Los procedimientos de control de acceso de BITNESS CORP. S.A.C se aplican a las sistema de pruebas?				100%
4.	¿La empresa BITNESS CORP. S.A.C realiza un control de acceso cada vez que la información de operación se copia a un entorno de prueba?	x 0			
5.	¿En la empresa BITNESS CORP. S.A.C la copia y uso de información operacional es registrada para futuras auditorias?	x 0			

Anexo 7. Guía de Entrevista

	GUÍA DE ENTREVISTA	CÓDIGO: F01–PM01
		VERSIÓN: 01
		FECHA: 07/09/20

PROGRAMACIÓN DE LA ENTREVISTA	
Modalidad: ( ) Presencial (x) Virtual	
Datos del Entrevistador	
Nombre: Andres Imer Rosas Huaman	
Cargo: Gerente de Operaciones	
Datos del Entrevistado	
Nombre:	
Cargo:	
Correo:	**Celular:**
Programación	
Fecha:	**Hora Inicio:**
Lugar:	**Hora Fin:**

Preguntas Generales acerca del Departamento

- ¿De qué trata su empresa?
- ¿Cómo está organizada la empresa?
- ¿Con cuántos empleados cuenta?
- ¿Cuenta con más de una sucursal?
- ¿Cuáles son los procesos existentes, incluyendo cualquier diagrama o procedimientos que hayan creado?
- ¿Cómo se comunican con los otros departamentos?
- ¿Cómo se comunican con los otros sistemas, servicios o clientes?
- ¿Cuáles son los actuales y futuros reglamentos y estándares de servicio al cliente que deben cumplir?
- ¿Qué herramientas de software se usan en la empresa?
- ¿Trabajan con algún tipo de estándar / manual de estilo de código?
- ¿Con qué tecnologías de base de datos trabaja la empresa?
- ¿Qué sistemas operativos se usan en la empresa?
- ¿Existen restricciones a la hora de usar alguna herramienta o algún software?

Preguntas Generales acerca del Procedimiento

- ¿Qué se necesita que haga el sistema?
- ¿Cómo comienza su procedimiento?
- ¿Qué documentos solicita al participante?
- ¿Recibe información de otros departamentos?
- ¿Cómo termina el procedimiento?

- ¿A quién le envía los resultados del proceso cuando termina su parte?
- ¿Con qué sistema trabajan hoy en día?
- ¿Qué es lo más difícil en el proceso actual y que cosa piensan que puede ser cambiada para mejor?
- ¿Existe algún requerimiento que se necesite implementar?
- ¿Cuál es el software que usan para realizar su trabajo?
- ¿Existe otro software que usan durante el día?
- ¿Reescriben información de un sistema a otro? ¿Cual es esta información?
- ¿Qué recomienda que se debe mejorar en el proceso?

Preguntas Indirectas

- ¿Qué se está haciendo?
- ¿Cuándo se hace?
- ¿Quién lo está haciendo?
- ¿Dónde se está haciendo?
- ¿Cuánto tiempo requiere?
- ¿Cómo se está haciendo?
- ¿Por qué……?

Anexo 8. Acta de Reunión

	ACTA DE REUNIÓN	CÓDIGO: F02–PM01
		VERSIÓN: 01
		FECHA: 07/09/20

DATOS GENERALES	
Razón Social:	**Contacto:**
RUC:	**Cargo:**
Fecha:	**Celular:**
Objetivos de la Reunión:	**Hora Inicio:**
	Hora Fin:
Responsable de la Reunión:	**Lugar:**
Modalidad: ( ) Presencial ( )Virtual	**Categoría:** ( )Interna ( )Externa

AGENDA

CONCLUSIONES - ACUERDOS

Estando los presentes de acuerdo con lo expresado, pasan a firmar para dar validez a este documento.

PARTICIPANTES			
N°.	Nombre y Apellido	Función/Cargo	Firma
1			
2			
3			
4			

Anexo 9. Requisitos Funcionales y No Funcionales

	REQUISITOS FUNCIONALES Y NO FUNCIONALES	CÓDIGO: F03-PM01
		VERSIÓN: 01
		FECHA: 07/09/20

DATOS GENERALES	
Razón Social:	**Hora Inicio:**
RUC:	**Hora Fin:**
Modalidad: ( ) Presencial ( )Virtual	**Fecha:**

En el siguiente formato se describirán los requisitos funcionales que exige el cliente para el desarrollo del software:

Código	Requisitos Funcionales
RF001	
RF002	
RF003	
RF004	

En el siguiente formato se describirán los requisitos no funcionales que exige el cliente para el desarrollo del software:

Tipos Requisitos no funcionales	Código	Clasificación	Descripción
Funcionalidad	RNF001	Exactitud	
	RNF002	Seguridad	
	RNF003	Interoperabilidad	
	RNF004	Eficiencia	
Usabilidad	RNF005	Entendimiento	
	RNF006	Desempeño	
	RNF007	Atracción	
Mantenimiento	RNF008	Capacidad de ser analizado	
	RNF009	Cambiabilidad	
	RNF010	Fácil mantenimiento	

	REQUISITOS FUNCIONALES Y NO FUNCIONALES	CÓDIGO: F03-PM01
		VERSIÓN: 01
		FECHA: 07/09/20

Fiabilidad	RNF011	Recuperabilidad	
Responsivo	RNF012	Adaptabilidad	

Estando los presentes de acuerdo con lo escrito, pasan a firmar para dar validez a este documento.

PARTICIPANTES			
N°.	**Nombre y Apellido**	**Función/Cargo**	**Firma**
1			
2			
3			
4			
5			

Anexo 10. Requisitos no funcionales de seguridad

	REQUISITOS NO FUNCIONALES DE SEGURIDAD	CÓDIGO: F04–PM01
		VERSIÓN: 01
		FECHA: 07/09/20

DATOS GENERALES	
Razón Social:	**Modalidad:** ( ) Presencial ( )Virtual
RUC:	
Fecha:	**Categoría:** ( )Interna ( )Externa
Objetivos de la Reunión:	**Hora Inicio:**
	Hora Fin:
Responsable de la Reunión:	

CÓDIGO	NOMBRE	DESCRIPCIÓN	RESPONSABLE

Anexo 11. Inventario de Requisitos de Seguridad (Confidencialidad, Integridad y Disponibilidad)

	INVENTARIO DE REQUISITOS DE SEGURIDAD (CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD)	**CÓDIGO: F05–PM01**
		VERSIÓN: 01
		FECHA: 07/09/20

DATOS GENERALES	
Razón Social:	**Hora Inicio:**
RUC:	**Hora Fin:**
Responsable de la Reunión:	**Fecha:**
Objetivos de la Reunión:	
Modalidad: ( ) Presencial ( )Virtual	

El presente documento tiene como finalidad describir los requisitos de seguridad en base a los tres pilares de la seguridad de la información.

N °	Requisito de Seguridad	Tipos requisitos de seguridad	Nivel de complejidad	Prioridad

Estando los presentes de acuerdo con lo escrito, pasan a firmar para dar validez a este documento.

PARTICIPANTES			
N°.	**Nombre y Apellido**	**Función/Cargo**	**Firma**
1			
2			
3			
4			

Anexo 12. Informe de Observaciones

	INFORME DE OBSERVACIONES	CÓDIGO: F06–PM01 VERSIÓN: 01 FECHA: 07/09/20

De:
A:
Asunto:
Fecha:

Observación 1	
Consecuencia	

Observación 2	
Consecuencia	

Observación 3	
Consecuencia	

Estando los presentes de acuerdo con lo expresado, pasan a firmar para dar validez a este documento.

CONFORMIDAD		
Nombres y Apellidos	**Función/Cargo**	**Firma**

Anexo 13. Matriz de Trazabilidad

	MATRIZ DE TRAZABILIDAD	CÓDIGO: F07–PM01
		VERSIÓN: 01
		FECHA:07/09/20

ESTADO ACTUAL	
ESTADO	ABREVIATURA
Activo	AC
Cancelado	CA

DATOS GENERALES		
Razón Social		
R.U.C.		
Fecha		
Responsable		
Modalidad de la Reunión	( ) Presencial	( )Virtual
Proyecto		

NIVEL DE COMPLEJIDAD	
ESTADO	ABREVIATURA
Alto	A
Moderado	M
Bajo	B

ID	Descripción del requisito	Versión	Estado actual	Última fecha estado registrado	Nivel de complejidad	Objetivo del proyecto	Entregables (EDT)	Estrategia y escenarios de pruebas	Interesado (Stakeholder) dueño del requisito	Nivel de prioridad

Anexo 14: Requisitos de Seguridad durante el proceso de desarrollo

	REQUISITOS DE SEGURIDAD DURANTE EL PROCESO DE DESARROLLO	**CÓDIGO: F08-PM01**
		VERSIÓN: 01
		FECHA: 07/09/20

DATOS GENERALES	
Razón Social:	**Hora Inicio:**
RUC:	**Hora Fin:**
Modalidad: ( ) Presencial ( )Virtual	**Fecha:**

DATOS DEL PROYECTO	
Nombre del proyecto	
Objetivo	
Alcance	
Cronograma	INICIO : FIN :

	Confidencialidad	**Integridad**	**Disponibilidad**
Elaboración			
Ejecución			
Transición			

Anexo 15:Informe de accesos del Equipo de Desarrollo

	INFORME DE ACCESOS DEL EQUIPO DE DESARROLLO	CÓDIGO: F09–PM01 VERSIÓN: 01 FECHA: 07/09/20

DATOS GENERALES
Razón Social:
RUC:
Fecha:
Nombre del Proyecto:

El presente documento permitirá establecer los accesos de la información teniendo en cuenta los tres pilares de la seguridad de la información:

Confidencialidad: Consiste en la capacidad de asegurar la información, delimitando los accesos de los miembros del equipo de desarrollo durante las etapas del proyecto.

Disponibilidad: Capacidad de garantizar que tanto el sistema como los datos van a estar disponibles para el equipo de desarrollo dependiendo del acceso de información que posean.

Integridad: Capacidad de garantizar que los datos no han sido modificados sin autorización desde su creación. La información que disponemos es válida y consistente. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos durante el desarrollo del sistema.

EMPLEADO	ROL	REQUISITOS A REALIZAR	ACCESO A MÓDULOS	ACCESO EN BASE A LOS TRES PILARES	REPORTAR A

Estando los presentes de acuerdo con lo escrito, pasan a firmar para dar validez a este documento.

PARTICIPANTES			
N°.	**Nombre y Apellido**	**Función/Cargo**	**Firma**
1			
2			
3			
4			

Anexo 16. Manual de la 1° Oportunidad de Mejora

	GESTIÓN DE REQUISITOS DE SEGURIDAD PARA EL DESARROLLO DE SISTEMAS	Código: MP-PM01
		Versión: 01
	MANUAL DEL PROCESO	Emisión: 07/09/20
		Página: 1 de 20

ÍNDICE

1. OBJETIVOS

El propósito de este documento es describir el proceso de "**Gestión de requisitos de seguridad para el desarrollo de sistemas**", con la finalidad de asegurar el cumplimiento del proceso y su adecuada ejecución. El proceso considera la identificación de los requisitos de seguridad para el proceso de desarrollo del sistema y del producto.

2. ALCANCE

El alcance del proceso de "**Gestión de requisitos de seguridad para el desarrollo de sistemas**", comprende la gestión de requisitos de seguridad del producto y los de gestión de requisitos de seguridad en el proceso de desarrollo. Además se considera la participación activa del stakeholder y de los involucrados.

El presente manual está dirigido a todo el personal del área de operaciones de la empresa BITNESS CORP. S.A.C.

3. DEFINICIONES

a. ***Confidencialidad:***

- En el producto: Consiste en la capacidad de garantizar que la información, almacenada en el sistema informático o transmitido por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir, que si los contenidos cayesen en manos ajenas, estas no podrían acceder a la información o a su interpretación.
- En el desarrollo del producto: Consiste en la capacidad de asegurar la información, delimitando los accesos de los miembros del equipo de desarrollo durante las etapas del proyecto.

b. ***Disponibilidad:***

- En el producto: Los sistemas constantemente reciben consultas, descargas a su sitio web, etc., por lo que deben estar disponible para los usuarios autorizados.
- En el desarrollo del producto: Capacidad de garantizar que tanto el sistema como los datos van a estar disponibles para el equipo de desarrollo dependiendo del acceso de información que posean.

c. ***Integridad:***

- En el producto: Este objetivo es muy importante para los usuarios especialmente cuando se realizan trámites bancarios en el software. La información que se dispone en el software debe ser válida y consistente.
- En el desarrollo del producto: Capacidad de garantizar que los datos no han sido modificados sin autorización desde su creación. La información que disponemos es válida y consistente. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos durante el desarrollo del sistema.

d. ***Requisitos no funcionales:***

Son aquellos requisitos que surgen de la necesidad del stakeholder, son considerados como atributos de calidad como: la seguridad, fiabilidad, mantenimiento del sistema, entre otros. El equipo es el encargado de analizar e identificar dichos requisitos para el producto y durante el desarrollo del producto

e. ***Requisitos de seguridad del producto:***

Un requisito de seguridad del producto debe definir las funciones, capacidades o atributos del sistema. La seguridad de un producto está dada por las características del producto (su diseño, componentes, composición, etc). La Seguridad del Producto es la seguridad del usuario y supone que todos los productos que se comercializan en el mercado deben ser seguros, esto es, que no presenten riesgos o presenten únicamente riesgos mínimos compatibles con el uso del producto.

f. ***Requisitos de seguridad durante el desarrollo del sistema:***

Es la identificación temprana de los requisitos de seguridad integrándolos durante todas las etapas del desarrollo del ciclo de vida del proyecto de manera que se ahorra tiempo y dinero.

g. ***Gerente de Operaciones:***

Es el rol que lidera al equipo de desarrollo en BITNESS CORP. S.A.C. y en el proceso es el encargado de Gestionar las reuniones con el stakeholder para obtener información y con el equipo de desarrollo para el desarrollo de este.

h. ***Equipo desarrollador:***

Son los expertos de desarrollo del sistema, su principal función es analizar y clasificar los requisitos de seguridad del producto, además de cumplirlos durante todas las etapas del desarrollo del producto.

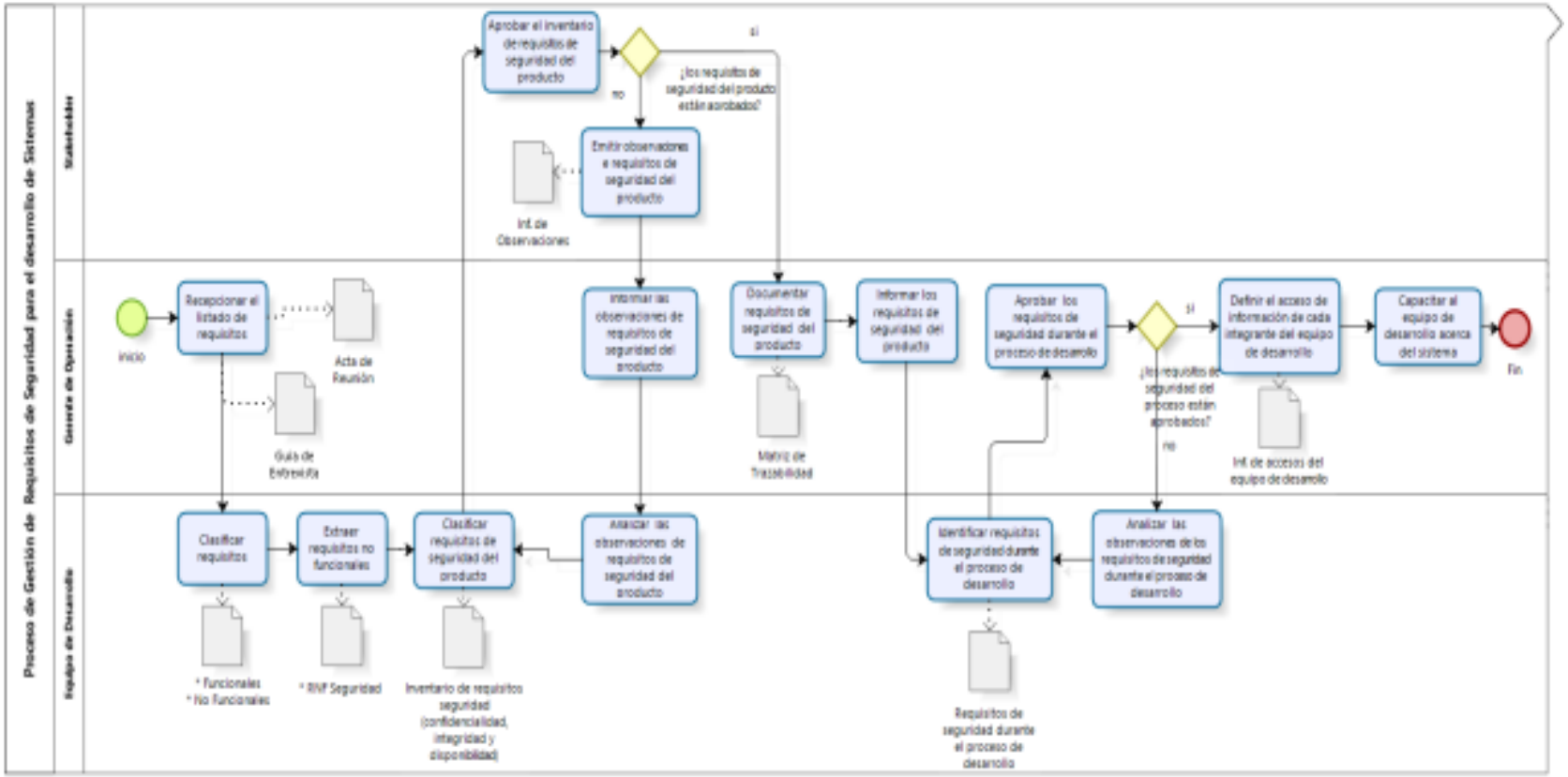
i. ***Stakeholder:***

Es aquella persona u organización interesada en recibir un servicio o un producto de BITNESS CORP. S.A.C.

4. BASE LEGAL Y NORMATIVA

- ISO 27002:2015, 14 Adquisición, desarrollo y mantenimiento de los sistemas de información
- Reglamento Interno de Trabajo de BITNES CORP. S.A.C.

5. DIAGRAMA DE PROCESOS



6. PROCEDIMIENTOS

N°	ACTIVIDAD	RESPONSABLE	ENTRADAS	TAREAS	SALIDAS
1	Recepcionar el listado de requisitos	Gerente de operaciones	Reunión programada con las siguientes especificaciones: • Hora • Fecha • Lugar • Modalidad • Participantes Guía de Entrevista	Iniciar la reunión dirigida por el gerente de operaciones de acuerdo a la modalidad que lo amerite (presencial o virtual) Dialogar con el Stakeholder sobre los requisitos utilizando la guía de entrevista con los siguientes campos: **F01–PM01** • Modalidad • Datos del entrevistador • Programación • Preguntas acerca del departamento • Preguntas acerca del procedimiento • Preguntas indirectas Registrar y elaborar los requisitos de acuerdo a la modalidad en la que se realiza la reunión. • Presencial: Plantilla de requisitos	Listado de requisitos Acta de la reunión firmada por participantes

				• Virtual: Grabación audible Firmar el acta de reunión de acuerdo a la modalidad a la cual se va rellenar el formato con los siguientes campos: **F02–PM01** • Razón social • RUC • Contacto • Cargo • Fecha • Celular • Objetivo de la reunión • Hora inicio • Hora fin • Responsable de la reunión • Modalidad (Presencial: firma o Virtual: firma virtual) • Categoría (Interna o Externa) • Agenda • Conclusiones • Participantes	
2	Clasificar requisitos	Equipo de desarrollo	Listado de requisitos	Analizar e Interpretar el listado de requisitos	

				Clasificar los requisitos funcionales y no funcionales Documentar los requisitos funcionales y no funcionales con los siguientes campos: **F03–PM01** • Razón social • RUC • Hora inicio • Hora fin • Modalidad • Fecha • Código • Requisitos funcionales • Tipo requisito no funcionales • Código • Clasificación • Descripción • Participantes	Requisitos funcionales y no funcionales documentados
3	Extraer requisitos no funcionales	Equipo de desarrollo	Requisitos funcionales y no funcionales	Revisar y analizar la documentación de los requisitos no funcionales Identificar los requisitos no funcionales de seguridad.	Requisitos no funcionales

				Documentar los requerimientos no funcionales de seguridad en el formato con los siguientes campos: **F04–PM01** • Razón social • Modalidad • RUC • Fecha • Categoría • Objetivo de Reunión • Hora inicio / fin • Responsable de la reunión • Código • Nombre • Descripción • Responsable	
4	Clasificar requisitos de seguridad del producto	Equipo de desarrollo	Requisitos no funcionales de usuario y de desarrollador	Analizar la clasificación de los requisitos no funcionales Identificar los requisitos no funcionales de seguridad en relación a: • Integridad • Confidencialidad • Disponibilidad	Inventario de requisitos seguridad del producto (confidencialidad, integridad y disponibilidad)

				Elaborar el inventario de requisitos de seguridad del producto con los siguientes atributos: **F05–PM01** • Razón social • RUC • Hora inicio • Hora fin • Fecha • Lugar • Objetivo de la reunión • Responsable de la reunión • Código • Requisitos de seguridad • Tipos de requisitos de seguridad • Nivel de complejidad • Prioridad • Participantes	
5	Aprobar el inventario de requisitos de seguridad del producto	Stakeholder	Inventario de requisitos seguridad del producto	Convocar a una reunión de acuerdo a la modalidad (virtual o presencial)	Inventario de requisitos de seguridad aprobado por el stakeholder
				Presentar el inventario de requisitos de seguridad dirigido por el gerente de operaciones	
				Debatir el inventario de requisitos de seguridad	

				Tomar la decisión si el inventario de requisitos de seguridad producto es válido. Si se aprueba para a la actividad 9. Si no se aprueba pasa a la actividad 6. Dialogar sobre las observaciones.	
6	Emitir observaciones de requisitos de seguridad del producto	Stakeholder	Conjunto de observaciones	Documentar las observaciones al inventario de requisitos de seguridad del producto, en el formato con los siguientes campos: **F06–PM01** • De • A • Asunto • Fecha • Observación • Consecuencia Enviar observaciones por correo electrónico a Gerente de operaciones	Informe de observaciones
7	Informar las observaciones de requisitos de	Gerente de operaciones	Informe de observaciones	Convocar a una reunión de acuerdo a la modalidad que lo amerite contando con la participación de todo el equipo de desarrollo	Recepción de las observaciones por parte del equipo de desarrollo

	seguridad del producto		Reunión programada con las siguientes especificaciones: • Hora • Fecha • Lugar • Modalidad • Participantes	Presentar y Difundir las observaciones Explicar en qué consiste cada una de las observaciones	
8	Analizar las observaciones de requisitos de seguridad del producto	Equipo de desarrollo	Recepción de las observación	Revisar y analizar las observaciones Realizar nuevamente la clasificación de requisitos de seguridad Elaborar una nueva versión del inventario de requisitos de seguridad	Inventario de requisitos de seguridad del producto con observaciones levantadas (confiabilidad, integridad y disponibilidad)
9	Documentar requisitos de seguridad del producto	Gerente de operaciones	Inventario de requisitos de seguridad del producto (confiabilidad, integridad y disponibilidad) aprobado por Stakeholder	Elaborar la matriz de trazabilidad con los siguientes atributos: **F07–PM01** • Razón social • RUC • Fecha • Responsable • Modalidad de reunión • Proyecto • Identificación (ID)	Matriz de Trazabilidad de los requisitos de seguridad del producto

				• Descripción del requisito • Versión • Estado actual • Última fecha de registro • Nivel de complejidad • Objetivo del proyecto • Entregables • Estrategias y escenario de pruebas • Stakeholder • Nivel de prioridad	
10	Informar los requisitos de seguridad del producto	Gerente de operaciones	Reunión programada con las siguientes especificaciones: • Hora • Fecha • Lugar • Modalidad • Participantes Matriz de trazabilidad	Convocar a una reunión al equipo de desarrollo Comunicar los requisitos de seguridad del producto Evaluar si la información brindada ha sido entendida.	Equipo de desarrollo capacitado en los requisitos de seguridad del producto en base a la matriz de trazabilidad
11	Identificar los requisitos de seguridad durante el	Equipo de desarrollo	Equipo de desarrollo capacitado en los requisitos de seguridad del	Dirigir la reunión por jefe de proyecto Debatir sobre los requisitos de seguridad durante el proceso de desarrollo	Informe de requisitos de seguridad durante el proceso de desarrollo

	proceso de desarrollo		producto en base a la matriz de trazabilidad Reunión programada con las siguientes especificaciones: • Hora • Fecha • Lugar • Modalidad • Participantes	Segmentar los requisitos de seguridad durante el proceso de desarrollo en base a: confidencialidad, integridad y disponibilidad. Documentar los requisitos de seguridad durante el proceso de desarrollo con los siguientes campos: **F08–PM01** • Razón social • RUC • Modalidad • Hora inicio • Hora fin • Fecha • Nombre del proyecto • Objetivo • Alcance • Cronograma • Etapas de proyecto • Confidencialidad • Integridad • Disponibilidad	
12	Aprobar los requisitos de seguridad	Gerente de operaciones	Informe de requisitos de seguridad durante el proceso de desarrollo	Recepcionar el informe de requisitos de seguridad durante el proceso de desarrollo	Requisitos de seguridad durante el proceso de desarrollo aprobados por

	durante el proceso de desarrollo			Evaluar el informe de requisitos de seguridad durante el proceso de desarrollo Tomar la decisión: • Si se aprueba Informe de requisitos de seguridad durante el proceso de desarrollo, pasa a la actividad 14 • Si no se aprueba pasa a la actividad 13. Realizar las observaciones. Devolver el informe de requisitos de seguridad durante el proceso de desarrollo con las observaciones añadidas.	el Gerente de operaciones
13	Analizar la observaciones de los requisitos de seguridad durante el proceso de desarrollo	Equipo de desarrollo	Recepcionar el informe de requisitos de seguridad durante el proceso de desarrollo con las observaciones añadidas	Revisar y analizar las observaciones Realizar nuevamente la identificación de requisitos de seguridad durante el proceso de desarrollo Elaborar una nueva versión del requisitos de seguridad durante el proceso de desarrollo	Informe de requisitos de seguridad durante el proceso de desarrollo

14	Definir el acceso de información de cada integrante del equipo de desarrollo	Gerente de operaciones	Informe de requisitos de seguridad durante el proceso de desarrollo Información acerca de las funciones de cada miembro del equipo de desarrollo	Analizar el informe de requisitos de seguridad durante el proceso de desarrollo Asignar las tareas que realizará cada miembro del equipo de desarrollo Delimitar los accesos a cada miembro del equipo estableciendo restricciones de acuerdo a las tareas Elaborar el informe de accesos del equipo de desarrollo con los siguientes campos: **F09–PM01** • Razón social • RUC • Fecha • Nombre del proyecto • Empleado • Rol • Requisitos a realizar • Acceso a módulos • Acceso en base a los tres pilares • Reportar a	Informe de acceso del equipo de desarrollo
15	Capacitar al equipo de	Gerente de operaciones	Informe de acceso del equipo de desarrollo	Reunión dirigida por el gerente de operaciones	Equipo de desarrollo capacitado

	desarrollo acerca del sistema		Reunión programada con las siguientes especificaciones: • Hora • Fecha • Lugar • Modalidad • Participantes	Presentar la forma de trabajo para el desarrollo del sistema Brindar asesoría personalizada Evaluar si la información brindada ha sido entendida.	

7. INDICADORES Y EVIDENCIAS DE CONTROL

INDICADORES

N°	NOMBRE	UM	META	RESPONSABLE	FRECUENCIA	FUENTE
01	Nivel de Cumplimiento de actividades del proceso	%	100	Gerente de Operaciones	En cada etapa del proceso	_
02	Calidad de los requisitos documentados	%	100	Gerente de Operaciones	Primera etapa del desarrollo	Inventario de requisitos de seguridad del producto

EVIDENCIAS DE CONTROL

N°	NOMBRE	RESPONSABLE	FRECUENCIA
01	Actas de Reunión	Gerente de Operaciones	Cada reunión
02	Inventario de Requisitos seguridad del producto aprobado por el Stakeholder	Gerente de Operaciones	Primera etapa
03	Requisitos de seguridad durante el desarrollo del producto aprobados por el Gerente de Operaciones	Gerente de operaciones	_

8. RIESGOS

N°	NOMBRE	PLAN DE ACCIÓN
01	Incumplimiento del cronograma	- Identificar las fortalezas y debilidades en las actividades más importantes en el cronograma. - Documentar las acciones implementadas, elaborando una guía de trabajo para que sirva de modelo para otros trabajos similares.
02	Disponibilidad del Stakeholder	- Proponer un tiempo de holgura para las actividades relacionadas con el Stakeholder, así no afecten a la planificación del proyecto.

9. FORMATOS

N°	CÓDIGO	DESCRIPCIÓN
1	F01–PM01	Guía de entrevista
2	F02–PM01	Acta de reunión
3	F03–PM01	Requisitos Funcionales y No Funcionales
4	F04–PM01	Requisitos No Funcionales de Seguridad
5	F05–PM01	Inventario de Requisitos de Seguridad (Confidencialidad, integridad y disponibilidad),
6	F06–PM01	Informe de Observaciones
7	F07–PM01	Matriz de Trazabilidad
8	F08–PM01	Requisitos de seguridad durante el proceso de desarrollo
9	F09–PM01	Informe de accesos del equipo de desarrollo

CONTROL DE CAMBIOS

N° Versión	DESCRIPCIÓN	FECHA

ANEXOS

- Guía de entrevista:
  https://docs.google.com/document/d/1wxPbN5D8EQAcz66LVXhMikb5q_puioVZ-_t1y0LwJ8/edit?usp=sharing
- Acta de reunión:
  https://docs.google.com/document/d/13FDBe8wVin4cfeQBkSMS4OKLIPZQHtHdc5td2y1BKX0/edit?usp=sharing
- Requisitos Funcionales y No Funcionales
  https://docs.google.com/document/d/1p00q33-uhR0rUv6GWrwYv_aFUECo0s821p5TKsSJZMc/edit?usp=sharing
- Requisitos No Funcionales de Seguridad
  https://docs.google.com/document/d/1iP5Sw_7ZuKtCcPPwglsJtlkLfsHtmpwyrSMID57MNIl/edit?usp=sharing

- Inventario de Requisitos de Seguridad (Confidencialidad, integridad y disponibilidad), https://docs.google.com/document/d/1cex6i1awAZx0iFjlojGRIQGD216Rq3x9UcXPJeb367w/edit?usp=sharing
- Informe de Observaciones: https://docs.google.com/document/d/1CZVJCbReCeP6e7rm94KqcIJCEpfj811gjoY9Cw12uRU/edit?usp=sharing
- Matriz de Trazabilidad https://docs.google.com/spreadsheets/d/1QeedbgmZJTHNcbPxTs6APNRCcqPSdl_CRVhup6VgdiQ/edit?usp=sharing
- Requisitos de seguridad durante el proceso de desarrollo https://docs.google.com/document/d/1rcvWyhKCaw5H9yMY529V-cNr9SOOHVJK_RFjTYM1fl0/edit?usp=sharing
- Informe de accesos del equipo de desarrollo https://docs.google.com/document/d/1vx6TVdZrVMwFREZxQG97fuQUOiBXyWpXR4H4RPhyjC0/edit?usp=sharing

Anexo 17. Características Técnicas del Producto o Servicio

	CARACTERÍSTICAS TÉCNICAS DEL PRODUCTO O SERVICIO	CÓDIGO: F02–PM01 VERSIÓN: 01 FECHA: 03/12/20

El presente documento permite establecer las características técnicas del producto o servicio a adquirir en la empresa BITNESS CORP. S.A.C. Se debe tener en cuenta las siguientes características:

DATOS GENERALES	
Nombre del Producto o Servicio	
Marca / Versión	
Sector	
Tipo de Soporte Técnico	Soporte Telefónico, Soporte Vía Internet, etc.
Formación del Personal	Manual y/o Capacitación

En la tabla de características técnicas se encuentran tres columnas, en la primera se encuentra la característica técnica general del producto o servicio a adquirir como, por ejemplo: funcionalidad, rendimiento, usabilidad, entre otros. En la segunda columna se observa las características técnicas específicas que se encuentran dentro de las generales, entre paréntesis se brinda información acerca de la característica técnica mencionada. En la tercera columna, se deberá llenar con un Si o un No dependiendo de lo deseado para el producto o servicio a adquirir.

CARACTERÍSTICAS TÉCNICAS		
Funcionalidad	Completitud (Capacidad de modificarlo)	
	Idoneidad (Capacidad de proporcionar un conjunto de tareas y objetivos)	
Rendimiento	Comportamiento en el tiempo (Tiempos de respuesta, tiempos de proceso y potencia)	
	Utilización de Recursos (Usar cantidades y recursos adecuados)	
Usabilidad	Inteligibilidad (Permite al usuario entender si el producto es adecuado y su forma de uso)	
	Aprendizaje (Permite al usuario aprender su aplicación)	
	Operabilidad (De uso simple)	

	Atractividad (Presentación acorde a las expectativas del usuario)	
Fiabilidad	Madurez (Evitar fallas)	
	Tolerancia a Fallos (Mantener un nivel específico de prestaciones en caso de fallos)	
	Capacidad de Recuperación (Capacidad de restablecer prestaciones y recuperar datos afectados en caso de fallos).	
Seguridad	Confidencialidad (Control de accesos)	
	Integridad (Datos y servicios acordados)	
	No repudio (Confirmación de acciones)	
Mantenibilidad	Modularidad (Los cambios en sus componentes tengan un impacto mínimo)	
	Reusabilidad (Se puede usar en más de un entorno)	
	Capacidad de ser probado (Permite que la modificación se valide)	
Portabilidad	Adaptabilidad (Adaptación a diferentes entornos)	
	Facilidad de Instalación (Facilidad de instalación en un entorno)	
	Intercambiabilidad (Capacidad para ser usado en lugar de otro producto)	
Compatibilidad	Coexistencia (Ejecución de distintas operaciones simultáneamente)	
	Interoperabilidad (Interactúa con uno o más entornos)	
Escalabilidad	(Capacidad de expandirse o incrementar la cantidad de usuarios)	

Anexo 18. Perfil del Producto o Servicio

	PERFIL DEL PRODUCTO O SERVICIO	CÓDIGO: F02–PM02 VERSIÓN: 01 FECHA: 03/12/20

Este presente documento permitirá establecer la información consolidada del cumplimiento de las características técnicas que se desea adquirir y otras informaciones adicionales que conciernen al producto o servicio.

Nombre del producto o servicio	Software de Requisitos
Objetivo	Identificar los requisitos de seguridad
Clasificación	Sistema de Gestión de Requisitos
Características Técnicas:	Atributos de Calidad
Información Adicional:	- **Página del Fabricante:** - **Datos de la Instalación:** - **Tamaño de la aplicación y versión:**

Anexo 19. Criterios de Aceptación

	LISTADO DE CRITERIOS DE ACEPTACIÓN DEL PRODUCTO O SERVICIO	CÓDIGO: F03–PM01 VERSIÓN: 01 FECHA: 03/12/20

El presente documento permite establecer el listado de criterios de aceptación del producto o servicio a adquirir en la empresa BITNESS CORP. S.A.C. Se tiene en cuenta los datos generales del producto o servicio:

DATOS GENERALES	
Nombre del Producto o Servicio	
Serie / Versión	
Marca	
Empresa Proveedora	

Y las características técnicas específicas como:

- Funcionabilidad: Cumplimiento con el objetivo (Completitud, corrección e idoneidad).
- Rendimiento: Tiempo de respuesta (Comportamiento en el tiempo y utilización de recursos).
- Usabilidad: Fácil de aprender (Inteligibilidad, aprendizaje, operabilidad, protección a errores de usuario, atractividad y accesibilidad).
- Fiabilidad: Habilidad para mantenerse operativo dentro de las condiciones normales (Madurez, disponibilidad, tolerancia a fallos y capacidad de recuperación).
- Seguridad: Resistente a ataques externos (Confidencialidad, integridad, no repudio, autenticidad y responsabilidad).
- Mantenibilidad: Puede ser modificado por los desarrolladores (Modularidad, reusabilidad y la capacidad de ser probado).
- Portabilidad: Puede ser utilizado en diversos equipos (Adaptabilidad, fácil instalación e intercambiabilidad).
- Compatibilidad: (Coexistencia e interoperabilidad).

Las cuáles serán evaluadas en base a los rangos de No Logrado, Parcialmente Logrado, Altamente Logrado y Completamente Logrado.

(NOMBRE DEL PRODUCTO)	FUNCIONALIDAD	RENDIMIENTO	USABILIDAD	FIABILIDAD	SEGURIDAD	MANTENIBILIDAD	PORTABILIDAD	COMPATIBILIDAD
No Logrado								
Parcialmente Logrado								
Altamente Logrado								
Completamente Logrado								

Anexo 20. Periodo de Prueba

	PLAN DE PERIODO DE PRUEBA	CÓDIGO: F04–PM02 VERSIÓN: 01 FECHA: 03/12/20

1. **DATOS GENERALES**

Producto	**Clasificación**
Software de Requisitos	Sistema de Gestión de Requisitos
Documento de Evaluación relacionados	
Documento de Criterios de Aceptación	
Equipo de Evaluación	
Responsable del equipo evaluador	

2. **ALCANCE DE LAS PRUEBAS**

A continuación se presentan los módulos del sistema representados en cuadros, cada uno con sus requerimientos de prueba bien definidos a cabo con éxito.

Cuadro 1: Modulo 1

Componentes a ser aprobados	
Objetivo de las pruebas	
Detalle del orden de ejecución de los componentes	
Responsabilidad de la prueba	

3. **ENTORNO Y CONFIGURACIÓN DE PRUEBAS**

Para el proceso de pruebas se requiere la disponibilidad de los siguientes entornos, a saber:

3.1. Equipo de Prueba

a. Servidor Virtual:
b. Sistema Operativo:
c. Procesador:
d. Disco duro:

3.2. Base de Datos de Prueba

a. Base de Datos:
b. Servidor BD:
c. Datos: Aleatorios

3.3. Criterios de aprobación/rechazo

Criterios	**Descripción**
Aprobado	Se aprobará el producto o servicio con un 100% de las pruebas ejecutadas pero con un 90% de aceptación.Esto quiere decir que el 90% de las pruebas deben ser exitosas y sin errores. En el restante 10% pueden existir errores medios o bajos, pero no graves
Rechazado	En caso de ocurrir que el producto o servicio no cumpla con el nivel exigido, el producto o servicio se rechaza por completo.

Proveedor **Gerencia General**

Anexo 21. Cronograma de Pruebas

	CRONOGRAMA DE PRUEBAS	CÓDIGO: F05–PM01 VERSIÓN: 01 FECHA: 03/12/20

El presente documento permitirá establecer fechas en las cuales se evaluará al producto o servicio a adquirir mediante los criterios de aceptación de la empresa BITNESS CORP. S.A.C.

Se aplicará el listado de criterios de aceptación los días marcados con las casillas rojas, por lo cual en el lapso de un mes se han de realizar 4 pruebas al producto o servicio.

CRONOGRAMA DE PRUEBAS					
(Nombre del Producto o Servicio)	MES / ANO				
	LUNES	MARTES	MIÉRCOLES	JUEVES	VIERNES
1° SEMANA DEL _____ AL ____					
2° SEMANA DEL _____ AL ____					
3° SEMANA DEL _____ AL ____					
4° SEMANA DEL _____ AL ____					

Anexo 22. Informe de Periodo de Pruebas

	INFORME PERIODO DE PRUEBA	CÓDIGO: F06–PM02 VERSIÓN: 01 FECHA: 03/12/20

El presente documento permitirá establecer todo la información que se obtuvo en base a la ejecución del plan de periodo de pruebas y a la aplicación del documento criterios de aceptación del producto o servicio a adquirir.

Nombre del producto o servicio:

Objetivo

Información general

Fecha de comienzo planificada	Fecha de finalización planificada	Casos de prueba (Total)	Casos Planificados	Casos exitosos	Casos con incidencias

Puntos de Atención y observación

-

Jefe de Proyecto

Anexo 23. Manual de la 2° Oportunidad de Mejora

	MANUAL DEL PROCESO	Código: MP–PM02
		Versión: 001
	ADQUISICIÓN FORMAL DEL PRODUCTO O SERVICIO ASEGURANDO LA CALIDAD	Emisión:01-10-20
		Página: 1 de 15

ÍNDICE

1. OBJETIVOS

El propósito de este documento es describir el proceso de "**Adquisición del producto o servicio asegurando la calidad**", con la finalidad de asegurar el cumplimiento del proceso y su adecuada ejecución. El proceso considera la adquisición formal del producto o servicio para el proceso de desarrollo del sistema y del producto.

2. ALCANCE

El alcance del proceso de "**Adquisición del producto o servicio asegurando la calidad**", comprende desde la identificación de la necesidad del producto o servicio hasta la negociación de la adquisición del producto o servicio. Además, se considera la participación activa del Proveedor y de los involucrados.

El presente manual está dirigido a todo el personal del área de operaciones de la empresa BITNESS CORP. S.A.C.

3. DEFINICIONES

a. ***Producto:*** Todo programa o sistema informático (Software).

b. ***Servicio:*** Es una actividad o función brindada por una empresa o persona jurídica para satisfacer las necesidades de BITNESS CORP. S.A.C. Un servicio puede ser la energía eléctrica, agua, internet, aire acondicionado, mantenimiento de equipos, entre otros.

c. ***Cotización:*** Es la acción de la empresa o persona jurídica para ofrecer el producto o servicio que desean vender.

d. ***Perfil del Producto o Servicio:*** Es el documento que describe las características y funcionalidad del servicio que la empresa requiere de acuerdo a sus necesidades.

e. ***Periodo de Prueba:*** Es el lapso de tiempo en el cual se hace uso del producto o servicio para su posterior adquisición.

f. ***Negociación:*** Son los acuerdos tomados para la adquisición del producto o servicio como: especificaciones del contrato, garantías, entre otros.

g. ***Contrato:*** Es el acuerdo legal, oral o escrito que sea manifiesta en común entre dos o más personas con capacidad jurídica. En el caso del proceso el contrato lo realiza el Gerente de operaciones con la empresa o persona jurídica que se realiza la negociación.

h. *Gerencia General (socios):* Es el área encargada de velar por las funciones de la empresa. En el proceso es el área encargada de tomar las decisiones mediante una evaluación de la adquisición del producto o servicio.

i. *Gerente de Operaciones:* Es el rol que lidera al equipo de desarrollo en BITNESS CORP. S.A.C. y en el proceso es el encargado de identificar la necesidad de los productos o servicios en la empresa y gestionar la adquisición de estos.

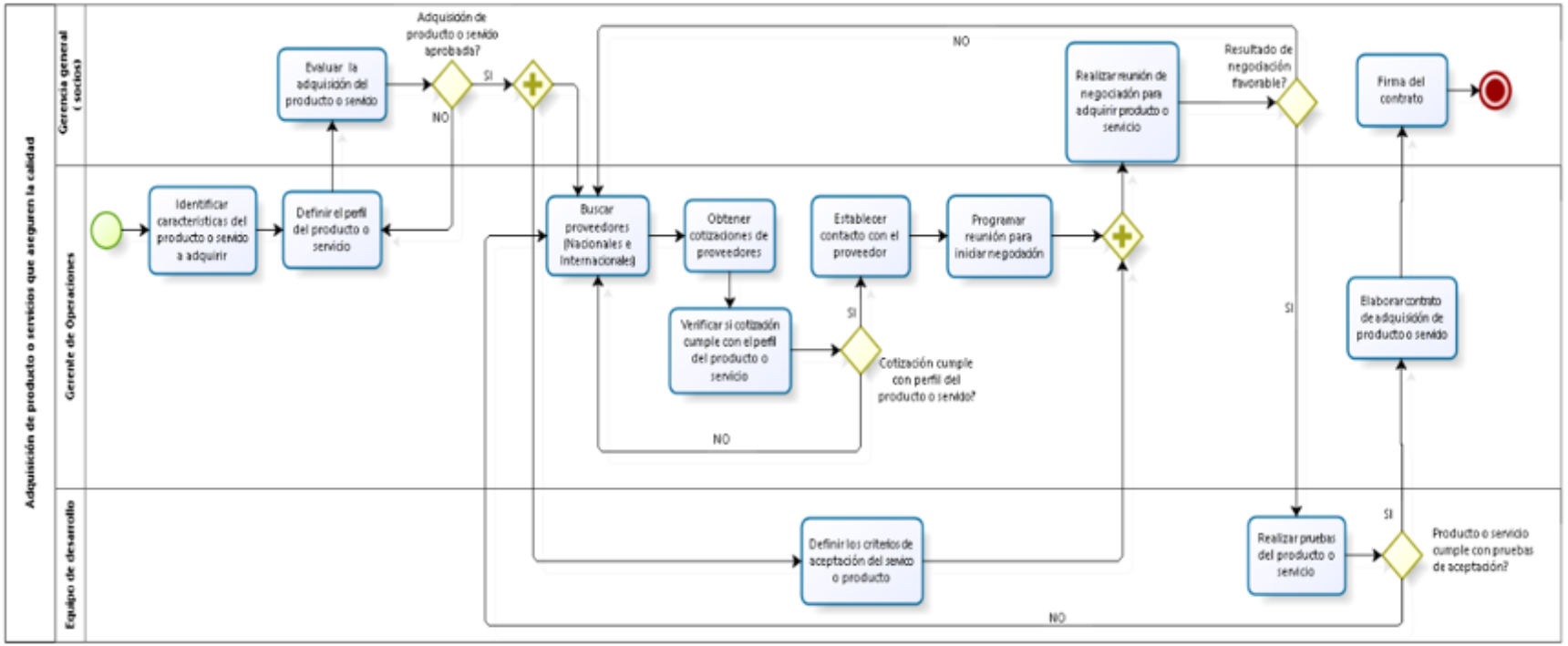
j. *Equipo desarrollador:* Son los expertos en el desarrollo de los sistemas, su principal función en el proceso es realizar los criterios de aceptación del producto y servicio que se va adquirir para posteriormente realizar las pruebas y verificar el cumplimiento de los criterios de aceptación para la adquisición del producto o servicio.

k. *Proveedores:* Es aquella persona jurídica u organización cuyo objetivo responde a las necesidades del cliente, en el proceso es el encargado de los productos o servicios.

4. BASE LEGAL Y NORMATIVA

- ISO 27002:2015, 14 Adquisición, desarrollo y mantenimiento de los sistemas de información
- Reglamento Interno de Trabajo de BITNES CORP. S.A.C.

5. DIAGRAMA DE PROCESOS



6. PROCEDIMIENTOS

N°	ACTIVIDAD	RESPONSABLE	ENTRADAS	TAREAS	SALIDAS
1	Identificar características del producto o servicio a adquirir	Gerente de Operaciones	Inventario de productos o servicios	Identificar los productos o servicios que hacen falta. Evaluar la compra o arrendamiento del producto o servicio. (Decisión) Identificar las características técnicas del producto o servicio en el formato **F01-PM01**, donde están las tablas de datos generales y características técnicas con los siguientes ítems: Datos Generales: - Nombre del Producto o Servicio - Marca / Versión - Sector - Tipo de Soporte Técnico - Formación del Personal Características Técnicas: - Funcionalidad - Rendimiento	Documento de las características técnicas del producto o servicio.

	Evaluar la adquisición del producto o servicio			Presentar el perfil del producto o servicio Debatir la adquisición del producto o servicio Tomar una decisión: • Si se aprueba la adquisición del producto o servicio se realizan dos actividades paralelamente 4 y 5. • Si no se aprueba la adquisición del producto o servicio regresa a la actividad 2.	
4	Definir los criterios de aceptación del producto o servicio	Equipo de Desarrollo	Adquisición del producto o servicio aprobada	El jefe de desarrollo convoca a una reunión de equipo. Debatir los posibles criterios de aceptación del producto o servicio. Elaborar la documentación de criterios de aceptación. llenando en el formato **F03-PM02**, los ítems: - Datos Generales: - Nombre del Producto o Servicio - Serie / Versión	Lista de criterios de aceptación del producto o servicio

				- Marca - Empresa Proveedora - Características Técnicas: - Funcionalidad - Rendimiento - Usabilidad - Fiabilidad - Seguridad - Mantenibilidad - Portabilidad - Compatibilidad Las cuáles serán evaluadas en base a los rangos de No Logrado, Parcialmente Logrado, Altamente Logrado y Completamente Logrado.	
				Presentar documentación al Gerente de Operaciones.	
5	Buscar proveedores nacionales e internacionales	Gerente de Operaciones	Adquisición del producto o servicio aprobada	Buscar proveedores nacionales e internacionales orientados al producto o servicio adquirir.	Proveedores identificados nacionales e internacionales
				Establecer contacto con proveedores nacionales e internacionales.	
				Obtener información de los proveedores: - RUC	

				- Razón Social - Contacto - Correo electrónico	
6	Obtener cotizaciones	Gerente de Operaciones	Proveedores identificados nacionales e internacionales	Enviar a la cuenta del correo electrónico el perfil del producto o servicio solicitándolas cotizaciones. Recepcionar las cotizaciones (Proformas)	Cotizaciones (Proformas)
7	Verificar si cotización cumple con el perfil del producto o servicio	Gerente de Operaciones	Proforma	Discriminar la procedencia del proveedor (priorizar proveedores nacionales) y según el nivel de cumplimiento del perfil del producto o servicio. Seleccionar un mínimo de tres proveedores Tomar decisión: • Si la cotización cumple con el perfil del producto o servicio se pasa a la actividad 9 • Si la cotización no cumple con el perfil del producto o servicio se regresa a la actividad 5	Cotización aceptada

9	Establecer contacto con el proveedor	Gerente de Operaciones	Cotización aceptada	Enviar un correo informando que la cotización ha sido aceptada.	Proveedor contactado
10	Programar reunión para iniciar negociación	Gerente de Operaciones	Proveedor contactado	Programar reunión: - Fecha y hora - Modalidad de reunión - Participantes - Documentación a utilizar.	Reunión programada y Acta de Reunión
				Enviar programación de la reunión a todos los participantes.	
				Preparar el formato **F04-PM02** de acta de reunión, que cuenta con los ítems de: - Datos Generales - Agenda - Conclusiones – Acuerdos - Participantes	
11	Realizar reunión de negociación para adquirir producto o servicio	Gerencia General	Reunión programada	Iniciar la reunión dirigida por el Gerente de Operaciones	Documento de Plan Periodo de prueba
				Negociar las especificaciones del plan periodo de prueba del producto o servicio en el formato **F05-PM02**, consta de los siguientes ítems: - Datos Generales:	

				- Producto - Clasificación - Documento de Evaluación relacionados - Equipo de Evaluación - Responsable del Equipo de Evaluación. - Alcance de las Pruebas: - Componentes a ser aprobados - Objetivo de las Pruebas - Detalle del orden de ejecución de los componentes - Responsabilidad de la prueba - Entorno y configuración de pruebas: - Equipo de Prueba - Base de Datos de Prueba - Criterios de aprobación o rechazo Establecer periodo de prueba (Condiciones).	
12	Realizar pruebas del producto o servicio	Equipo de desarrollo	Documento de Periodo de prueba	Establecer un cronograma de pruebas según el formato **F06-PM02**, en el cual se llenan las fechas de prueba y se ejecutan las pruebas según las casillas rojas.	Cronograma de pruebas e Informe del Periodo de Prueba

				Medir el cumplimiento en base a los criterios de aceptación.	

				Elaborar el informe del periodo de prueba en el formato **F07-PM02,** consta de siguientes ítems:
				- Nombre del producto o servicio
				- Objetivo
				- Información General
				  - Fecha de inicio planificada
				  - Fecha fin planificada
				  - Casos de prueba (Total)
				  - Casos planificados
				  - Casos exitosos
				  - Casos con incidencias
				- Puntos de Atención y Observación	

				Tomar decisión: • Si el producto o servicio cumple con los criterios de aceptación pasar a la actividad 13 • Si el producto o servicio no cumple con los criterios de aceptación regresar a la actividad 5	

13	Firmar contrato de adquisición de producto o servicio	Gerente de Operaciones	Cumplimiento de los criterios de aceptación	Convocar a una reunión con el proveedor	Contrato y Producto o servicio adquirido
				Documentar los acuerdos	
				Recepción del contrato	
				Evaluación del contrato	
				Firma del contrato	

7. INDICADORES Y EVIDENCIAS DE CONTROL

INDICADORES

N°	NOMBRE	UM	META	RESPONSABLE	FRECUENCIA	FUENTE
01	Cumplimiento	%	100	Gerente de Operaciones	En cada actividad del proceso	–

EVIDENCIAS DE CONTROL

N°	NOMBRE	RESPONSABLE	FRECUENCIA
01	Doc. Características técnicas del Producto o Servicio	G. de Operaciones	Proceso
02	Perfil del Producto o Servicio	G. de Operaciones	Proceso
03	Lista de Criterios de Aceptación	Equipo de Desarrollo	Proceso
04	Doc. Periodo de Prueba	Gerencia General	Proceso
05	Acta de Reunion	G. de Operaciones	Proceso
06	Cronograma de Pruebas	Equipo de Desarrollo	Proceso
07	Informe de Periodo de Pruebas	Equipo de Desarrollo	Proceso

8. RIESGOS

N°	NOMBRE	PLAN DE ACCION

9. FORMATOS

N°	CODIGO	DESCRIPCION
01	F01–PM02	Doc. Características técnicas del Producto o Servicio
02	F02–PM02	Perfil del Producto o Servicio
03	F03–PM02	Lista de Criterios de Aceptación
04	F04–PM02	Doc. Plan de Periodo de Prueba

05	F05–PM02	Acta de Reunión
06	F06–PM02	Cronograma de Pruebas
07	F07-PM02	Informe de Periodo de Pruebas

CONTROL DE CAMBIOS

N° Versión	DESCRIPCION	FECHA

10. ANEXOS

- Doc. Características técnicas del Producto o Servicio:

https://docs.google.com/document/d/1TjMjNbZP7KouJe7_JtPPrduYkUC4Szzu_AwREjO2dGss/edit

- Perfil del Producto o Servicio:

https://docs.google.com/document/d/1j-XqM7H2o3SQazzPodWvZbUR00_aqbkqALBZCZy_f9s/edit

- Lista de Criterios de Aceptación
- Doc. Plan Periodo de Prueba:

https://docs.google.com/document/d/1iGrvSIME35WTYOAfgoQQCuo3yjCTpvcoFFXL0q7Ibt4/edit

- Acta de Reunión:

https://docs.google.com/document/d/1LT0EuVZP1z_SqssMRdwhTccAj99pNfat7who85c1rZg/edit

- Cronograma de Pruebas:

https://docs.google.com/document/d/1q4IWCWrFMM9o0bDCW4Hvl2LVdybcw4kqfHhsHfmRajA/edit

- Informe de Periodo de Pruebas:

https://docs.google.com/document/d/11uVSqc-0rBStec-QZjlpIMUO_adTRi5_0Vnh0_-mSo/edit

Anexo 24. Solicitud de Cambio

	SOLICITUD DE CAMBIO	CÓDIGO: F01–PM03
		VERSIÓN: 1
		FECHA: 14/01/2021

El presente documento permite registrar el cambio correctamente, y obtener la información necesaria para una gestión de cambio eficaz. Se pide describir los campos de ambas tablas de manera objetiva ya que son clave para una gestión óptima de cambio.

DATOS GENERALES	
Nombre del Solicitante	
Correo del Solicitante	
Naturaleza del cambio	Cambio en los requerimientos ( ) Procesos operativos o misionales ( ) Procesos de gestión del proyecto ( )

(Nombre del Proyecto al cual se realizará el cambio)
Descripción del Cambio propuesto
(Incluye referencias a documentos que contengan más detalles)
Razón del Cambio (Justificación)
(Justifica la necesidad del cambio, como por ejemplo imposibilidad para desempeñar la actividad, cambio en la reglamentación, ahorro en costos, mejora en el proceso, riesgo legal, entre otros, junto con el correspondiente análisis de riesgo/beneficio)
Modulos que afecta
Alternativas

Solicitante:

Puesto:

Gerente de Operaciones

Ing. Imer Andres Rosas H.

Anexo 25. Control de Cambio

	CONTROL DE CAMBIOS	CÓDIGO: F02–PM03 VERSIÓN: 1 FECHA:14/01/2021

Código de Formato	Nombre del Solicitante	Correo del Solicitante	Naturaleza del Cambio	Fecha	Nombre del Proyecto	Descripción del cambio propuesto	Razón del cambio	Modulos que afecta	Alternativas	Criterios de Aceptación de Solicitud	Estado de Solicitud	Tipo de Cambio	Responsables	Fecha Inicio de Cambio	Código de Plan de Cambio
003															

Anexo 26. Clasificación de Cambio

	CLASIFICACIÓN DE CAMBIO	CÓDIGO: F03–PM03
		VERSIÓN: 01
		FECHA: 14/01/21

Este documento interno permitirá el registro de la información necesaria para continuar con el proceso del cambio, en estos campos se precisara básicamente la información personal del solicitante para el posterior contacto del avance del cambio, el nombre del proyecto del cual se está realizando el cambio y la elección mediante un (x) el tipo de cambio correspondiente con respecto a la evaluación de la solicitud de cambio y asimismo el origen de la solicitud y su prioridad del cambio.

1. DATOS ESPECIFICOS	
Fecha de registro:	Fecha de solicitud del cambio:
Nombre del solicitante:	
Cargo:	Correo:
Nombre del Proyecto:	

2. DATOS GENERALES	
Tipo de cambio: ☐ Estándar ☐ Normal ☐ Emergencia	
Origen de la solicitud del cambio: ☐ Solicitud de Mejora ☐ Cambio por tendencia tecnológica ☐ Falla ☐ Cambio en política o regulación	Prioridad: ☐ Critica ☐ Alta ☐ Media ☐ Baja

Validado por:

Jefe de proyecto

Revisado por:

Gerente de Operaciones

Anexo 27. Plan de Cambio

	PLAN DE CAMBIO	CÓDIGO: F04–PM03
		VERSIÓN: 01
		FECHA: 14/01/21

Este documento permitirá detallar la información que se requiera para dar solución a la petición del cambio que presentó el solicitante.

Nombre del Proyecto
xxxxxxxxxx
Objetivo
xxxc

Roles de Gestión de Cambio		
Nombre del rol	Responsabilidad	Niveles de Autoridad

Herramientas de Gestión de Cambios: Describir con qué herramientas se cuenta para operar el cambio	
Software	
Formatos	Solicitud de Cambios
Otros	

Plan de Actividades: Se realiza un cronograma indicando, mediante el sombreado de celdas, el tiempo que nos tomará concluir cada una de las actividades.

(Para el sombreado de tiempos generalmente se utiliza el color azul para el tiempo establecido inicialmente, el color verde si la acción se realizó en tiempo y el color rojo para indicar si hubo algún contratiempo.)

Análisis de Riesgos

Para realizar el análisis de riesgos se debe realizar una identificación preliminar, en la cual se analizaron los tipos de riesgos que podrían existir:

Riesgos relativos a BITNESS CORP S.A.C.
La alta gerencia está comprometida con el proyecto
La solución tiene claros beneficios para BITNESS CORP. S.A.C.
El proyecto está alineado a la estrategia de la Empresa

Riesgos relativos a las organizaciones participantes del proyecto (clientes)
¿Se poseen experiencias anteriores de trabajo entre las organizaciones participantes del proyecto? ¿Se conocen las lecciones aprendidas de dichas experiencias
El proyecto está directamente alineado a la estrategia de BITNESS CORP. S.A.C. y las partes que intervienen.
Está claramente definida y comunicada la estrategia para todas las partes del proyecto

Riesgos respecto a factores tecnológicos
Se posee experiencia con tecnologías similares en el Estado. Se poseen las lecciones aprendidas de estas experiencias
Se posee experiencia con tecnologías similares a nivel Nacional. Se poseen las lecciones aprendidas de estas experiencias
El equipo técnico de BITNESS CORP. S.A.C. posee experiencia en proyectos de este.

Riesgo relativos al proveedor de la solución
Existen proveedores en plaza con conocimiento y experiencia en las tecnologías del proyecto
Se posee experiencia con los proveedores candidatos. Se tiene acceso a las lecciones aprendidas de dichas experiencias
El proveedor ha producido software o brindado un servicio similar al necesario al del proyecto anteriormente

Riesgo relativos a la gestión del proyecto
Los objetivos del proyecto están definidos
El proyecto está claramente definido en todas sus etapas
Están claramente definidos y comunicados los roles en el proyecto

Representa un Riesgo (SI/NO/NO APLICA)	Riesgos Identificados	Impacto si Ocurre (ALTO/BAJO/NO APLICA)

Luego de realizar la identificación preliminar se realiza la identificación con la cual se trabajara:

	PLAN DE CAMBIO	CÓDIGO: F04–PM03 VERSIÓN: 01 FECHA: 14/01/21

ID Riesgo	Nombre	Descripción	Clasificación / Categoría	Condiciones (Causa)	Consecuencias (Resultado Potencial)	Destinatario (Quién o quienes quedan expuestos ante la consecuencia de riesgo

Plan de Pruebas

La finalidad del plan de pruebas es entregar los pasos a seguir para la aplicación correcta de las estrategias y pruebas necesarias.

1. DATOS GENERALES

Producto	Clasificación
Software de Requisitos	Sistema de Gestión de Requisitos
Documento de Evaluación relacionados	
Equipo de Evaluación	
Responsable del equipo evaluador	

1. ALCANCE DE LAS PRUEBAS

A continuación se presentan los módulos del sistema representados en cuadros, cada uno con sus requerimientos de prueba bien definidos a cabo con éxito.

Cuadro 1: Modulo 1

Componentes a ser aprobados	Sub Módulos a realizar las pruebas
Objetivo de las pruebas	-
Detalle del orden de ejecución de los componentes	Ordenar de manera independiente

2. ENTORNO Y CONFIGURACIÓN DE PRUEBAS

Para el proceso de pruebas se requiere la disponibilidad de los siguientes entornos, a saber:

3.1. Equipo de Prueba

a. Servidor Virtual:
b. Sistema Operativo:
c. Procesador:
d. Disco duro:
e. Memoria RAM:

3.2. Base de Datos de Prueba

a. Base de Datos:
b. Servidor BD:
c. Datos: Aleatorios

3.3. Criterios de aprobación/rechazo

Criterios	Descripción
Aprobado	Se aprobará el producto o servicio con un 100% de las pruebas ejecutadas pero con un 90% de aceptación.Esto quiere decir que el 90% de las pruebas deben ser exitosas y sin errores. En el restante 10% pueden existir errores medios o bajos, pero no graves
Rechazado	En caso de ocurrir que el producto o servicio no cumpla con el nivel exigido, el producto o servicio se rechaza por completo.

Anexo 28. Manual de la 3° Oportunidad de Mejora

	CONTROL DE CAMBIOS PARA EL DESARROLLO DE SISTEMAS	Código: MP–PM03
		Versión:01
	MANUAL DEL PROCESO	Emisión:14/01/21
		Página: 1 de 14

ÍNDICE

1. OBJETIVOS

El propósito de este documento es describir el proceso de "**Control de cambios para el desarrollo de sistemas**", con la finalidad de asegurar el cumplimiento del proceso y su adecuada ejecución. El proceso considera el control de cambios adecuado para el proceso de desarrollo del sistema.

2. ALCANCE

El alcance del proceso de "**Control de cambios para el desarrollo de sistemas**", comprende desde la solicitud del cambio hasta la gestión de la aprobación del cambio. Además, se considera la participación activa del Gerente de operaciones, Jefe de Proyecto e involucrados.

El presente manual está dirigido a todo el personal del área de operaciones de la empresa BITNESS CORP. S.A.C.

3. DEFINICIONES

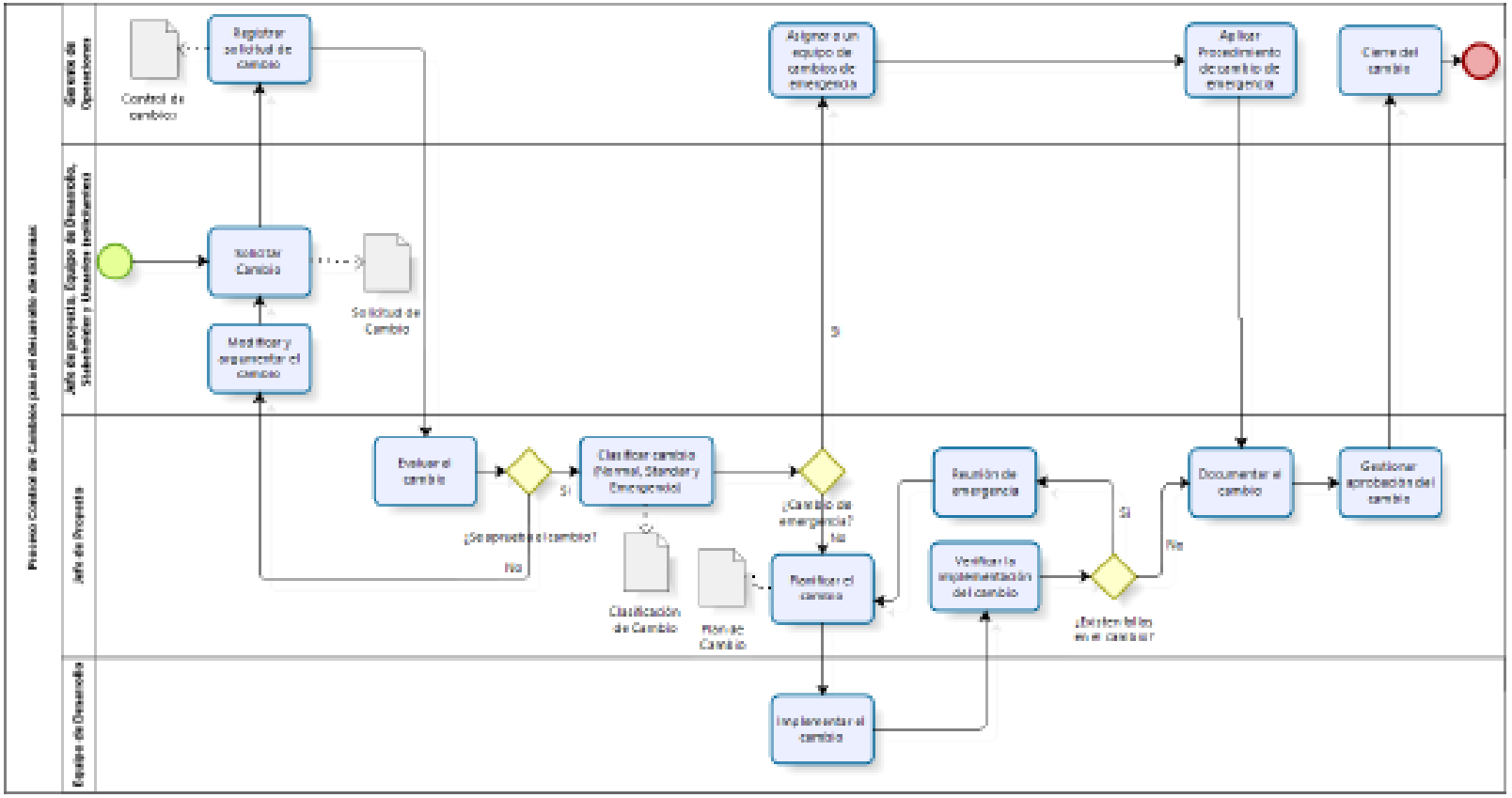
- ***Cambio estándar:*** Es todo cambio ejecutado en el desarrollo de un sistema cuyo riesgo de ejecución es bajo, debe ser documentado.
- ***Cambio normal:*** Es toda modificación realizada en el desarrollo de un sistema de carácter temporal o permanente. Este tipo de cambios deben ser pre aprobado, requiere análisis de riesgos, impacto, beneficios costo.
- ***Cambio de emergencia:*** Es todo cambio que de no realizarse afectará negativamente al sistema influyendo en la prestación de servicios y la operación del cliente. Este debe ser revisado y aprobado por el equipo de cambios de emergencia y documentado posteriormente a su ejecución.
- ***Control de cambios:*** Registro organizado de las modificaciones a realizarse durante el desarrollo de un sistema y la ejecución de este.
- ***Equipo de cambios de emergencia:*** Personal capacitado para actuar con rapidez ante una situación no prevista, mitigando los errores que afectarían negativamente a los usuarios del sistema.
- ***Solicitante de cambio:*** Es la persona que solicita y registra el cambio, puede ser un usuario o integrante del Equipo de Desarrollo.

- ***Gerente de Operaciones:*** Es encargado del equipo de desarrollo en BITNESS CORP. S.A.C. y en el proceso es el encargado de registrar los cambios del sistema y actuar ante un cambio de emergencia.
- ***Jefe del proyecto:*** Es el líder del proyecto, en el proceso es el que realiza la mayor cantidad de actividades ya que cuenta con la función de clasificar el cambio, planificarlo, verificarlo entre otras actividades importantes en el control de cambios.
- ***Equipo de Desarrollo:*** Son los expertos en el desarrollo de los sistemas, su principal función en el proceso es implementar el cambio.

4. BASE LEGAL Y NORMATIVA

- ISO 27002:2015, 14 Adquisición, desarrollo y mantenimiento de los sistemas de información
- Reglamento Interno de Trabajo de BITNES CORP. S.A.C.

5. DIAGRAMA DE PROCESOS



6. PROCEDIMIENTOS

N°	ACTIVIDAD	RESPONSABLE	ENTRADAS	TAREAS	SALIDAS
1	Solicitar cambio	Solicitante de cambio	Necesidad de cambio.	Identificar las características de la necesidad: (tecnológica, cambio en el proceso, etc.)	Solicitud de Cambio
				Llenar el formato de solicitud de cambio con los siguientes campos: Anexo **F01–PM03** • Nombre del solicitante • Correo del solicitante • Naturaleza del cambio • Nombre del proyecto • Descripción del cambio propuesto • Razón del cambio (Justificación) • Módulos que afectan • Alternativa	
				Enviar el formato de solicitud de cambio al Gerente de Operaciones	

2	Registrar cambio	Gerente de Operaciones	Solicitud de cambios	Recepcionar solicitud de cambio Verificar si tiene la información necesaria para realizar el cambio Registrar la solicitud de cambio en un formato Excel con los siguientes campos. Anexo **F02–PM03** • Código de formato • Nombre del solicitante • Correo del solicitante • Naturaleza del cambio • Fecha • Nombre del proyecto • Descripción del cambio propuesto • Razón del cambio (Justificación) • Módulos que afectan • Alternativa • Criterios de aceptación de solicitud • Estado de solicitud • Tipo de cambio • Responsables • Fecha inicio de cambio • Código del plan de cambio • Fecha fin de cambio	Solicitud de cambio registrada

				• Estado de cambio Programar la reunión con el Jefe de Proyecto para evaluar el cambio.	
3	Evaluar cambio	Jefe de Proyecto	Solicitud de cambio registrada	Asignar un comité para el cambio. Comité de cambio conformado: • Jefe de proyecto • Analista Evaluar la solicitud de cambio en un periodo de 24 horas. (Aprobado o Denegado) Tomar una decisión: • Si se aprueba el cambio se procede a la actividad 5. • Si no se aprueba el cambio va a la actividad 4. Informar el estado de la solicitud de cambio al solicitante mediante un correo electrónico.	Solicitud de cambio aprobada o denegada
4	Modificar y argumentar el cambio	Solicitante del cambio	Observaciones	Analizar las Observaciones Subsanar las observaciones en un periodo de 24 horas.	Solitud de Cambio modificado

				Solicitar cambio	
5	Clasificar cambio (Normal, Estándar y Emergencia)	Jefe de Proyecto	Solicitud de cambio aprobada	Analizar el tipo de cambio con el comité de cambio: Normal, Estándar o Emergencia. Cambio Estándar: Cuyo carácter de riesgo es bajo. • Ejm: es cuando no afecta al sistema. (cambio de mouse, monitor, etc.), son cambios materiales. Cambio Normal: Realizan el procedimiento de cambio, necesitan ser aprobados y si afecta al sistema. • Ejm: (migrar los servicios en nube, adquirir un servicio, etc.) Cambio de Emergencia: Tiene un impacto de urgencia, requieren ser evaluados con rapidez. . • Ejm: (falla de servidor primario, parche de emergencia para vulnerabilidades, etc.)	Tipo de cambio identificado documentado

				Identificar el tipo de cambio y documentarlo con los siguientes campos: Anexo **F03–PM03** • Fecha de registro • Fecha de solicitud de cambio • Nombre del solicitante • Cargo • Correo • Nombre del proyecto • Tipo de cambio • Origen de la solicitud de cambio • Prioridad • Validado por jefe de proyecto • Revisado por Gerente de Operaciones	
6	Planificar el cambio	Jefe de Proyecto	Tipo de cambio identificado: normal o éstandar	Elaborar el plan de cambio considerando los siguientes campos: Anexo **F04–PM03** • Nombre de Proyecto • Objetivo • Roles • Herramientas • Plan de actividades • Análisis de riesgos • Plan de pruebas	Plan de cambio

8	Implementar el cambio	Equipo de Desarrollo	Plan de cambio	Convocar a una reunión a todo el equipo de desarrollo. • Jefe de Proyecto • Analista • Programador Analizar el plan de cambio Programar la implementación Ejecutar el plan de cambio	Plan de cambio implementado
9	Verificar la implementación del cambio	Jefe de Proyecto	Plan de cambio implementado	Analizar los resultados de la implementación Tomar una decisión: • Si la implementación es aprobada se procede a la actividad 13. • Si no es aprobada la implementación procede a la actividad 10.	Implementación del cambio aprobada
10	Reunión de emergencia	Jefe de Proyecto	Fallas en el cambio	Convocar a una reunión al Gerente de Operaciones. Dialogar las fallas del cambio. Subsanar las fallas del cambio	Corrección de la implementación del cambio.

				Convocar a una reunión con el jefe de proyecto. Asignar Consejo Consultor para Cambios de Emergencia. Está conformado por: • Gerencia General • Jefe de proyecto • Contador (Dependiendo del cambio)	
11	Aplicar procedimiento de cambio de emergencia	Gerente de Operaciones	Consejo Consultor para Cambios de Emergencia	Convocar a una reunión con el Consejo Consultor para Cambios de Emergencia Analizar el cambio juntamente con el Consejo Consultor para Cambios de Emergencia Resolver el cambio juntamente con el Consejo Consultor para Cambios de Emergencia	Cambio de emergencia resuelto.
12	Documentar el cambio	Jefe de Proyecto	• Implementación aprobada • Cambio de emergencia resuelto.	• Registrar la información de la implementación de cambios en el formato de control de cambios.	Información registrada

13	Gestionar aprobación del cambio	Jefe de Proyecto	Información de resultados del cambio	Convocar a una reunión al Gerente de operaciones para firmar el documento de cambio	Documento de cambio firmado
14	Cierre del cambio	Gerente de Operaciones	Documento de cambio firmado	Registrar el estado del cambio	Estado de Cambio

7. INDICADORES Y EVIDENCIAS DE CONTROL

INDICADORES

No	NOMBRE	UM	META	RESPONSABLE	FRECUENCIA	FUENTE
01	Cumplimiento	%	100	Gerente de Operaciones	En cada actividad del proceso	–
02	Número de cambios programados / implementados	%	100	Gerente de Operaciones	Al término del proceso	-
03	Número de cambios exitosos / ejecutados	%	100	Gerente de Operaciones	Al término del proceso	-

EVIDENCIAS DE CONTROL

No	NOMBRE	RESPONSABLE	FRECUENCIA
01	Solicitud de cambio	Solicitante	Durante todo el proyecto
02	Control de cambio	Gerente de Operaciones	Durante todo el proyecto
03	Clasificación de cambio	Jefe de Proyecto	Durante todo el proyecto
04	Plan de cambio	Jefe de Proyecto	Durante todo el proyecto

8. RIESGOS

No	NOMBRE	PLAN DE ACCIÓN
01	Incumplimiento del control de cambios	Capacitación
02		

9. FORMATOS

Nº	CODIGO	DESCRIPCION
01	FO1–PM03	Solicitud de cambio
02	FO2–PM03	Control de cambio
03	FO3–PM03	Clasificacion de cambio
04	FO4–PM03	Plan de cambio

CONTROL DE CAMBIOS

Nº Versión	DESCRIPCION	FECHA

10. ANEXOS

- Doc. Solicitud de cambio
  https://docs.google.com/document/d/1pXccubfigwXVQUZIxc8PHv13oi7nuG3bd6jP87LvFno/edit
- Control de cambio
  https://docs.google.com/spreadsheets/d/1CHUc627yAWtfaMcfwXyvpVcvGDlUoACkxBP3UAdgIXA/edit?usp=drive_web&ouid=102522498972365542887
- Clasificación de cambio
  https://docs.google.com/document/d/1JIKNBiXXZIVvtOmjc80MtCRkdPG3dlxEsg8YcU7133E/edit
- Plan de cambio
  https://docs.google.com/document/d/1TaknuYtaXmA-IufL4dWjswUyCNvyF6OYuVYI3Yv3-A8/edit

Anexo 29. Formato de Contrato de Confidencialidad

CONTRATO DE CONFIDENCIALIDAD

Conste el presente contrato de Confidencialidad que suscriben de una parte la Empresa BITNESS CORP. SAC con RUC 20602895506 con dirección en
epresentada por su Gerente General de Operaciones ING. ANDRES ROSAS HUAMAN con N° DNI 77477509 a quien se les llamara LA EMPRESA y de la otra EL PROMITENTE en los términos y condiciones siguientes:

PRIMERO.

OBJETO DEL CONTRATO

El objeto del contrato es de garantizar la confidencialidad del presente Proyecto por lo que se hace necesario la firma de un acuerdo que garantice niveles de confianza entre las partes.

Las partes, anteriormente citadas, suscriben el presente acuerdo de Confidencialidad con el fin de establecer el procedimiento que regirán la custodia y la no transmisión a terceros de la información distribuida entre las partes, así como los derechos, responsabilidades y obligaciones inherentes en calidad de remitente, Propietario y «Destinatario» de la Referida información.

SEGUNDO.

DE LAS PARTES

Derechos de la empresa

La empresa BITNESS CORP S.A.C es la entidad encargada de la PRODUCCION DE SOTWARE y tendrá derechos sobre los conceptos, ideas, conocimientos, técnicas, diseños, dibujos, borradores, diagramas, textos, modelos, muestras, bases de datos contenidos en el CONTRATO DE CONFIDENCIALIDAD contenido en el arriendo, venta, cesión de uso, de las aplicaciones, programas, marcas, logotipos, así como cualquier información de tipo técnico, industrial, financiero, publicitario, de carácter personal o comercial de cualquiera de las partes, esté o no incluida en la solicitud de oferta presentada, independientemente de su formato de presentación o distribución, y aceptada por los «Destinatarios».

La obligación de los destinatarios es el de conservar el bien, no modificarlo, y no divulgarlo a ninguna persona natural, o entidad jurídica, sobre su origen de producción, valor, e identificación.

Derechos de los promitentes

Tiene derecho a solicitar cualquier información con respecto de las características del producto.

TERCERA.

INFORMACIÓN CONFIDENCIAL

Las partes acuerdan que cualquier información relativa a sus aspectos financieros, comerciales, técnicos, y/o industriales suministrada a la otra parte como consecuencia de la solicitud de Oferta para el desarrollo del presente proyecto objeto del contrato, sea oral, escrita, en soporte magnético o en cualquier otro mecanismo informático, gráfico, o de la naturaleza que sea tendrá consideración de información confidencial esta información, y sus copias y/o reproducciones tendrán la consideración de «Información propia» y por tal información confidencial .

Las partes exponen que las negociaciones llevadas a cabo (o el proyecto a desarrollar en conjunto) entre el titular de la información descrita a continuación, en adelante el Divulgador, y el receptor de la misma, en adelante el Receptor, relativas a cualidades financieras, planes de negocios, información personal, dibujos, ejemplos y prototipos de artefactos, demostraciones, secretos comerciales, información técnica, sistemas de computación y software, resultados de investigaciones, listas de clientes otros datos en forma oral o escrita. Relacionada con la tecnología, ya sea que dicha comunicación se produzca verbalmente, visualmente, o mediante

demostraciones o cualquier otro medio, tanto en forma de dibujos, modelos, documentos impresos, y/o formato de archivos electrónicos o de cualquier otra manera, en adelante la Información son inherentes al presente CONTRATO DE CONFIDENCIALIDAD PARA LA EMPRESA BITNESS CORP. S.A.C. y su divulgación es materia de resolución de contrato e indemnización de daños.

CUARTA.
INFORMACION QUE NO ES PARTE DEL CONTRATO

No se entenderá por «Información propia», ni recibirá tal tratamiento aquella información que sea de conocimiento público en el momento de su notificación al «Destinatario» después de producida la notificación alcance tal condición de pública, Así, como la divulgada por su legítimo creador.

QUINTO.

CUSTODIA Y NO DIVULGACIÓN

Las partes consideran confidencial la «Información propia» la cual nos e puede divulgar y pactan su guarda y custodia estricta, así como a su no divulgación o suministro, ni en todo ni en parte, a cualquier tercero sin el previo, expreso y escrito consentimiento de «Fuente». Tal consentimiento no será necesario cuando la obligación de suministrar o divulgar la «Información propia» sea impuesta por Ley en vigor o Sentencia Judicial Firme .

SEXTO.

CARACTERISTICA DE LA «INFORMACIÓN PROPIA».

La información propia será de carácter secreto y confidencial para los custodios de la información que la empresa designe.

SEPTIMO.

RESPONSABILIDAD EN LA CUSTODIOS DE LA "INFORMACIÓN PROPIA"

La «Información propia» podrá ser dada a conocer por el «Destinatario» o sus directivos y/o sus empleados, sin perjuicio de que el «Destinatario» tome cuantas medidas sean necesarias para el exacto y fiel cumplimento del presente Acuerdo, debiendo necesariamente informar a unos y otros del carácter secreto, confidencial, o restringido de la información que da a conocer, así como da existencia del presente acuerdo. Así mismo, el «Destinatario» deberá dar a sus directivos y/o sus empleados, las directrices e instrucciones que considere oportunas y convenientes a los efectos de mantener el secreto, confidencial, o restringido de la información propia de la «Fuente».

El destinatario deberá advertir a todos sus directivos, empleados, etc., que de acuerdo con lo dispuesto en este acuerdo tengan acceso a la «Información propia», de las consecuencias y responsabilidades en las que el «Destinatario» puede incurrir por la infracción por parte de dichas personas.

Toda entrega de documentación sea escrita o virtual deberá ser suscrita con un cargo de notificación. Sin perjuicio de lo previsto en los párrafos anteriores, cada parte será responsable tanto de la conducta de sus directivos y/o empleados como de las consecuencias que de ella pudieran derivarse de conformidad con lo previsto en el presente Acuerdo.

OCTAVO.

DEL INCUMPLIMIENTO

Incumplimiento de las obligaciones de confidencialidad plasmadas en este documento, por cualquiera de las partes, sus empleados o directivos, facultará a la otra a reclamar por la vía legal que estime más procedente, a la indemnización de los daños y perjuicios ocasionados, incluido el lucro cesante, daño moral, y daño emergente.

NOVENO.

DURACIÓN DE ACUERDO DE CONFIDENCIALIDAD

Ambas partes acuerdan mantener el presente Acuerdo de Confidencialidad, en un año Después de terminar sus relaciones comerciales.

DÉCIMO.

LEGISLACIÓN APLICABLE

Se aplicara lo establecido en el Código civil de 1984, así como supletoriamente el código procesal civil. En caso de controversia se fijan los juzgados y tribunales del departamento de Lima.

Estando las partes de acuerdo en cada uno de los artículos del presente contrato lo suscriben en señal de conformada y aceptación el DIA..... DEL MES DE .....EN LA CIUDAD DE LIMA CAPÌTAL DEL PÈRU.

LA EMPRESA **EL PROMITENTE**

Anexo 30. Acta de Aceptación de la 1ª Oportunidad de Mejora

Lima, 07 de Septiembre de 2020

CONSTANCIA DE ACEPTACIÓN DE DISEÑO DE PROCESO

Por medio de la presente la empresa BITNESS CORP. S.A.C. representada por Imer Andrés Rosas Huamán, identificado con DNI Nº 77477509, da constancia de la ACEPTACIÓN del diseño del proceso "Gestión de Requisitos de Seguridad para el desarrollo de sistemas", desarrollado por Bach. Gaby Alvarado Limaymanta y Bach. Miryam Raquel Sánchez Torre.

Vale resaltar que el diseño del proceso Gestión de requisitos de seguridad para el desarrollo de sistemas fue desarrollado con la participación activa de los principales interesados de la empresa BITNES CORP SAC y validado por su representante. La implementación, ejecución y seguimiento queda a responsabilidad de los administradores de la empresa según lo vean conveniente.

Se recomienda que la implementación y ejecución del proceso se lleve a cabo bajo las condiciones y características estipuladas en el Documento del Proceso.

Saludos cordiales,

Gaby Alvarado L.

Miryam Sánchez T.

Imer Andres Rosas H.
Representante

Anexo 31. Acta de Aceptación de la 2ª Oportunidad de Mejora

Lima, 03 de Diciembre del 2020

CONSTANCIA DE ACEPTACIÓN DE DISEÑO DE PROCESO

Por medio de la presente la empresa BI1NESS CORP. S.A.C. representada legalmente por Andrés Rosas Huamán, identificado con DNI Nº 77477509, da constancia de la ACEPTACIÓN del diseño del proceso "Adquisición formal del producto o servicio asegurando la calidad", desarrollado por Bach. Gaby Alvarado Limaymanta y Bach. Miryam Raquel Sánchez Torre.

Vale resaltar que el diseño del proceso Adquisición formal del producto o servicio asegurando la calidad fue desarrollado con la participación activa de los principales interesados de la empresa BI1NES CORP SAC y validado por su representante legal. La implementación, ejecución y seguimiento queda a responsabilidad de los administradores de la empresa según lo vean conveniente.

Se recomienda que la implementación y ejecución del proceso se lleve a cabo bajo las condiciones y características estipuladas en el Documento del Proceso.

Saludos cordiales,

Gaby Alvarado L.

Miryam Sánchez T.

Andrés Rosas H.
Representante legal

Anexo 32. Acta de Aceptación de la 3ª Oportunidad de Mejora

Lima, 13 de Enero del 2021

TESISTAS:

Gaby M. Alvarado Limaymanta

Miryam R. Sánchez Torre

Por medio de la presente, **BITNESS CORP. S.A.C.**, nos permite notificar la **ACEPTACIÓN** del tercer proceso de **"Control de Cambios"** a llevarse a cabo por las tesistas **Gaby Alvarado Limaymanta y Miryam Raquel Sánchez Torre** a partir del **13 de enero del 2021**.

Como se indicó en la presentación del tercer proceso, el **Gerente de Operaciones Andrés Rosas Huamán**, estará a cargo de la implementación, ejecución y seguimiento del proceso de "Control de Cambios". Por su lado, la empresa BITNESS CORP. S.A.C., se compromete a aplicar el proceso en base a lo propuesto.

Esperamos que la ejecución del proceso se lleve a cabo bajo las condiciones y características estipuladas en el Documento del Proceso.

Saludos cordiales,

Gaby Alvarado L.	Miryam Sánchez T.	Andres Rosas H.
(Tesista)	(Tesista)	(G. de Operaciones en BITNESS CORP. S.A.C.)

Anexo 33. Acta de Aceptación de la 4ª Oportunidad de Mejora

CONSTANCIA DE ACEPTACIÓN DEL FORMATO DE CONTRATO DE CONFIDENCIALIDAD

Por medio de la presente la empresa BITNESS CORP. S.A.C. representada legalmente por Andrés Rosas Huamán, identificado con DNI N° 77477509, da constancia de la ACEPTACIÓN del formato del Contrato de Confidencialidad, desarrollado por Bach. Gaby Alvarado Limaymanta y Bach. Miryam Raquel Sánchez Torre.

Vale resaltar que el Contrato de Confidencialidad fue desarrollado con la participación activa de los principales interesados de la empresa BITNESS CORP. S. A. C. y validado por su representante legal. La implementación, ejecución y seguimiento queda a responsabilidad de los administradores de la empresa según sea conveniente.

Se recomienda que la implementación y ejecución del Contrato de Confidencialidad se lleve a cabo bajo las condiciones y características estipuladas en la ISO 27002:2015.

Saludos cordiales,

Gaby Alvarado L.	Miryam Sánchez T.	Andrés Rosas H.
Tesista	Tesista	Representante legal

Anexo 34: Guía de Entrevista Implementada a la empresa Miguelito S.A.C.

	GUÍA DE ENTREVISTA	CÓDIGO: F01–PM01 VERSIÓN: 01 FECHA: 07/09/20

PROGRAMACIÓN DE LA ENTREVISTA	
Modalidad: ( ) Presencial (x) Virtual	
Datos del Entrevistador	
Nombre: Andres Imer Rosas Huaman	
Cargo: Gerente de Operaciones	
Datos del Entrevistado:	
Nombre: Gerente de Corporación Miguelito S.A.C.	
Cargo:	
Correo:	**Celular:**
Programación	
Fecha:	**Hora Inicio: 9:00 a.m.**
Lugar: Virtual	**Hora Fin: 10:00 a. m.**

Preguntas Generales acerca del Departamento

- ¿De qué trata su empresa?
- ¿Cómo está organizada la empresa?
- ¿Con cuántos empleados cuenta?
- ¿Cuenta con más de una sucursal?
- ¿Cuáles son los procesos existentes, incluyendo cualquier diagrama o procedimientos que hayan creado?
- ¿Cómo se comunican con los otros departamentos?
- ¿Cómo se comunican con los otros sistemas, servicios o clientes?
- ¿Cuáles son los actuales y futuros reglamentos y estándares de servicio al cliente que deben cumplir?
- ¿Qué herramientas de software se usan en la empresa?
- ¿Trabajan con algún tipo de estándar / manual de estilo de código?
- ¿Con qué tecnologías de base de datos trabaja la empresa?
- ¿Qué sistemas operativos se usan en la empresa?
- ¿Existen restricciones a la hora de usar alguna herramienta o algún software?

	GUÍA DE ENTREVISTA	CÓDIGO: F01–PM01
		VERSIÓN: 01
		FECHA: 07/09/20

Preguntas Generales acerca del Procedimiento

- ¿Qué se necesita que haga el sistema?
- ¿Cómo comienza su procedimiento?
- ¿Qué documentos solicita al participante?
- ¿Recibe información de otros departamentos?
- ¿Cómo termina el procedimiento?
- ¿A quién le envía los resultados del proceso cuando termina su parte?
- ¿Con qué sistema trabajan hoy en día?
- ¿Qué es lo más difícil en el proceso actual y que cosa piensan que puede ser cambiada para mejor?
- ¿Existe algún requerimiento que se necesite implementar?
- ¿Cuál es el software que usan para realizar su trabajo?
- ¿Existe otro software que usan durante el día?
- ¿Reescriben información de un sistema a otro? ¿Cual es esta información?
- ¿Qué recomienda que se debe mejorar en el proceso?

Anexo 35: Acta de Reunión Implementada en la empresa Miguelito S.A.C.

	ACTA DE REUNIÓN	CÓDIGO: F02–PM01
		VERSIÓN: 01
		FECHA: 07/09/20

DATOS GENERALES	
Razón Social: Corporación Industrial Miguelito	**Contacto:**
RUC: 20544763025	**Cargo:** Stakeholder
Fecha: 10/12/20	**Celular:** -
Objetivos de la Reunión: Requisitos del sistema	**Hora Inicio:** 9:00 a.m
	Hora Fin: 9:30 a.m
Responsable de la Reunión: Andres Imer Rosas Huaman	
Modalidad: ( ) Presencial (x)Virtual	**Categoría:** (x)Interna ( )Externa

AGENDA
1. Analizar requisitos funcionales 2. Identificar requisitos de seguridad relacionado al sistema 3. Identificar requisitos de seguridad relacionado durante el proceso de desarrollo

CONCLUSIONES - ACUERDOS
Se acordó con la aprobación de los miembros presentes: 1. Clasificar los requisitos de seguridad relacionado al sistema y durante el proceso de desarrollo en base de los tres pilares de la seguridad de la información: confidencialidad, disponibilidad e integridad.

Anexo 36: Clasificación de los Requisitos Funcionales y No Funcionales del Sistema Miguelito

	REQUISITOS FUNCIONALES Y NO FUNCIONALES	CÓDIGO: F03-PM01
		VERSIÓN: 01
		FECHA: 10/12/20

DATOS GENERALES	
Razón Social: Corporación Industrial Miguelito S.A.C	**Hora Inicio:** 9:00 a.m
RUC: 20544763025	**Hora Fin:** 9:30 a.m
Modalidad: ( ) Presencial (x)Virtual	**Fecha:** 11/12/20

En el siguiente formato se describirán los requisitos funcionales que exige el cliente para el desarrollo del software:

Código	Requisitos Funcionales
RF001	Si se registra un nuevo código, el sistema debe notificarlo como una novedad.
RF002	El sistema no debe permitir registrar un correo inexistente.
RF003	El sistema debe contar con dos casilleros uno marcado con un check predefinidamente con el mensaje "SI, ACEPTO BRINDAR MIS DATOS PERSONALES Y ESTOY DE ACUERDO CON LOS TÉRMINOS Y CONDICIONES" y el otro no marcado donde diga "acepto y quiero recibir promociones de la marca". En la frase "términos y condiciones" el cliente puede dar click y se le desglosa una ventana emergente sin url donde aparece una imagen con los términos y condiciones.
RF004	El sistema no debe guardar sus datos cuando un cliente compra se registra como invitado.

En el siguiente formato se describirán los requisitos no funcionales que exige el cliente para el desarrollo del software:

Tipos Requisitos no funcionales	Código	Clasificación	Descripción
Funcionalidad	RNF001	Seguridad	• La nueva información registrada(código del producto) debe estar disponible a los usuarios que interactúen con el sistema.
	RNF002		• El sistema debe mantener la integridad de la información del correo electrónico mediante una estructura.
	RNF003		• Los permisos de acceso para

			términos y condiciones deberán ser actualizados por el administrador de la página.
	RNF004		• El sistema debe limpiar los datos temporales del cliente(invitado) al finalizar la compra.
Usabilidad	RNF005	Entendimiento	• El sistema debe contar con un manual de usuario estructurado adecuadamente
	RNF006		• El sistema debe contar con un módulo de ayuda en línea
	RNF007	Desempeño	• El sistema debe tener un tiempo de respuesta inmediata.
	RNF008	Atracción	• El sistema debe tener gráficos visualmente estéticos.

Anexo 37: Requisitos No Funcionales del Sistema Miguelito

	REQUISITOS NO FUNCIONALES DE SEGURIDAD	CÓDIGO: F04–PM01 VERSIÓN: 01 FECHA: 07/09/20

DATOS GENERALES	
Razón Social: Corporación Industrial Miguelito	**Modalidad:** ( ) Presencial (x)Virtual
RUC: 20544763025	
Fecha: 12/12/20	**Categoría:** (x)Interna ( )Externa
Objetivos de la Reunión: Asignar un responsables a cada requisito de seguridad del producto	**Hora Inicio:** 9:00 a.m
	Hora Fin: 9:30 a.m
Responsable de la Reunión: Andres Imer Rosas Huaman	

CÓDIGO	NOMBRE	DESCRIPCIÓN	RESPONSABLE
RNF01	Seguridad	La nueva información registrada(código del producto) debe estar disponible a los usuarios que interactúen con el sistema.	Programador
RNF02		El sistema debe mantener la integridad de la información del correo electrónico mediante una estructura.	
RNF03		Los permisos de acceso para términos y condiciones deberán ser actualizados por el administrador de la página.	
RNF04		El sistema debe limpiar los datos temporales del cliente(invitado) al finalizar la compra.	

Anexo 38: Inventario de Requisitos de Seguridad del Sistema Miguelito

	INVENTARIO DE REQUISITOS DE SEGURIDAD (CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD)	CÓDIGO: F05–PM01 VERSIÓN: 01 FECHA: 07/09/20

DATOS GENERALES	
Razón Social: Corporación Industrial Miguelito	**Hora Inicio:** 11:00
RUC: 20544763025	**Hora Fin:** 11:30
Responsable de la Reunión: Luis Caro Galoc	**Fecha:** 13/12/20
Objetivos de la Reunión: Identificar los requisitos de seguridad en base a los tres pilares	
Modalidad: ( ) Presencial (x)Virtual	

El presente documento tiene como finalidad describir los requisitos de seguridad en base a los tres pilares de la seguridad de la información.

N °	Requisito de Seguridad	Tipos requisitos de seguridad	Nivel de complejidad	Prioridad
RNF01	La nueva información registrada(código del producto) debe estar disponible a los usuarios que interactúen con el sistema.	Disponibilidad	Alto	Alto
RNF02	El sistema debe mantener la integridad de la información del correo electrónico mediante una estructura.	Integridad	Alto	Alto
RNF03	Los permisos de acceso para términos y condiciones deberán ser actualizados por el administrador de la página.	Disponibilidad	Moderado	Alto
RNF04	El sistema debe limpiar los datos temporales del cliente(invitado) al finalizar la compra.	Disponibilidad	Alto	Alto

Anexo 39: Matriz de Trazabilidad

	MATRIZ DE TRAZABILIDAD	CÓDIGO: F07–PM01
		VERSIÓN: 01
		FECHA:07/09/20

ESTADO ACTUAL	
ESTADO	ABREVIATURA
Activo	AC
Cancelado	CA

DATOS GENERALES	
Razón Social	Corporación Industrial Miguelito S.A.C.
R.U.C.	20544783025
Fecha	13/12/20
Responsable	Luis Ciero Geloc - Analista
Modalidad de la Reunión	( ) Presencial (x)Virtual
Proyecto	Miguelito

NIVEL DE COMPLEJIDAD	
ESTADO	ABREVIATURA
Alto	A
Moderado	M
Bajo	B

ID	Descripción del requisito	Versión	Estado actual	Última fecha estado registrado	Nivel de complejidad	Objetivo del proyecto	Entregables (EDT)	Estrategia y escenarios de pruebas	Interesado (Stakeholder) dueño del requisito	Nivel de prioridad
001	La nueva información registrada(código del producto) debe estar disponible a los usuarios que interactúen con el sistema.	1	AC	13/12/20	A	Clasificar los requisitos de seguridad relacionado al sistema y durante el proceso de desarrollo en base de los tres pilares de la seguridad de la información: confidencialidad, disponibilidad e integridad.	Manual Técnico	Notificación del nuevo código del producto al usuario que interactua con el módulo del sistema.	Corporación Industrial Miguelito	ALTO
002	El sistema debe mantener la integridad de la información del correo electrónico mediante una estructura.	1	AC	13/12/20	A			Prueba unitaria (Ingreso de correos sin estructura y vacios).		ALTO
003	Los permisos de acceso para términos y condiciones deberán ser actualizados por el administrador de la página.	1	AC	13/12/20	M			Prueba unitaria(Ingreso como administrador).		ALTO
004	El sistema debe limpiar los datos temporales del cliente(invitado) al finalizar la compra.	1	AC	13/12/20	A		Capacitación	Pruebas unitarias (Realizar varios procesos de compra como invitado)		ALTO

Anexo 40: Requisitos de seguridad durante el proceso de desarrollo

	REQUISITOS DE SEGURIDAD DURANTE EL PROCESO DE DESARROLLO	**CÓDIGO: F0-PM01** **VERSIÓN:** 01 **FECHA: 07/09/20**

DATOS GENERALES	
Razón Social: Corporación Industrial Miguelito	**Hora Inicio:** 9:00
RUC: 20544763025	**Hora Fin:** 9:30
Modalidad: ( ) Presencial (x)Virtual	**Fecha:** 14/12/20

DATOS DEL PROYECTO	
Nombre del proyecto	Sistema Miguelito
Objetivo	Implementar los requisitos de seguridad relacionado al sistema y durante el proceso de desarrollo en base de los tres pilares de la seguridad de la información: confidencialidad, disponibilidad e integridad.
Alcance	La ejecución de los requisitos de seguridad, comprenden desde la primera etapa de elaboración hasta la transición del sistema, para la entrega de un producto de calidad. Los involucrados en la ejecución son todo el equipo de desarrollo y el stakeholder.
Cronograma	INICIO : 14/12/2020 FIN : 15/01/2021

	Confidencialidad	**Integridad**	**Disponibilidad**
Elaboración	Solo el equipo asignado debe tener conocimiento sobre el plan de trabajo Análisis de requerimientos no funcionales de seguridad	Las modificaciones se realizarán con previa autorización del Gerente de Operaciones. Mantener una estructura de trabajo que cumpla con patrones de seguridad.	Acceso de código sólo al rol programador
Ejecución	El programador debe mantener el código seguro sin ser divulgado	La estructura de trabajo propuesta no debe ser modificada sin autorización del jefe del proyecto.	El programador será encargado de realizar las pruebas necesarias al sistema
Transición	El gerente de operaciones será el encargado de entregar la documentación del sistema al Stakeholder.	Los módulos del sistema deben mantener la integridad de sus componentes contra los usuarios que no tengan acceso al sistema.	El gerente de operaciones dará acceso al rol correspondiente para la implementación del sistema

Anexo 41: Informe de acceso del equipo de desarrollo

	INFORME DE ACCESOS DEL EQUIPO DE DESARROLLO	**CÓDIGO: F09–PM01**
		VERSIÓN: 01
		FECHA: 07/09/20
DATOS GENERALES		
Razón Social: Corporación Industrial Miguelito		
RUC: 20544763025		
Fecha: 14/12/20		
Nombre del Proyecto: Sistema de Miguelito		

El presente documento permitirá establecer los accesos de la información teniendo en cuenta los tres pilares de la seguridad de la información:

Confidencialidad: Consiste en la capacidad de asegurar la información, delimitando los accesos de los miembros del equipo de desarrollo durante las etapas del proyecto.

Disponibilidad: Capacidad de garantizar que tanto el sistema como los datos van a estar disponibles para el equipo de desarrollo dependiendo del acceso de información que posean.

Integridad: Capacidad de garantizar que los datos no han sido modificados sin autorización desde su creación. La información que disponemos es válida y consistente. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos durante el desarrollo del sistema.

EMPLEADO	ROL	REQUISITOS A REALIZAR	ACCESO A MÓDULOS	ACCESO EN BASE A LOS TRES PILARES	REPORTAR A
Andres Rosas Huaman	Programador	Acceso de código sólo al rol programador	Todo el sistema	Disponibilidad	Gerente de Operaciones
Andres Rosas Huaman / Luis Caro		Realizar las pruebas necesarias al sistema		Disponibilidad	

Andres Rosas Huaman / Luis Caro	Programador	Las modificaciones del código se realizarán con previa autorización del Gerente de Operaciones.		Integridad	
Andres Rosas Huaman / Luis Caro	Programador	El programador debe mantener el código seguro sin ser divulgado		Confidencialidad	
Andres Rosas Huaman	Gerente de Operaciones	Dará acceso al rol correspondiente para la implementación del sistema		Disponibilidad	
Andres Rosas Huaman / Luis Caro	Analista /Programador	Solo el equipo asignado debe tener conocimiento sobre el plan de trabajo		Confidencialidad	
Andres Rosas Huaman	Gerente de Operaciones	Será el encargado de entregar la documentación del sistema al Stakeholder.		Confidencialidad	
Andres Rosas Huaman /Luis Caro	Analista / Programador	Mantener una estructura de trabajo que cumpla con patrones de seguridad.		Integridad	
Andres Rosas Huaman	Analista	Análisis de requerimientos no funcionales de seguridad.		Disponibilidad	
		La estructura de trabajo propuesta no debe ser modificada sin autorización del jefe del proyecto.		Integridad	
Luis Caro Galoc	Analista	Los módulos del sistema deben mantener la integridad de sus componentes contra los usuarios que no tengan acceso al sistema.		Integridad	

Estando los presentes de acuerdo con lo escrito, pasan a firmar para dar validez a este documento.

PARTICIPANTES			
N°.	**Nombre y Apellido**	**Función/Cargo**	**Firma**
1	Andres Rosas Huaman	Analista /Programador	
2	Luis Caro Galoc		

Anexo 42: Implementación contrato de confidencialidad

CONTRATO DE CONFIDENCIALIDAD

Conste el presente contrato de Confidencialidad que suscriben de una parte La empresa CORPORACIÓN INDUSTRIAL MIGUELITO SAC con RUC 20544763025 en domicilio fiscal en Jr. Antonio Bazo N° 776 Int. M17 (Centro Comercial El Marquez) Lima, Lima, La Victoria LA EMPRESA y la otra parte BITNESS CORP. SAC con RUC 20602895506 con dirección en Av. República de Colombia N° 791 Int. 791 Urb. Santa Cruz - Lima representada por su Gerente General de Operaciones ING. ANDRES ROSAS HUAMAN con N° DNI 77477509 a quien se les llamará PROMITENTE en los términos y condiciones siguientes:

PRIMERO.

OBJETO DEL CONTRATO

El objeto del contrato es garantizar la confidencialidad del presente **Proyecto Miguelito** por lo que se hace necesario la firma de un acuerdo que garantice niveles de confianza entre las partes.

Las partes, anteriormente citadas, suscriben el presente acuerdo de Confidencialidad con el fin de establecer el procedimiento que regirán la custodia y la no transmisión a terceros de la información distribuida entre las partes, así como los derechos, responsabilidades y obligaciones inherentes en calidad de remitente, Propietario y «Destinatario» de la información referida.

SEGUNDO.

DE LAS PARTES

Derechos de la empresa

La empresa Corporación Industrial Miguelito S.A.C. es una entidad dedicada a la fabricación de prendas de vestir , excepto prendas de piel y ventas al por mayor de productos textiles, prendas de vestir y calzados, la cual requiere servicios de tecnologías para mejorar su sistema actual.

La obligación de los destinatarios es el de conservar el bien, no modificarlo, y no divulgar a ninguna persona natural, o entidad jurídica, sobre su origen de producción, valor, e identificación.

Derechos de los promitentes

La empresa BITNESS CORP. S.A.C es la entidad encargada de la PRODUCCION DE SOTWARE y tendrá derechos sobre los conceptos, ideas, conocimientos, técnicas, diseños, dibujos, borradores, diagramas, textos, modelos, muestras, bases de datos contenidos en el CONTRATO DE CONFIDENCIALIDAD contenido en el arriendo, venta, cesión de uso, de las aplicaciones, programas, marcas, logotipos, así como cualquier información de tipo técnico, industrial, financiero, publicitario, de carácter personal o comercial de cualquiera de las partes,

esté o no incluida en la solicitud de oferta presentada, independientemente de su formato de presentación o distribución, y aceptada por los «Destinatarios».

Tiene derecho a solicitar cualquier información con respecto a las características del sistema a realizar.

TERCERA.

INFORMACIÓN CONFIDENCIAL

Las partes acuerdan que cualquier información relativa a sus aspectos financieros, comerciales, técnicos, y/o industriales suministrada a la otra parte como consecuencia de la solicitud de Oferta para el desarrollo del presente proyecto objeto del contrato, sea oral, escrita, en soporte magnético o en cualquier otro mecanismo informático, gráfico, o de la naturaleza que sea tendrá consideración de información confidencial esta información, y sus copias y/o reproducciones tendrán la consideración de «Información propia» y por tal información confidencial .

Las partes exponen que las negociaciones llevadas a cabo (o el proyecto a desarrollar en conjunto) entre el titular de la información descrita a continuación, en adelante el Divulgador, y el receptor de la misma, en adelante el Receptor, relativas a cualidades financieras, planes de negocios, información personal, dibujos, ejemplos y prototipos de artefactos, demostraciones, secretos comerciales, información técnica, sistemas de computación y software, resultados de investigaciones, listas de clientes otros datos en forma oral o escrita. Relacionada con la tecnología, ya sea que dicha comunicación se produzca verbalmente, visualmente, o mediante demostraciones o cualquier otro medio, tanto en forma de dibujos, modelos, documentos impresos, y/o formato de archivos electrónicos o de cualquier otra manera, en adelante la Información son inherentes al presente CONTRATO DE CONFIDENCIALIDAD PARA LA EMPRESA BITNESS CORP. S.A.C. y su divulgación es materia de resolución de contrato e indemnización de daños.

CUARTA.

INFORMACION QUE NO ES PARTE DEL CONTRATO

No se entenderá por «Información propia», ni recibirá tal tratamiento aquella información que sea de conocimiento público en el momento de su notificación al «Destinatario» después de producida la notificación alcance tal condición de pública, Así, como la divulgada por su legítimo creador.

esté o no incluida en la solicitud de oferta presentada, independientemente de su formato de presentación o distribución, y aceptada por los «Destinatarios».

Tiene derecho a solicitar cualquier información con respecto a las características del sistema a realizar.

TERCERA.

INFORMACIÓN CONFIDENCIAL

Las partes acuerdan que cualquier información relativa a sus aspectos financieros, comerciales, técnicos, y/o industriales suministrada a la otra parte como consecuencia de la solicitud de Oferta para el desarrollo del presente proyecto objeto del contrato, sea oral, escrita, en soporte magnético o en cualquier otro mecanismo informático, gráfico, o de la naturaleza que sea tendrá consideración de información confidencial esta información, y sus copias y/o reproducciones tendrán la consideración de «Información propia» y por tal información confidencial .

Las partes exponen que las negociaciones llevadas a cabo (o el proyecto a desarrollar en conjunto) entre el titular de la información descrita a continuación, en adelante el Divulgador, y el receptor de la misma, en adelante el Receptor, relativas a cualidades financieras, planes de negocios, información personal, dibujos, ejemplos y prototipos de artefactos, demostraciones, secretos comerciales, información técnica, sistemas de computación y software, resultados de investigaciones, listas de clientes otros datos en forma oral o escrita. Relacionada con la tecnología, ya sea que dicha comunicación se produzca verbalmente, visualmente, o mediante demostraciones o cualquier otro medio, tanto en forma de dibujos, modelos, documentos impresos, y/o formato de archivos electrónicos o de cualquier otra manera, en adelante la Información son inherentes al presente CONTRATO DE CONFIDENCIALIDAD PARA LA EMPRESA BITNESS CORP. S.A.C. y su divulgación es materia de resolución de contrato e indemnización de daños.

CUARTA.

INFORMACION QUE NO ES PARTE DEL CONTRATO

No se entenderá por «Información propia», ni recibirá tal tratamiento aquella información que sea de conocimiento público en el momento de su notificación al «Destinatario» después de producida la notificación alcance tal condición de pública, Así, como la divulgada por su legítimo creador.

OCTAVO.

DEL INCUMPLIMIENTO

Incumplimiento de las obligaciones de confidencialidad plasmadas en este documento, por cualquiera de las partes, sus empleados o directivos, facultará a la otra a reclamar por la vía legal que estime más procedente, a la indemnización de los daños y perjuicios ocasionados, incluido el lucro cesante, daño moral, y daño emergente.

NOVENO.

DURACIÓN DE ACUERDO DE CONFIDENCIALIDAD

Ambas partes acuerdan mantener el presente Acuerdo de Confidencialidad, un año después de terminar sus relaciones comerciales.

DÉCIMO.

LEGISLACIÓN APLICABLE

Se aplicará lo establecido en el Código civil de 1984, así como supletoriamente el código procesal civil. En caso de controversia se fijan los juzgados y tribunales del departamento de Lima.

Estando las partes de acuerdo en cada uno de los artículos del presente contrato lo suscriben en señal de conformidad y aceptación el DIA 07 DEL MES DE DICIEMBRE .EN LA CIUDAD DE LIMA CAPÌTAL DEL PERÚ.

LA EMPRESA

EL PROMITENTE

Anexo 43: Evaluación del instrumento final

INSTRUMENTO DE EVALUACIÓN DE LOS CONTROLES DE SEGURIDAD EN EL PROCESO DE DESARROLLO

INTRODUCCIÓN

El presente documento tiene como objetivo medir los controles de seguridad en el proceso de desarrollo de sistemas de información de la empresa BITNESS CORP. S.A.C. Las preguntas se elaboraron en función al dominio 14 de la ISO 27002:2015.

Dominio 14: Adquisición, desarrollo y mantenimiento de los sistemas de información					
14.1 Requisitos de seguridad de sistemas de información					
14.1.1 Análisis de requisitos y especificaciones de seguridad de información					
N°	**PREGUNTA**	**NL** **0– 20%**	**PL** **21 – 49%**	**AL** **50– 79%**	**CL** **80 – 100%**
1.	La empresa BITNESS CORP. S.A.C. tiene requisitos de seguridad de información identificados para el desarrollo de sistemas de información?1°Oportunidad de Mejora: Requisitos de Seguridad Durante el Proceso de Desarrollo				x100
2.	¿Utilizan o aplican algún método o proceso para la identificación de requisitos de seguridad para el desarrollo de un sistema de información en BITNESS CORP S. A.C? 1°Oportunidad de Mejora: Requisitos de Seguridad Durante el Proceso de Desarrollo				x100
3.	¿Los requisitos de seguridad identificados para el desarrollo de sistemas han sido documentados por todas las partes interesadas en BITNESS CORP S.A.C.?1°Oportunidad de Mejora: Requisitos de Seguridad Durante el Proceso de Desarrollo			X70	
4.	¿Los requisitos de seguridad identificados para el desarrollo de sistemas han sido revisados por todas las partes interesadas en BITNESS CORP S.A.C.?1°Oportunidad de Mejora: Requisitos de Seguridad Durante el Proceso de Desarrollo			X 75	
5.	¿Los requisitos y controles de seguridad de la información recibidos para el desarrollo de aplicaciones o sistemas reciben un nivel adecuado de protección de acuerdo a su importancia en la organización? Contrato de Confidencialidad				X100
6.	¿Los requisitos de seguridad de la información y los procesos asociados se integran desde las primeras etapas del proyecto de sistemas de información?				X100
7.	¿Los requisitos de la seguridad de la información consideran el nivel de confianza de la identidad declarada por los usuarios para obtener los requisitos de autentificación?				X100
8.	¿Los requisitos de la seguridad de la información consideran la aprobación y autorización de acceso para los usuarios(usuarios de negocio, usuarios con privilegios o usuarios técnicos)?1°Oportunidad de Mejora:Informe de accesos del equipo de desarrollo				X100
9.	¿Los requisitos de la seguridad de la información consideran la información de los usuarios privilegiados y técnicos respecto a sus deberes y responsabilidades en BITNESS CORP S.A.C.?1°Oportunidad de Mejora:Informe de accesos del equipo de desarrollo				X100

10.	¿Los requisitos de la seguridad de la información consideran la protección requerida para los activos en base a la disponibilidad, confidencialidad e integridad(análisis de riesgos) en BITNESS CORP S.A.C.?				X100
11.	¿Los requisitos de la seguridad de la información consideran los procesos de negocio (registro de transacciones, supervisión y monitoreo, requisitos de no repudio entre otros) en BITNESS CORP S.A.C.?				x100
12.	¿La empresa BITNESS CORP S.A.C. consideran los requisitos impuestos por otros controles de seguridad como interfaces para el registro, monitorización sistemas, detección de fugas de datos entre otros?	X0			
13.	¿La empresa BITNESS CORP. S.A.C ofrece seguridad para evitar actividades fraudulentas a aquellas empresas que solicitan sistemas de información que contengan datos sensibles como transacciones?				X100
14.	¿Existe un proceso de pruebas y adquisición formal para la adquisición de productos en BITNESS CORP S.A.C.? 2°Oportunidad de Mejora				X100
15.	¿Los contratos con los proveedores de productos o servicios cumplen con los requisitos de seguridad identificados en BITNESS CORP S.A.C.? 2°Oportunidad de Mejora:				x80
16.	¿Se consideran los riesgos que se introducen al adquirir un producto o servicio que no satisface los requisitos especificados en BITNESS CORP S.A.C.?				X100
17.	¿Se evalúan o implementan las guías disponibles para la configuración de seguridad del producto adquirido alineado con el software y los servicios finales en BITNESS CORP S.A.C.?				X100
18.	¿Se han definido criterios de aceptación para la adquisición de productos respecto a su funcionalidad para asegurar el cumplimiento de los requisitos de seguridad identificados en BITNESS CORP S.A.C.?2°Oportunidad de Mejora:Listado de criterios de aceptación del producto o servicio				X100
19.	¿Para la adquisición de un producto o servicios se realizan evaluaciones de acuerdo a los criterios de aceptación definidos en BITNESS CORP. S.A.C.?2°Oportunidad de Mejora:Listado de criterios de aceptación del producto o servicio				X100
20.	¿Las funciones adicionales de los productos o servicios adquiridos son revisadas para asegurar que no presenten nuevos riesgos inaceptables en BITNESS CORP S.A.C.?				X100

14.2 Seguridad en el desarrollo y en los procesos de soporte

14.2.1 Política de desarrollo seguro

N°	PREGUNTA	NL 0– 20%	PL 21 – 49%	AL 50 – 79%	CL 80 – 100%
1.	¿La empresa BITNESS CORP. S.A.C. tiene establecido reglas dentro de la organización para el desarrollo de aplicaciones y sistemas?1°Oportunidad de Mejora: Requisitos de Seguridad Durante el Proceso de Desarrollo				X80
2.	¿La empresa BITNESS CORP. S.A.C. aplica políticas de desarrollo seguro en el entorno de desarrollo (personas, proceso y tecnología)?1°Oportunidad de Mejora: Requisitos de Seguridad Durante el Proceso de Desarrollo			x70	
3..	¿ La empresa BITNESS CORP. S.A.C.aplica políticas de desarrollo seguro en el ciclo de vida de desarrollo de software?1°Oportunidad de Mejora: Requisitos de Seguridad Durante el Proceso de Desarrollo				X100

4.	¿ La empresa BITNESS CORP. S.A.C. cuenta con una metodología de desarrollo del software?			x50	
5.	¿ La empresa BITNESS CORP. S.A.C.aplica políticas de desarrollo seguro en la metodología de desarrollo del software?				x100
6.	¿La empresa BITNESS CORP. S.A.C. aplica guías de desarrollo seguro para cada lenguaje de programación utilizado?			x50	
7.	¿La política de desarrollo seguro en BITNESS CORP. S.A.C considera requisitos de seguridad en la fase de diseño(Etapa de ejecución)?1°Oportunidad de Mejora: Requisitos de Seguridad Durante el Proceso de Desarrollo				X100
8.	¿La política de desarrollo seguro en BITNESS CORP. S.A.C consideran puntos de verificación en los hitos del proyecto (Entregables o indicadores de progreso)?				x100
9.	¿La política de desarrollo seguro en BITNESS CORP. S.A.C consideran los repositorios seguros?1°Oportunidad de Mejora: Requisitos de Seguridad Durante el Proceso de Desarrollo				X100
10.	¿La política de desarrollo seguro en BITNESS CORP. S.A.C.considera el control de versiones?1°Oportunidad de Mejora: Requisitos de Seguridad Durante el Proceso de Desarrollo				X100
11.	¿La política de desarrollo seguro en BITNESS CORP. S.A.C. considera el conocimiento sobre seguridad de aplicaciones?1°Oportunidad de Mejora: Requisitos de Seguridad Durante el Proceso de Desarrollo			x70	
12.	¿La política de desarrollo seguro considera la capacidad de los desarrolladores de evitar, encontrar y reparar vulnerabilidades en BITNESS CORP. S.A.C.?				x100
13.	¿La empresa BITNESS CORP. S.A.C. utiliza técnicas de programación segura.(para los nuevos desarrollos o situaciones de reutilización de códigos)?				x100
14	¿La empresa BITNESS CORP. S.A.C. considera las indicaciones correspondientes para el uso de las técnicas de programación segura?				x100
15.	¿Los desarrolladores están formados en el uso de las técnicas de programación segura ?			x50	
16.	La empresa BITNESS CORP. S.A.C exige que la parte externa (desarrolladores externos) cumplan con las normas de desarrollo seguro?				X100
14.2.2 Procedimientos de control de cambios en sistemas					
N°	**PREGUNTA**	**NL 0– 20%**	**PL 21 – 49%**	**AL 50 – 79%**	**CL 80 – 100%**
1.	¿La empresa BITNESS CORP. S.A.C realiza el control de cambios mediante el uso de procedimientos formales durante el ciclo de vida del desarrollo de software?3°Opotunidad de Mejora			X75	
2.	¿En la empresa BITNESS CORP. S.A.C se han documentado los procedimientos formales de control de cambios?3°Opotunidad de Mejora			x50	
3.	¿La empresa BITNESS CORP. S.A.C. cumple los procedimientos formales de control de cambios?3°Opotunidad de Mejora			x75	

4.	¿La incorporación de sistemas nuevos y cambios importantes sigue un proceso formal de documentación, especificaciones, pruebas, control de calidad y gestión de implantación?3°Opotunidad de Mejora: Control de cambios			x75	
5.	¿Para el proceso de control de cambios se incluye una evaluación de riesgos?3°Opotunidad de Mejora: Plan de Cambio			X75	
6.	¿El proceso de control de cambios asegura que los procedimientos de seguridad y controles existentes no sean accesibles a los programadores de apoyo y que estos accedan a las partes necesarias de su trabajo?				x100
7.	Los procedimientos de control de cambios deberían incluir, pero no limitarse a: a) el mantenimiento de un registro de los niveles de autorización aprobados;				x100
8	¿El procedimiento de control de cambios asegura que los cambios son enviados a los usuarios autorizados?				x100
9.	¿Los procedimiento de control de cambios deben incluir la revisión de los controles y procedimientos de integridad asegurando que estos no se vean comprometidos por los cambios? Formato control de cambios			X75	
10.	¿El procedimiento de control de cambios incluye la identificación de todo el software,la información, las entidades de base de datos y el hardware que requiere cambios? Plan de cambio			X75	
11.	¿El procedimiento de control de cambios incluye la identificación y comprobación de la seguridad del código crítico? Formato Plan de cambios			X75	
12.	¿El procedimiento de control de cambios incluye la aprobación formal de las propuestas detalladas antes de que comience el trabajo? Formato Plan de cambios			x75	
13.	¿El procedimiento de control de cambios incluye la aceptación de los cambios de los usuarios autorizados antes de su implementación? Formato Plan de cambios			X75	
14.	¿El procedimiento de control de cambios actualiza la documentación del sistema al finalizar cada cambio y elimina la documentación obsoleta? Formato control de cambios			X75	
15.	¿El procedimiento de control de cambios incluye el mantenimiento de un control de versiones para las actuaciones del software? Formato control de cambios			X75	
16.	¿El procedimiento de control de cambios incluye el mantenimiento de registros de auditoría de las solicitudes de cambio?Formato control de cambios			X75	
17.	¿El procedimiento de control de cambios incluye la implantación de los cambios en el momento adecuado sin perturbar los procesos de negocio involucrados? Formato Plan de cambios			x75	

14.2.6 Entorno de desarrollo seguro

N°	PREGUNTA	NL 0– 20%	PL 21 – 49%	AL 50 – 79%	CL 80 – 100%
1.	¿Las personas que forman parte del equipo de desarrollo cumplen con los requisitos de seguridad establecidos? Primera oportunidad de mejora				X100
2.	¿Los procesos de cada etapa de desarrollo cumplen con los requisitos de seguridad establecidos? Primera oportunidad de mejora				X100

3.	¿Las tecnologías(computadoras, servidores, software, código) que se usan para el desarrollo de sistemas cumplen con los requisitos de seguridad establecidos?			X50	
4.	¿Los requisitos funcionales(datos de entrada) que ingresan como información están protegidos(como por ejemplo en un repositorio)?				X100
5.	¿Los datos procesados están almacenados en dispositivos seguros?				X100
6.	¿La empresa BITNESS CORP. S.A.C realiza copias de seguridad de los datos procesados?			X50	
7.	¿La empresa BITNESS CORP. S.A.C transmite la información de manera protegida(mediante correos electrónicos, usb,archivos compartidos, entre otros)?			X50	
8.	¿La empresa BITNESS CORP. S.A.C aplica los requisitos de seguridad externos e internos?				X100
9.	¿Los controles de seguridad de la organización apoyan el desarrollo del sistema?				X100
10.	¿El personal de BITNESS CORP. S.A.C. cumple con los requisitos de seguridad(no realizan copias indebidas, no sacan la información fuera del entorno de desarrollo)?			X75	
11.	¿Existe algún documento de confidencialidad para la contratación de personal externo?				X100
12.	¿Existen sanciones en caso de no cumplir el contrato de confidencialidad? Cuarta oportunidad mejora				X100
13.	¿La empresa BITNESS CORP. S.A.C. segrega la información cuidadosamente de acuerdo al trabajo que ejerce cada personal?				X100
14.	¿La empresa BITNESS CORP. S.A.C. maneja un control de acceso físico(ambiente de trabajo, oficinas)?	X0			
15.	¿La empresa BITNESS CORP. S.A.C. maneja un control de acceso lógico(acceso a los servidores, acceso a cuentas de usuario)?				x100
16.	¿La empresa BITNESS CORP. S.A.C. realiza la monitorización de los cambios en el producto?				X100
17.	¿La empresa BITNESS CORP. S.A.C. realiza la monitorización de los cambios durante el proceso de desarrollo(código)?				X100
18.	¿La empresa BITNESS CORP. S.A.C. realiza copias de seguridad fuera de las instalaciones?	x0			
19	¿La empresa BITNESS CORP. S.A.C. almacena de manera segura sus copias de respaldo?				x100
20.	¿La empresa BITNESS CORP. S.A.C. tiene identificado al personal que accede a las copias de respaldo?				x100
21.	¿La empresa BITNESS CORP. S.A.C realiza una gestión adecuada para la presentación de avances(entregables)?				x100
22.	¿La empresa BITNESS CORP. S.A.C cumple con las medidas de seguridad para la presentación de avances(entregables)?				x100
14.2.8 Pruebas funcionales de seguridad de sistemas		**100%**			
N°	**PREGUNTA**	**NL 0– 20%**	**PL 21 – 49%**	**AL 50 – 79%**	**CL 80 – 100%**

1.	¿Realizan pruebas y verificaciones exhaustivas en el proceso de desarrollo de sistemas nuevos y los actualizados.?				x100
2.	¿Las pruebas y verificaciones exhaustivas son realizadas por el equipo de desarrollo?				x100
3.	¿Se realizan pruebas de aceptación independientes(para desarrollos internos y desarrollos externalizados)?			X75	
14.2.9 Pruebas de aceptación de sistemas					
N°	**PREGUNTA**	**NL 0– 20%**	**PL 21 – 49%**	**AL 50 – 79%**	**CL 80 – 100%**
1.	¿La empresa BITNESS CORP. S.A.C. establece programas de pruebas de aceptación?				X100
2.	¿Las pruebas de aceptación del sistema incluyen las pruebas de los requisitos de seguridad de la información?				X100
3.	¿Las pruebas de aceptación del sistema incluyen las prácticas de desarrollo seguro del sistema?				X100
4.	¿Se realizan pruebas a los componentes recibidos?			X50	
5.	¿La empresa BITNESS CORP. S.A.C. utiliza herramientas automatizadas(herramientas de análisis de código o los escáneres de vulnerabilidad) para la seguridad?	X0			
6.	¿La empresa BITNESS CORP. S.A.C. realiza pruebas realistas que eviten la introducción de vulnerabilidades en la organización?	X0			
14.3.1 Protección de los datos de prueba					
N°	**PREGUNTA**	**NL 0– 20%**	**PL 20 – 49%**	**AL 50 – 79%**	**CL 80 – 100%**
1.	¿En la empresa BITNESS CORP. S.A.C. evita el uso de datos reales o la información confidencial para las pruebas? contrato confidencial				X100
2.	¿En caso la empresa BITNESS CORP. S.A.C use datos o información confidencial está es protegia mediante su retirada o modificación?				X100
3.	¿Los procedimientos de control de acceso de BITNESS CORP. S.A.C se aplican a las sistema de pruebas?			X50	
4.	¿La empresa BITNESS CORP. S.A.C realiza un control de acceso cada vez que la información de operación se copia a un entorno de prueba?	X0			
5.	¿En la empresa BITNESS CORP. S.A.C la copia y uso de información operacional es registrada para futuras auditorias?	X0			