UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS
ESCUELA DE INGENIERÍA INFORMÁTICA

TESIS DE GRADUACIÓN

Para optar por el grado de Licenciatura en Ingeniería con énfasis en Gerencia.

PROPUESTA PARA EL MANEJO DE LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO/IEC 27001:2013 PARA LA EMPRESA FINANCIERA DESYFIN S.A, UBICADA EN SAN JOSÉ.

OLMAN JESÚS CHACÓN GARCÍA

AUTOR

MÁSTER. FABIÁN RODRÍGUEZ SIBAJA

TUTOR

MBD. OLMAN NÚÑEZ PERALTA

LECTOR

San José, Costa Rica

Agosto, 2020

AGRADECIMIENTO

Al concluir esta etapa tan importante en mi vida, únicamente puedo agradecer a Dios por darme el don de la vida, por todo lo que soy, lo que tuve y lo que tengo, por siempre enseñarme el camino correcto en esta vida además de todas las bendiciones que en estos años he recibido y que me han impulsado a seguir adelante para lograr una de mis metas más grandes.

A mi mamá y papá, no hay palabras que puedan expresar mi completo agradecimiento por estar a mi lado, ser los mejores ejemplos en mi vida, por todo lo que me han enseñado, sin ellos, nada de esto sería posible.

A mi hermana y hermano, por ser más que hermanos ser amigos y cada uno a su manera me mostraron diferentes perspectivas de la vida. A mi sobrina, por ser una luz en mi vida y por quererme tanto como yo a ella.

Para doña Elvia, una de las personas que siempre me dio palabra de apoyo y con sus gestos y acciones diarias me motivaron en continuar y concluir esta etapa.

Agradezco a todos los docentes que hicieron posible mi formación como profesional, forjando valores de responsabilidad y ética. Principalmente, quiero agradecer a mi tutor, Fabián Rodríguez, por su gran apoyo en estos meses tan importantes para mí, la atención brindada y el seguimiento continuo marcaron mucha diferencia en la elaboración de la propuesta.

Por último, pero no menos importante, agradezco a Financiera Desyfin S.A por estar siempre anuente con ayudarme en todo este proceso y lo que el implica, en especial a Christopher Benítez por el apoyo brindado en todo momento, gracias al esfuerzo en conjunto fue posible realizar mi proyecto de manera exitosa.

DEDICATORIA

A Dios, por darme los pilares fuertes y sólidos para que pueda construir mi base de vida, ser la fuerza espiritual y mi guía en todo momento.

A mis padres, por estar en todas conmigo, la compresión de ambos y el trabajo diario por mi comodidad demuestran el amor que poseen como los buenos padres que son, el amor de ellos hizo que nunca bajaran los brazos.

Para todos mis grandes amigos, siempre estuvieron pendientes y con palabras de motivación hicieron posible los aumentos de ánimo en momentos de caras bajas.

Contenido

Tablas de Cuadros

Tablas de Imágenes

Tablas de Gráficas

RESUMEN EJECUTIVO

Las diversas empresas que conforman el mundo de los negocios, independientemente del tipo de producto o servicio que ofrecen, han entrado en un proceso evolutivo en el que intentan integrar métodos y estándares sólidos en sus rutinas diarias para garantizar un posicionamiento óptimo para llegar al mercado y conseguir una reputación positiva de los clientes, socios y evaluadores.

Consecuente a lo anterior, muchas empresas hacen un esfuerzo por adaptar mejores prácticas y metodologías que ofrece el mercado referente a la seguridad de la información, al mismo tiempo formar un equipo de trabajo donde se desempeñen de manera integral para conseguir los objetivos.

Dichos esfuerzos permiten ordenar, concentrar y sistematizar información relacionada con la operativa de un área o proyecto en particular, definiendo también la confidencialidad, disponibilidad e integridad que conforman los pilares de la seguridad de la información. A su vez mitigar o minimizar las amenazas tanto externas como internas, que podrían representar un riesgo sobre la información en las empresas modernas, dado que la información es valorizada como unos de los recursos más importantes y por lo tanto debe ser protegida.

La siguiente propuesta está orientada en la elaboración de un marco para el manejo de la seguridad de la información definiendo las políticas y procedimientos acordes con los objetivos de la normativa ISO 27001:2013 para el Departamento de Informática de la Financiera Desyfin S.A.

CAPÍTULO I: INTRODUCCIÓN

Muchas organizaciones se enfocan más en sus actividades comerciales y en su productividad, y dejan por un lado aspectos tan importantes como los de establecer y fortalecer los controles sobre la seguridad de la información y sus datos para prevenir y detectar fraudes en la organización.

La seguridad de la información no solo es responsabilidad del departamento de tecnología, sino de toda la organización, por eso es importante concientizar a todo el personal sobre las las consecuencias que las amenazas generan.

He aquí el grado de importancia de seguir un modelo de seguridad que garantice el manejo adecuado de la información y aseguren los activos vitales a través de normativas o políticas que regulen las actividades diarias de la organización, las cuales deben ser conocidas por todos los empleados a través de capacitaciones, para que se comprometan a hacer buen uso de la información y de los recursos, y finalmente entre todos, mantener los principios como la integridad, disponibilidad y confidencialidad de la información.

Con la presente propuesta, se pretende ofrecer a la Financiera Desyfin un sistema de gestión de seguridad de la información que permita implementar lineamientos que aseguren la información y los demás activos informáticos, utilizando como marco de referencia la norma ISO 27001:2013, la cual emplea las mejores prácticas para cumplir los objetivos de la propuesta.

Descripción del problema

En la actualidad, el área de tecnologías de información, dado su gran soporte a toda la estructura operativa de la Financiera se encuentra en constante evolución. Dicha evolución se ve reflejada en la optimización de las arquitecturas tanto de *hardware* como de *software*.

No obstante, ligado a este proceso evolutivo de los servicios de TI, existen eventos que toda compañía debe contemplar tales como:

- Control de tecnología y equipos obsoletos.

- Cambios en el enfoque del negocio.
- Necesidad obtener productos tecnológicos para abastecer las demandas del mercado.
- Optimizar los recursos utilizados.

Esos eventos traen amenazas o riegos a las que se enfrentan las empresas a nivel mundial de ahí que se opte por el uso de medidas como son: el desarrollo de documentos, directrices y controles que orienten el correcto uso de las tecnologías de información para sacar el mejor aprovechamiento de los recursos; de esta manera, se evita que tanto personal interno como externo realicen un inadecuado manejo de recursos, que pueden originar problemas tanto en los servicios que se ofrecen a los clientes como en la operatividad del negocio.

En este sentido, las políticas, procedimientos, controles y directrices de seguridad de la información surgen como una herramienta para concientizar a los colaboradores sobre la importancia de la sensibilidad en la información de los servicios críticos que posibilitan a las empresas mantenerse en el mercado y poder competir.

Actualmente no se cuenta con un cuerpo normativo para el manejo de la Seguridad de la Información, tanto a nivel de la estructura organizacional como para los sistemas tecnológicos que permiten resguardar la información y garantizar en forma razonable su confidencialidad, disponibilidad e integridad.

Con base en lo expuesto en los párrafos anteriores, en la Financiera Desyfin S.A se han detectado los siguientes problemas:

1. Falta de un gobierno de la seguridad de la información en la Financiera: Actualmente la Financiera Desyfin S.A no dispone del personal respectivo que vele por la seguridad de la información y la comunicación del personal a la alta directiva es nula, esto hace que no exista una dirección clara acerca de la seguridad de la información, ya que no se encuentran formalmente establecidas las responsabilidades en las distintas áreas de la Financiera, comprometiendo la disponibilidad, confidencialidad e integridad de los datos.

2. No se cuenta con una cultura de seguridad de la información en la Financiera: Por parte de los funcionarios de la Financiera existe una falta de concientización, apropiación y conocimiento en temas de seguridad de la información por lo que aumenta el riesgo de la divulgación de información sensible o confidencial de manera no autorizada.

3. No existe una adecuada gestión de riesgos de seguridad: La Financiera no cuenta con una visión global del estado de su seguridad de la información, y por lo tanto no puede determinar con exactitud la efectividad de las medidas que sobre seguridad implemente.

4. La inadecuada identificación de riesgos y controles de seguridad hace que Financiera Desyfin S.A se vea comprometida ante la amenaza de pérdida de información sensible causando pérdidas financieras o administrativas ante la explotación de un riesgo.

5. Dificultad para el control y clasificación de los activos de la información, exponiéndose a robo o pérdida de los activos sin responsabilidad alguna.

6. La documentación formal relacionada a procedimientos o políticas alineadas a los objetivos de la Financiera se encuentran desactualizadas y no se ajustan a la situación actual de la Financiera, causando un mal manejo de los incidentes, falta de accesos o disponibilidad de la información, amenaza de modificación accidental o malintencionada de la información de peligros tanto internos como externos.

Objetivos

Objetivo general

Desarrollar una propuesta para el manejo de la seguridad de la información basada en la Norma ISO/IEC 27001:2013 para el Departamento de Informática de la empresa Financiera Desyfin S.A, para la determinación del cumplimiento de su aplicación y establecimiento de las correcciones necesarias en caso de que el presente estudio las plantee.

Objetivos específicos

- Realizar un diagnóstico de la situación actual de la Financiera con relación a los controles de seguridad de información implementados para la definición de los hallazgos y oportunidades de mejora en el Departamento de Informática.

- Implantar el nivel de cumplimiento de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la ISO 27001:2013 y la definición de los planes de acción orientados a cerrar las brechas de seguridad encontradas.

- Definir la política, alcance y objetivos del sistema de gestión de seguridad de la información.

Justificación

Hoy las compañías deben velar por una correcta gestión de la seguridad de la información, siendo más conscientes del costo beneficio y el uso de los recursos que se destinan para garantizar su ~~la~~ confidencialidad, integridad y disponibilidad.

La seguridad de la información no debe limitarse únicamente a la seguridad de datos en los computadores. Debe estar, básicamente, orientada a proteger y resguardar la propiedad intelectual y la información de mayor importancia de las organizaciones y de las personas.

Financiera Desyfin al igual que toda compañía maneja a diario información de alta importancia que le genera valor, la cual tiene diferente nivel de valor para cada área, dado

que un “documento” importante o confidencial para un departamento, para otro puede no ser tan relevante. Por esa razón antes de empezar a implementar controles de seguridad se debe analizar y considera la situación actual de la seguridad de la información; de tal forma que se pueda mitigar vulnerabilidades y amenazas con el fin de determinar cuáles son las necesidades para garantizarle la confidencialidad, integridad y disponibilidad.

Con lo anterior se considera que los datos de la Financiera son de gran relevancia para la entrega y soporte de los servicios que se desarrollan hacia clientes también como para las operaciones internas que se llevan a cabo día con día.

Es primordial crear una propuesta para el adecuado manejo de un sistema de gestión de seguridad de la información, la cual permitirá a la financiera poder contar con un gobierno de seguridad de información alineado a las necesidades y objetivos estratégicos del negocio, compuesto por una estructura organizacional con roles y responsabilidades y un conjunto coherente de políticas, y procedimientos, con el objetivo de idear, promover y desarrollar una cultura de seguridad en todos los niveles de la organización y de esta forma gestionar de manera adecuada la seguridad de su información.

La Financiera se verá beneficiada con la creación del conjunto de políticas que brindarán los lineamientos necesarios para velar por la protección de los datos de la información ante posibles amenazas, con el objetivo de asegurar que los riesgos y sus impactos provoquen un menor daño tanto interno como externo. Además, todo ello asegura una mejor rentabilidad de los costos y beneficios, esto con la finalidad de garantizar la continuidad de las operaciones del negocio como de la reducción del impacto de los incidentes en temas de seguridad de la información.

Estudios de viabilidad

Viabilidad técnica.

Para el desarrollo de la propuesta a nivel de *software* y *hardware*, se requiere disponer de una computadora que cuente con las características mínimas como las siguientes:

Hardware:

- Memoria de 4 Gb de memoria RAM o superior.

- Procesador Intel core i3 o superior.

- Disco Duro 250 Gb.

- Tarjeta de red.

- Pantalla 15.6’’ LED.

- Mouse.

- Teclado.

Software:

- Al ser un trabajo de tipo investigativo, se puede utilizar cualquier versión de Windows 10.

- Paquete de Office 2013 o superior.

- Adobe Reader.

- Explorador (Internet Explorer, Chrome o Firefox).

El *software* utilizado debe contar con su respectiva licencia en caso de ser requerida.

Viabilidad operativa.

Por parte de la Financiera, se cuenta con el auditor de TI, quien posee experiencia en temas de la normativa ISO 27001. También se presenta una buena disposición por parte de las jefaturas para la propuesta presentada.

Viabilidad económica.

Es variable económicamente porque se logra contar con las herramientas por utilizar: Pc, sistema operativo, paquete Office, Adobe y documento de la normativa ISO27001:2013.

Se logra contar también con el conocimiento y disponibilidad para realizar la propuesta, por lo tanto, el costo es mínimo dado que no se requiere utilizar herramientas por las que se

debe realizar un desembolso. En sí el único costo sería si se llega a la implementación de la propuesta, sumado al costo del equipo que se utilizará, el cual es parte integral de la propuesta; esta se observa en la tabla.1:

Tabla 1. Tareas y duración de la implementación de la propuesta

Tareas	**Duración**
Levantamiento de requerimientos	1 semana
Analizar la documentación brindada por la Empresa.	2 semana
Verificar el grado de cumplimiento de las diferentes políticas que tiene la Financiera con el fin de verificar si se están cumpliendo.	2 semana
Elaborar las diferentes políticas y controles.	2 semana

Fuente: elaboración propia.

Por cada día laboral, se trabaja 8 horas diarias, que en total representan 280 horas.

En la página del Ministerio de Trabajo y Seguridad Social, se valida que, para el primer semestre del 2020, el salario de un analista de computación por jornada ordinaria de 8 horas corresponde a ¢ 13.872 lo que representa ¢ 1,734 por hora.

En total las 280 horas multiplicadas por los ¢ 1,734.087 representa un total de ¢ 485,530 en pago por la implementación sumado a esto el costo de un computador con las características mínimas que oscila en los ¢ 250,000 más la normativa ISO27001:2013 la cual en la página de INTECO se encuentra con un valor de ¢ 35,040 representaría un costo de ¢ 770,560.

Sin embargo, todos estos costos son absorbidos por el estudiante dado que representan parte de la propuesta de graduación, además ya se cuentan con los materiales requeridos para llevar la propuesta sin incurrir en mayor gasto.

Viabilidad legal.

Para la propuesta se toman en cuenta dos leyes de Costa Rica.

- Ley n.° 9048 de Delitos informáticos:

Se establecen nuevos tipos penales como suplantación de identidad, suplantación de páginas electrónicas e instalación o propagación de programas informáticos maliciosos. También se contemplan otros delitos como la violación de correspondencia y datos personales, extorsión, estafa informática, daño informático y espionaje. Con lo anterior, se busca no solo la protección de personas físicas, sino también de personas jurídicas.

- Ley n.° 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales:

Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

Dado que en el proceso de elaboración de esta investigación, se respetan las leyes antes mencionadas y no se viola ninguna ley de la república, la investigación es legalmente viable.

Proyecciones

Con esta propuesta se pretende proveer las condiciones de gobernabilidad, oportunidad y viabilidad necesarias para que la seguridad de la información apoye y extienda los objetivos estratégicos del negocio, mediante la protección y aseguramiento de su información que es fundamental para garantizar la debida gestión financiera, administrativa y operativa de la entidad, y con ello asegurar el cumplimiento de su Misión.

Alcance

El alcance de la propuesta presente para Financiera Desyfin aplica a todos los servicios financieros que son brindados por Desyfin a sus clientes desde su sede central en Sabanilla, San José, Costa Rica. Dicho alcance cubre el manejo de la información y las actividades de negocio, así como el personal y los activos que soportan la entrega de este servicio y en concordancia con la declaración de aplicabilidad descrita en este mismo documento.

Se excluyen en esta primera iteración del SGSI la infraestructura tecnológica implementada en las sucursales de la Financiera (Rohrmoser, Heredia, Guanacaste, Grecia y Santa Ana), las cuales serán consideradas cuando se encuentre probado e implementado un marco de seguridad en la sucursal de Sabanilla; no obstante, el personal de las sucursales excluidas del alcance si formarán parte de esta primera iteración.

Con el propósito de elaborar un conjunto de políticas y procedimientos de administración de la seguridad de la información, se toma como base los Objetivos de Control del Estándar de la Norma ISO/IEC 27001: 2013, los cuales se enumeran a continuación:

- A.5 Políticas de seguridad.

- A.6 Organización de la seguridad de la información.

- A.8 Gestión de activos.

- A.9 Control de acceso.

- A.11 Seguridad física y del entorno.

- A.12 Seguridad de las operaciones.

- A.13 Seguridad de la comunicación.

- A.16 Gestión de incidentes de la seguridad de la información.

Etapas

Evaluación inicial.

Se realizará una evaluación bajo la normativa ISO 27001:2013, tendrá contemplado los objetivos del control y controles que brinda la norma.

Dentro del alcance de la presente propuesta se determinaron los controles a desarrollar, que serán sometidos para identificar su cumplimiento y los riesgos a los que se expone la Financiera.

Dentro de este punto se darán a conocer las principales faltas encontradas y causas de la problemática.

Confección de una matriz de riesgo.

Para esta etapa los riegos encontrados a los que se exponen las áreas al no contar con los controles requeridos por la ISO 27001:2013 serán documentados.

Para la matriz se tomarán dos factores: probabilidad e impacto, identificando así los riesgos más significativos a las actividades de la empresa.

Elaboración de la estructura.

En la presente etapa definimos una estructura en la cual se basarán las políticas y procedimientos que se serán creados durante la propuesta.

Toda política creada y presentada será confeccionada tomando la fase 3 “elaboración de la política” de la ISO27001:2013 la cual establece los siguientes puntos:

1. Redactar una política de acuerdo con las necesidades de cada organización.

2. La política de la seguridad de la información debe tener en cuenta los objetivos de cada organización.

3. La política de la Financiera Desyfin S.A debe demostrar que se tienen en cuenta los requisitos de las partes interesadas.

4. La comunicación de la política a las partes interesadas.

5. Propietario de la política.

Para la elaboración de los documentos se mantendrá una base formal de redacción y confección considerando los siguientes aspectos mismos serán ilustrados en tabla.2:

- Logo de la empresa.

- Título del documento.

- Código del documento.

- Versión.

- Tabla de contenido.

- Control de cambios.

- Visto bueno.

- Objetivo.

- Alcance.

- Contenido.

Tabla 2. Formato para la elaboración de documentos

Logo	**FINANCIERA DESYFIN S.A.**	Versión: 1.0
	CODIGO: XX.XX.XX	Página 31 de 12
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha de emisión: Mes 2020
		Fecha de última revisión:
		Código:
	Realizado por:	Aprobado por:

Fuente: elaboración propia.

Al momento que a una política o procedimiento se le realice un cambio, deben ser incluidos los datos pertenecientes al control de cambio; en la tabla.3 se especifican los aspectos solicitados.

Tabla 3. Control de Cambios

Fecha	Versión	Actualizado por	Información de los Cambios Realizados

Fuente: elaboración propia.

Para cada política y procedimiento se mantendrá un estándar de fuente de letra y tamaño, la utilización de colores para letras y relleno debe ser alusivo a los colores de la Financiera.

CAPÍTULO II: MARCO REFERENCIAL

El presente capítulo muestra los principales temas de la base teórica del trabajo. Se abarcan varios conceptos que facilitarán la comprensión de la investigación.

Financiera Desyfin cuenta con una serie de servicios para los cuales, la propuesta de seguridad de la información velará por la integridad, disponibilidad y confidencialidad de los datos y servicios presentados por la entidad; dentro de ellos se destaca: seguros, inversiones y ahorro, y descuentos de facturas. Según Miranda (2016), las empresas, al vender un producto o servicio, ofrecen a sus clientes más recurrentes o confiables el crédito hasta una fecha determinada. Se firma como respaldo documentos que se pueden negociar (letras de cambio, pagarés, etcétera). En muchas ocasiones, principalmente en el caso de las pymes, se requiere de algún tipo de financiamiento para solventar la falta de liquidez que se genera al brindar crédito a sus clientes. Por ello, "existe otra forma de financiamiento muy común y utilizada por las empresas, llamado descuento comercial o descuento de efectos" muy conocido también como factoreo. (p. 125)

Otro de los servicios que brinda la Financiera corresponde al *leasing*, según PARA, C& EMPRESARIOS, E. Y. (2017) es una operación financiera a medio y largo plazo que tiene como base fundamental un contrato de arrendamiento. Este consiste en que la persona física o jurídica propietaria del bien cede los derechos de uso a otra, tomando en contrapartida unas prestaciones (tasa de arrendamiento) y se obliga a ceder una opción de compra. (p.127)

Para el desarrollo de la propuesta se busca crear una serie de políticas de seguridad y procedimientos. Según Sain (2018), una política de seguridad de una organización comprende los principios y líneas de acción fundamentales que sirven de base para la seguridad de los sistemas informáticos y definen las responsabilidades para las cuestiones técnicas y organizativas y los procedimientos de seguridad son tareas y operaciones a ejecutar de acuerdo a las políticas de seguridad de la organización. (pp. 04-05), de manera que se apoye a la Financiera con la preservación de la confidencialidad, integridad y disponibilidad de la información.

Según Sain (2018), la confidencialidad hace alusión a la garantía de que cada mensaje transmitido por las redes de comunicaciones o almacenado en un sistema informático pueda ser leído por su legítimo destinatario, garantizando las medidas de seguridad apropiadas para ese objetivo. La integridad está relacionada con la garantía de que los contenidos de un documento no hayan sido alterados desde su creación o durante su transmisión en red (pp. 01-02), mientras que la disponibilidad, según Chilán y Pionce (2017), "es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones". (p.04).

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. (ISO/IEC 27000:2014, p. 4).

Uno de los conceptos claves para el principio de la seguridad informática que complementa a la disponibilidad, integridad y confidencialidad es el no repudio, el cual es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación. Para Barajas e Izaguirre (2017), "el no repudio sirve a los emisores o a los receptores para negar un mensaje transmitido. Por lo que cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto" (p.20) dando así la validación de los principios clave de la seguridad informática.

Imagen 1. Relación de los servicios de seguridad

Fuente: padawanceh.blogspot.com

Para asegurar que las políticas y procedimientos se ajusten a la necesidad de la Financiera, se cuenta con el apoyo de auditoría informática; según Castillo, Salomón y Tapia (2016), la auditoría informática es la revisión y evaluación de los controles, sistemas y procedimientos de informática de los equipos de cómputo, su utilización, eficiencia y seguridad de la organización, los cuales participan en el procesamiento de la información, a fin de que por medio de los cursos alternativos se logre una utilización eficiente y segura de la información que da soporte a la toma de decisiones.

Para una correcta gestión de la información se requiere la participación de toda la organización. Para Pacheco (2010) citado por Pico y Santana (2017):

> Un Sistema de Gestión de Seguridad de la Información (SGSI) es, tal como su nombre lo indica, un elemento para administración relacionado con la seguridad de la información, aspecto fundamental de cualquier empresa. Un SGSI implica crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de la información. (p.04)

Dado que se busca la disminución o corrección a vulnerabilidades, se toma la medición del impacto y riesgo; según Sain (2018), una vulnerabilidad es una debilidad que presenta un sistema informático que puede permitir que las amenazas causen daños en los mismos y así producir pérdidas para la organización, mientras que un incidente de seguridad es un evento que puede producir una interrupción de los servicios brindados por un sistema informático y/o posibles pérdidas materiales o financieras. El impacto es la medición y valoración de un daño que podría producir en una organización un incidente de seguridad, mientras que el riesgo es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización. (p.04)

Es frecuente que se refiera a seguridad de la información con seguridad informática. Según ISOTools Excellece, la seguridad informática, con sus siglas en inglés IT security, es la disciplina que se encarga de llevar a cabo las soluciones técnicas de protección de la información. En este sentido:

> La seguridad informática protege el sistema informático, tratando de asegurar la integridad y la privacidad de la información que contiene. Por lo tanto, podríamos decir, que se trata de implementar medidas técnicas que preservarán las infraestructuras y de comunicación que soportan la operación de una empresa, es decir, el hardware y el software empleados por la empresa. (ISOTools Excellence, 2017)

Según Sain (2018), los diferentes planos donde actúa la seguridad informática son el técnico, el legal, el humano y el organizativo. En cuanto al aspecto más importante, el técnico, incluye el nivel físico (*hardware*) como el nivel lógico (*software*) y comprende la ejecución de las medidas de seguridad implementadas por una organización para la protección de los sistemas informáticos y sus redes de comunicación. En cuanto al aspecto legal, el mismo hace alusión a las diferentes normativas legales o administrativas que obligan a las organizaciones a adoptar medidas de seguridad específicas. El aspecto humano, en cambio, alude a la sensibilización, capacitación de personal que desempeña funciones relacionadas con el mantenimiento de los sistemas informáticos. Por último, está el plano organizativo, que refiere al diseño e implementación de las políticas de seguridad de una organización tales como los planes, las normas y los procedimientos, entre otros. (p.03)

Las medidas técnicas serán llevadas a cabo por el equipo de seguridad informática, administradores de sistemas. Según Binwal (2015), el término que describe el compromiso de la alta dirección es el gobierno corporativo, que es el conjunto de responsabilidades y prácticas ejercidas por los responsables de una empresa (por ejemplo, el consejo y la alta dirección) con el objetivo de proporcionar dirección estratégica, asegurar que los objetivos sean alcanzados, garantizar que los riesgos sean gestionados adecuadamente, y verificar que los recursos de la empresa sean utilizados de manera responsable. (p.03-04)

Cristian David Macen Rojas, realizó una investigación titulada “Políticas de Seguridad de la Información” (2014); y en ella enfocó la relación que existe con respecto a la ausencia de las políticas de seguridad en los departamentos de informática en las organizaciones, dicha ausencia puede ocasionar graves efectos para las operaciones de las organizaciones. Se menciona en su investigación y coloca como ejemplo el ataque que sufrió la empresa Ebay,

en el que intrusos enviaron de forma fraudulenta correos a sus 55 millones de usuarios para solicitarles que confirmaran sus datos a través de un portal o sitio web de Ebay, igualmente falso, para una comprobación técnica, por ese motivo pocos clientes sospecharon que se tratase de un fraude. Es por eso que toda organización debe contar con políticas de seguridad de la información. En la investigación se analizan los riegos de la seguridad de la información, se dan a conocer los aspectos culturales y técnicos para el manejo de la información, así como también explica el desarrollo de las políticas que se deben llevar a cabo para garantizar una gestión efectiva de la seguridad de la información.

Cristian Macen, citado por la Dirección de Tecnología Informática de la Universidad Distrital José de Caldas, se refiere a "Políticas para la Seguridad de la Información como un manual de seguridad de la información", que formaliza su compromiso con el proceso de gestión responsable de la información, que tiene como objetivo garantizar la integridad, confiabilidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales (p. 20).

Se refleja la importancia que deben tener las políticas de la seguridad de la información, de manera que las organizaciones elaboren un manual que contemple todos los procedimientos y políticas de seguridad que se deben llevar a cabo ante cualquier situación de fallas o problemas que se presenten. El manual debe ser elaborado por el gerente del Departamento de Informática en conjunto con su equipo de trabajo, luego de haber realizado un estudio previo sobre las amenazas y vulnerabilidades en los sistemas de información en la organización.

En cuanto a las normas de referencia, la familia de las normas ISO/IEC 27000, son un marco de referencia de seguridad a nivel mundial desarrollado por la International Organization for Standardization - ISO e International Electrotechnical Commission – IEC, que proporcionan un marco, lineamientos y mejores prácticas para la debida gestión de seguridad de la información en cualquier tipo de organización. Estas normas especifican los requerimientos que deben cumplir las organizaciones para establecer, implementar, poner en funcionamiento, controlar y mejorar continuamente un sistema de gestión de seguridad de la información.

El Instituto de Normas Técnicas de Costa Rica (INTECO), es el organismo encargado de normalizar este tipo de regulaciones para nuestro país, dentro de la familia de las ISO/IEC 27000 se destacan las que se consideran un aporte a este trabajo de investigación:

ISO/IEC 27000: esta norma proporciona una visión general de los sistemas de gestión de seguridad de la información y contiene los términos y definiciones que se utilizan en las diferentes normas de la 27000.

ISO/IEC 27001: la última versión de esta norma fue publicada a finales del 2013, y corresponde a la principal norma de la serie 27000 debido a que contiene los diferentes requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información en las organizaciones independiente de su tipo, tamaño o naturaleza. También incluye los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adoptadas a las necesidades de la organización.

El Anexo A de la norma ISO 27001, contiene los diferentes objetivos de control y controles que las organizaciones deberían tener en cuenta para la planeación e implementación de su sistema de gestión de seguridad de la información, los cuales se describen con más detalle en la norma ISO 27002.

ISO/IEC 27002: guía de buenas prácticas en seguridad de la información que describe de forma detallada las acciones que se deben tener en cuenta para el establecimiento e implementación de los objetivos de control y controles descritos de una forma general en el Anexo A de la norma ISO 27001.

ISO/IEC 27003: guía que contiene aspectos necesarios para el diseño e implementación de un sistema de gestión de seguridad de la información de acuerdo con los requerimientos establecidos en la norma ISO/IEC 27001, donde se describe el proceso desde la planeación hasta la puesta en marcha de planes de implementación.

ISO/IEC 27004: guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un sistema de gestión de seguridad de la información y de los objetivos de control y controles implementados de acuerdo con el Anexo A de la norma ISO 27001.

ISO/IEC 27005: esta norma establece los lineamientos para la gestión de riesgos de seguridad de la información y está diseñada para ayudar a las organizaciones en la implementación de un sistema de gestión de seguridad de la información basada es un enfoque de gestión de riesgos. Entre otros aspectos, establecer lo requerimiento que se deben tener en cuenta para el proceso de valoración de riesgos, relacionados con la identificación, análisis, evaluación y tratamiento de los riesgos en la seguridad de la información.

El propósito de un SGSI no es garantizar la seguridad que nunca podrá ser resuelta en un 100% sino garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la pequeña empresa de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la organización, los riesgos, el entorno y las tecnologías.

La norma ISO 27001 adopta el ciclo de Deming como metodología, la cual se puede aplicar a todos los procesos que abarca el SGSI. Esta metodología es conocida por sus siglas en inglés PDCA: Plan- Do- Check - Act, según Cano y Maldonado (2014), el del ciclo de Deming es caracterizar una metodología que genere conciencia sobre la importancia de la seguridad de la información y la aplicabilidad de esta en pequeñas empresas, que garantice un tratamiento seguro de la integridad, disponibilidad y confidencialidad para evitar que dicha información se vuelva pública de una manera no autorizada (p.23).

Imagen 2. Ciclo de Deming

Fuente: https://metodoss.com/

Tiene una serie de fases y acciones que permiten establecer un modelo de indicadores y métricas comparables en el tiempo, de manera que se pueda cuantificar el avance en la mejora de la organización:

- Plan: esta fase corresponde con establecer el SGSI. Se planifica y diseña el programa, sistematizando las políticas a aplicar en la organización, cuáles son los fines por alcanzar y en qué ayudarán a lograr los objetivos de negocio, qué medios se utilizarán para ello, los procesos de negocio y los activos que los soportan, cómo se enfocará el análisis de riesgos y los criterios que se seguirán para gestionar las contingencias de modo coherente con las políticas y objetivos de seguridad.
- Do: es la fase en la que se implementa y pone en funcionamiento el SGSI. Las políticas y los controles escogidos para cumplirlas se implementan mediante recursos técnicos, procedimientos o ambas cosas a la vez, y se asignan responsables a cada tarea para comenzar a ejecutarlas según las instrucciones.
- Check: esta fase es la de monitorización y revisión del SGSI. Hay que controlar que los procesos se ejecutan como se ha establecido, de manera eficaz y eficiente, alcanzando los objetivos definidos para ellos. Además, hay que verificar el grado de cumplimiento de las políticas y procedimientos, identificando los fallos que pudieran existir y, hasta donde sea posible, su origen, mediante revisiones y auditorías.
- Act: es la fase en la que se mantiene y mejora el SGSI, decidiendo y efectuando las acciones preventivas y correctivas necesarias para rectificar los fallos, detectados en las auditorías internas y revisiones del SGSI, o cualquier otra información relevante para permitir la mejora permanente del SGSI.

Los protocolos de seguridad son un conjunto de reglas que gobiernan dentro de la transmisión de datos entre la comunicación de dispositivos para ejercer una confidencialidad, integridad, autenticación y el no repudio de la información. Se componen de:

Criptografía (cifrado de datos): se ocupa del cifrado de mensajes, es decir, cuando un mensaje es enviado por el emisor, lo que hace es transposicional u ocultar el mensaje hasta que llegue a su destino y puede ser descifrado por el receptor.

Lógica (estructura y secuencia): esta consiste en llevar un orden en el cual se agrupan los datos del mensaje, su significado y saber cuándo se va a enviar el mismo.

Autenticación: es una validación de identificación, es la técnica mediante la cual un proceso comprueba que el compañero de comunicación es quien se supone que es y no se trata de un impostor. Dentro de los principales atacantes de la seguridad de la información se encuentran: el *hacker*, es una persona con amplios conocimientos en tecnología, el cracker, se denomina así a aquella persona con comportamiento compulsivo, que alardea de su capacidad para reventar sistemas electrónicos e informáticos.

El *copyhacker*, es una nueva generación de falsificadores dedicados al crackeo de *hardware*, el *phreak* este se caracteriza por poseer vastos conocimientos en el área de telefonía y el *newbie*: es el típico novato de red, tropieza con una página de *hacking*.

Dentro de la seguridad en la información se lleva a cabo la clasificación de las diferentes opciones para manejar los posibles riegos que un activo o bien puede tener dentro de los procesos de la organización. Esta clasificación lleva el nombre de manejo de riegos, lo cual implica contar con una estructura bien definida y un control adecuado para su respectivo manejo, habiéndolos identificado, priorizado y analizado, a través de acciones factibles y efectivas. Para Cedillo, Arévalo y Moscoso (2017), la gestión de riesgos suele tener los siguientes objetivos vinculados: eliminar los riesgos, reducir a niveles “aceptables” aquellos riesgos que no se pueden eliminar y entonces, convivir con ellos, es decir, aceptarlos ejerciendo cuidadosamente los controles que los mantienen en niveles “aceptables” o transferirlos, por medio de aseguradoras, por ejemplo, a alguna otra organización (p.33).

Imagen 3. Respuesta al riesgo

Fuente: https://slideplayer.es/slide/1650436/

Para lograr una adecuada protección de los activos informáticos, los sistemas de información, los datos y la información, es necesaria la intervención de todo el personal de la empresa, incluyendo a los directivos que deben avalar el proyecto y brindar el apoyo a todo el personal que esté involucrado en el manejo de los activos y sistemas informáticos

CAPÍTULO III: MARCO METODOLÓGICO

En este capítulo se describen todos los aspectos metodológicos que se utilizan para la recopilación de información importante para realizar el análisis y obtener resultados que ayudarán en el diseño de la propuesta metodológica para el adecuado manejo de la seguridad de la información en la Financiera Desyfin.

Enfoque de investigación

Para la presente propuesta se entenderá por método los instrumentos utilizados para determinar el camino para la realización de los objetivos que se plantean por el investigador en un tema determinado. Según Campos (2017), investigar es producir un saber a partir de la experiencia y de la curiosidad. La búsqueda del investigador es producir un saber que, en la medida de lo posible, sea útil y aporte algo nuevo a la sociedad, en relación con el objeto estudiado (p.07).

Se definen tres grandes grupos en los que se clasifican los métodos de investigación de acuerdo con las características y aplicaciones, los cuales se presentan a continuación.

Enfoque cuantitativo

La metodología cuantitativa utiliza la recolección y el análisis de datos para contestar preguntas de investigación y probar hipótesis establecidas previamente, y confía en la medición numérica, el conteo y frecuentemente el uso de estadística para establecer con exactitud, patrones de comportamiento en una población.

Rodríguez Peñuelas (2010) agrega la siguiente descripción del enfoque cuantitativo:

> Señala que el método cuantitativo se centra en los hechos o causas del fenómeno social, con escaso interés por los estados subjetivos del individuo. Este método utiliza el cuestionario, inventarios y análisis demográficos que producen números, los cuales pueden ser analizados estadísticamente para verificar, aprobar o rechazar las relaciones entre las variables definidas operacionalmente, además regularmente la presentación de resultados de estudios cuantitativos viene sustentada con tablas estadísticas, gráficas y un análisis numérico. (p.32)

Enfoque cualitativo

Herrera (2018), citando a Flores, García, & Rodríguez (1996) señala el concepto de enfoque cualitativo como:

> Estudian la realidad en su contexto natural, tal y como sucede, intentando sacar sentido de o interpretar los fenómenos de acuerdo a los significados que tienen para las personas implicadas. La investigación cualitativa implica la utilización y recogida de una gran variedad de materiales, entrevistas, experiencia personal, etc., que describen la rutina, las situaciones problemáticas y los significados en la vida de las personas. (p.124)

Entre las técnicas y los tipos de metodología de investigación cualitativa más populares nos encontramos con la comunicación entre los individuos, como la base de toda ellas, pero existen otras tres las cuales se definen a continuación:

Observación participativa.

El investigador participa del problema o situación a analizar. Vive en primera persona las experiencias y eso es una ventaja a la hora de entender a los sujetos de la investigación. Según Evertson y Merlin (2008), la observación participativa, conocida también como interna o activa, es aquella en la que le investigador selecciona un grupo o colectivo de personas y participa con ellas en su forma de vida y en sus actividades cotidianas con mayor o menor grado de implicación. Su finalidad genérica es obtener información sobre la cultura de ese grupo o población y, en concreto, pretende descubrir las pautas de conducta y comportamiento. (p.29)

Observación no participativa.

El investigador no participa del problema o situación. Dos ejemplos de este tipo de observación son: simulaciones y estudios de caso. En los primeros se crea una situación y los participantes actúan. Se les observa. Y la segunda práctica, lleva a cabo un estudio exhaustivo de una persona o empresa, institución, etc.

Para Evertson y Merlin (2008):

> El investigador se mantiene al margen del fenómeno estudiado, como un espectador pasivo, que se limita a registrar la información que aparece ante él, sin interacción, ni implicación alguna. Se evita la relación directa con el fenómeno, pretendiendo obtener la máxima objetividad y veracidad posible. Este modo de observar es muy apropiado para el estudio de reuniones, manifestaciones, asamblea entre otras y en general para la observación de actividades periódicas de grupos sociales más que para el estudio de su estructura y vida cotidiana. (p.32)

Investigación etnográfica.

Combina los dos tipos de observación anteriores. Se utiliza para extraer el máximo de datos, al aplicarse tanto técnicas participativas como tipos de observación en los que el investigador no se involucra.

Enfoque mixto

Los métodos mixtos combinan la perspectiva cuantitativa y cualitativa en un mismo estudio, con el objetivo de darle profundidad al análisis cuando las preguntas de investigación son complejas. Más que la suma de resultados cuantitativos y cualitativos, la metodología mixta es una orientación con su vocabulario y sus propias técnicas, adaptada en la filosofía con énfasis en las consecuencias de la acción en las prácticas del mundo real.

Enfoque por utilizar

Una vez mencionados y analizados los distintos tipos de métodos de investigación, se puede indicar que el presente estudio se desarrollará bajo el enfoque de los métodos mixtos ya que se tiene una serie de afirmaciones, en donde cada una constituyen una premisa o una afirmación, a la vez se deben aplicar métodos como la observación, el registro de hechos, análisis de riegos, amenazas y clasificación de los hechos. También se debe comprobar que se está cumpliendo con las políticas o procedimientos, en el caso de que existan.

Tipos de investigación

A continuación, se presenta una tipología de investigaciones, la tipología se refiere al alcance que puede tener una investigación.

La tipología considera cuatro clases de investigaciones: exploratorias, descriptivas, correlaciónales y explicativas. En seguida se detalla la naturaleza y el propósito de estos tipos de estudio.

Investigación exploratoria

Una investigación exploratoria es una aproximación que un investigador pueda abordar sobre el objeto de su estudio. Al no existir estudios previos, la investigación exploratoria hace que se tenga una idea aproximada y previa de algo sobre aún no hay información.

Este tipo de investigación resulta muy útil, ya que permitirá tener un primer acercamiento o una primera idea sobre el tema a estudiar, será de gran ayuda para que nos familiaricemos con el mismo.

No existe una metodología determinada y las fuentes de información son libres, por decirlo de otra manera, aquéllas que podamos encontrar: opiniones de expertos, algún artículo de revista, sesiones de un grupo tipo grupo de enfoque para opinar, obtención de formularios entre otros; se trata siempre de una primera etapa, de un estudio previo exploratorio que nos permitirá iniciar investigaciones posteriores, ya con información previa, y en este caso utilizando ya técnicas de estadística y diversas metodologías de estudios de mercado más avanzadas.

Investigación descriptiva

Consiste en llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas. Su meta no se limita a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables.

Se recogen los datos sobre la base de una hipótesis o teoría, exponen y resumen la información de manera cuidadosa y luego analizan minuciosamente los resultados, a fin de extraer generalizaciones significativas que contribuyan al conocimiento.

En esta clase de estudios el investigador debe ser capaz de definir qué se medirá y cómo se logrará. Así mismo, debe ser capaz de especificar quién o quiénes deben incluirse en la medición, a la vez se requiere considerable conocimiento del área que se investiga para formular las preguntas específicas que busca responder.

Investigación correlacional

Este tipo de investigación está indicada para determinar el grado de relación y semejanza que pueda existir entre dos o más variables, es decir entre características o conceptos de un fenómeno.

Ella no pretende establecer una explicación completa de la causa-efecto de lo ocurrido, solo aporta indicios sobre las posibles causas de un acontecimiento

Investigación explicativa

Los estudios explicativos se centran en explicar por qué ocurre un fenómeno y en qué condiciones se da este, o por qué dos o más variables están relacionadas.

Este tipo de investigación se debe plantear muy bien y conocer con exactitud cuál es el evento o tema que se quiere investigar a fondo para crear una investigación con las direcciones correctas que se desean tomar para conseguir información que llegue a conclusiones sólidas sobre lo investigado.

Investigación por utilizar

Una vez que se confirman y evalúan los diversos tipos de investigación, se puede decir que dicha investigación se desarrollará bajos los estudios exploratorios y descriptivos, esto se debe a que ya existen medidas de seguridad básicas, sin embargo, hace falta una mayor recopilación de requerimientos de seguridad, así como un análisis sólido de los controles; además, una descripción detallada de lo que se está investigando y lo que sucede con la investigación en marcha. De esta manera, en esta propuesta se exploran y describen los parámetros del estándar ISO27001 y cómo se usan en el campo de análisis.

Fuentes de información

Se puede deducir que las fuentes de información son tipos de documentos que contienen datos útiles para satisfacer una demanda de información o conocimiento.

Conocer, distinguir y seleccionar las fuentes de información adecuadas para el trabajo que se está realizando es parte del proceso de investigación. Según el nivel de información que proporcionan las fuentes de información, pueden ser primarias y secundarias.

Según García (2019),

> Las fuentes de información son instrumentos para el conocimiento, acceso y búsqueda de la información, su objetivo principal es el de buscar, fijar y difundir la fuente de información implícita en cualquier soporte físico, estas se pueden catalogar desde diferentes perspectivas, sin embargo, cada autor puede elaborar su propia clasificación dependiendo su grado de información. De acuerdo con el grado de información que proporcionan, las fuentes de información se dividen en primarias, secundarias y terciarias; esta división se utiliza generalmente en el ámbito académico. (pp. 57-58)

Fuentes de información primarias

Es una fuente que el investigador crea en un momento específico para resolver un problema concreto, se puede decir que estas fuentes no existen hasta el momento en que se necesitan; para reunirlas se acude a diversas técnicas como la observación, reuniones de grupo, métodos experimentales, encuestas, entrevistas, experiencias de campo o laboratorio, entre otros.

Según Torres y Salazar (2019), “las fuentes primarias son aquellas en las que los datos provienen directamente de la población o muestra de la población.” (p.03)

Fuentes de información secundaria

Son datos o estudios realizados previamente sobre los temas que se desea investigar, los cuales ya existen en algún medio como informes, páginas web, libros, investigaciones previas, documentos, etc. En la investigación documental la recolección de datos se efectúa por medio de fichas. Si es una información secundaria interna es porque ha sido creada en el pasado por el mismo investigador

Según Torres y Salazar (2019), “las fuentes secundarias son aquellas que parten de datos preelaborados, como pueden ser datos obtenidos de anuarios estadísticos, de Internet, de medios de comunicación.” (p.03)

Fuentes de información terciarias

Son documentos que reúnen nombres, títulos de revistas, biografías, publicaciones periódicas, fuentes de internet; recapitula fuentes de segunda mano. Según Ruiz & Jorge (2008):

> las fuentes secundarias contienen información primaria, sintetizada y reorganizada. Están especialmente diseñadas para facilitar y maximizar el acceso a las fuentes primarias o a sus contenidos. Componen la colección de referencia de la biblioteca y facilitan el control y el acceso a las fuentes primarias. (p.3)

Fuente por utilizar en la propuesta

Para la presente propuesta, las fuentes primarias son los funcionarios de la Financiera Desyfin, dado que se realizarán encuestas, entrevistas y una serie de cuestionarios.

En cuanto a las fuentes secundarias, las principales serían: el documento estándar internacional ISO 27001:2013, COBIT5 en español y las Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información (N-2-2007-CO-DFOE), también se toma la literatura de revistas de Internet, libros de auditoría.

Además, como fuentes terciarias, se hace referencias bibliográficas de otros documentos, los cuales ayudan a consolidar la información obtenida con las fuentes primarias y secundarias.

Variables

En el momento en que se desarrolla un trabajo de investigación es frecuente que estén presentes conductas esperadas o cambios inusuales, por lo que en los estudios se implementan las variables con la finalidad de verificar si se cumple lo formulado por el investigador. Según Cauas (2015):

> Se entiende por variable una característica observable ligada, con una relación determinada, a otros aspectos observables. Estas relaciones pueden ser de causalidad, variación, dependencia, asociación, influencia, etc. En los estudios explicativos, la palabra variable siempre se utiliza con este alcance más estricto. (p.3)

Variable conceptual

Corresponde al significado de la variable, para ampliar esta definición, Cauas (2015), "define que en el nivel conceptual se enumeran las propiedades de interés inmediato para la investigación y se postulan la relación entre ellas." (p.4).

Variable operacional

Equivale a hacer que la variable sea medible a través de la concreción de su significado, y está muy relacionada con una adecuada revisión de la literatura.

Según Cauas (2015), "En el nivel operacional, el análisis debe poder establecer las asociaciones o correlaciones existentes entre variables tal como se dan en los datos observados y se verifica si esas relaciones se 'apegan' al modelo conceptual." (p.4).

Variable instrumental

Es el medio o instrumento por el cual recogerá la información, podrían ser varios instrumentos o uno solo para todas las variables, dependiendo de los sujetos que brinden la información y su complejidad.

Para Barragán (2003):

> El conjunto de procedimientos que describen las actividades y operaciones que deben realizarse para medir las variables. Es decir, después de a ver dado una definición, tenemos que ver cómo vamos a "medir las variables" y, para ello, es necesario definirla operacionalmente (p.83)

A continuación, se muestra un cuadro de variables influyentes con su correspondiente información y grado de operación. Además, se observan las herramientas utilizadas para la respectiva recolección de datos, las cuales surgen a través de los objetivos específicos

definidos en el apartado de introducción del presente documento, el cual tiene como finalidad sintetizar una guía para llevar a cabo la investigación sobre el objeto de estudio:

Tabla 4. Análisis de las variables

Objetivo Específico	Variable	Variable Conceptual	Variable Operacional	Variable Instrumental
Crear la política, alcance y objetivos del Sistema de Gestión de Seguridad de la información.	Política	Según un blog de emprendimiento: "Las políticas de seguridad son un conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de la empresa. Se trata de una especie de plan realizado para combatir todos los riesgos a los que está expuesta la empresa en el mundo digital. De esta forma mantendremos nuestra organización alejada de cualquier ataque externo peligroso" (Recuperado de: https://www.emprendepyme.net/politicas-de-seguridad.html)	Elaboración de un conjunto de Políticas y procedimientos de seguridad informática	ISO27001. Excel. Word. Adobe Reader.
Implantar el nivel de cumplimiento de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la ISO 27001:2013 y definir los planes de acción orientados a cerrar las	Objetivos	Según Méndez (2001) "La definición de los objetivos se hace en relación con el problema. Sirven de guía para el estudio, determinan los límites y la amplitud, orientan sobre los resultados que se esperan obtener, y permiten determinar las etapas del proceso del estudio por realizar." (p.05) Méndez, I (2001). El protocolo de investigación. México DF: Trillas.	Diseño de la matriz de riesgo.	Excel

brechas de seguridad encontradas				
Realizar un diagnóstico de la situación actual de la Financiera con relación a los controles de seguridad de información implementados para documentar los hallazgos y oportunidades de mejora en el Departamento de Informática.	Diagnóstico	Según Fernández y Martinez (2015) “El diagnóstico es la instancia en que se estudian los problemas, necesidades y características de la población y su contexto.”(p.02) Martinez, J., & Fernández, A. (2015). El diagnóstico.	Entrevistas Encuestas Observación	Guía de Entrevistas Guía de Encuestas Guía de Observación

Fuente: Elaboración propia.

Instrumentos de recolección de datos

Las técnicas de investigación permiten la recopilación de información para enunciar las teorías que sustentan el estudio de los fenómenos y procesos. Incluye el uso de instrumentos definidos según la fuente documental a que hacen referencia.

Los instrumentos por utilizar durante el desarrollo de esta investigación son la observación mediante una tabla de cotejo.

Partiendo de la definición de observación según Puente (2000), es es una técnica que consiste en observar atentamente el fenómeno, hecho o caso, tomar información y registrarla para su posterior análisis. La observación es un elemento fundamental de todo proceso investigativo; en ella se apoya el investigador para obtener el mayor número de datos. (p.02)

Otros métodos por emplear son los cuestionarios, encuestas y las entrevistas, tomando como explicación los conceptos por presentar.

Puente (2000)menciona que encuesta se explica cómo: la encuesta es una técnica destinada a obtener datos de varias personas cuyas opiniones impersonales interesan al investigador. Para ello, a diferencia de la entrevista, se utiliza un listado de preguntas escritas que se entregan a los sujetos, a fin de que las contesten igualmente por escrito. Ese listado se denomina cuestionario.

Su definición de entrevista: es una técnica que consiste en observar atentamente el fenómeno, hecho o caso, tomar información y registrarla para su posterior análisis. Es una técnica para obtener datos que consisten en un diálogo entre dos personas: El entrevistador "investigador" y el entrevistado; se realiza con el fin de obtener información de parte de este, que es, por lo general, una persona entendida en la materia de la investigación. (p.05)

Población

Los sujetos de información son todas aquellas personas involucradas de una u otra manera en la intervención del estudio y se puede asumir de dos formas: contemplando a todos los involucrados (población) o a un sector o porcentaje de la totalidad (muestra).

La población estudiada es finita, ya que se conoce que el número de empleados que laboran para la Financiera Desyfin es de 210 colaboradores, con los cuales se trabajará en conjunto para obtener la información necesaria para el desarrollo de la propuesta.

Muestra

Se puede entender como muestra como una porción de la población conformada en su totalidad, misma debe considerarse de manera representativa.

A nivel de estadística, la muestra se puede obtener de varias formas, la más común es mediante la aplicación de la fórmula misma que se muestra a continuación:

$$n = \frac{K^2 Npq}{e^2(N-1) + K^2 pq}$$

Donde: n= tamaño de la muestra. N= tamaño de la población. *K*= nivel de confianza.

p= proporción esperada. q=probabilidad de fracaso. e= precisión (margen de error)

Para el caso del nivel de confianza (*K*) es un valor constante que, si se desconoce, se toma en relación con el 95% de confianza, equivalente a 1,96 (como más usual), o con el 99% de confianza, equivalente a 2,58, valor que queda a criterio del investigador.

El margen o posibilidad de error (*e*) es la diferencia que pueda darse entre los resultados obtenidos con la muestra y los que se hubieses obtenido si la encuesta se aplicara a toda la población. Lo ideal es que el margen de error ronde el 5 %.

La cantidad de sujetos de la población que tienen en común la variable que buscamos medir, se indica con la letra (p). El número de individuaos que no comparten esa variable, se marca con (q). En estos casos se coloca 0,5 para ambos.

Basado en la fórmula para determinar la muestra, los sujetos de información serán los colaboradores los cuales se encuentra únicamente en oficinas centrales de la Financiera, dado así una población de 102 individuos.

Aplicando la fórmula para calcular la muestra, en este proyecto se tiene que:

N= 102 *K*: 0.95 *e:* 0.05 *pq*: 0.5

$$n = \frac{(0.95)^2 * (102) * (0.5)}{(0.05)^2 * (75-1) + (0.95)^2 * (0.5)}$$

n= 72

De acuerdo con la aplicación de la fórmula anteriormente expuesta para obtener la muestra ideal para el proyecto, utilizando un margen de error de 0.05 y un nivel de confianza del 95%; la muestra debe ser de 72 colaboradores de la Financiera.

Proceso para la recolección y análisis de datos

Para obtener la información necesaria para la realización de la propuesta, como se mencionó anteriormente, se utiliza la entrevista, encuestas y observación. Las mismas serán aplicadas personalmente en la Financiera Desyfin.

La entrevista se aplicará al gerente de operaciones, jefatura de TI y auditor informático de la Financiera, con el fin de que los conocimientos en el desempeño y procesos diarios de la empresa fueran de ayuda para poder considerar las necesidades que la misma posee para su

producción. Por otra parte, la encuesta será aplicada a una muestra de empleados de la empresa con el fin de conocer la falta de controles de la seguridad de la información.

Con la información recolectada, se analizan los datos y se tomarán en consideración todo lo que en las políticas y procedimientos debe contemplar, con el fin de darle solución a los problemas presentados en la Financiera.

CAPÍTULO IV: ANÁLISIS DE RESULTADOS

Interpretación de resultados

La encuesta efectuada se basó en la utilización de un cuestionario compuesto por 49 preguntas, las mismas son de selección única o múltiple. Esta fue aplicada a una muestra de 72 colaboradores de la Financiera. Cabe destacar que se realizó dos encuestas, la primera fue aplicada al total de la muestra y corresponde a 39 preguntas dado que las preguntas son de carácter general y el segundo cuestionario se aplicó a los compañeros del Departamento de Informática y corresponde a 10 preguntas cuya respuesta dependía del conocimiento técnico del Departamento.

Se realizó la encuesta para cada objetivo de la ISO 27001 aplicable al trabajo de graduación y las preguntas fueron segmentas según a cada control.

La aplicación de estas técnicas de investigación permite conocer la percepción de los colaboradores acerca del tema de la seguridad de la información que se tiene en la actualidad. Seguidamente, se presentan los temas evaluados con la aplicación del cuestionario, con su respectivo trabajo gráfico e interpretación.

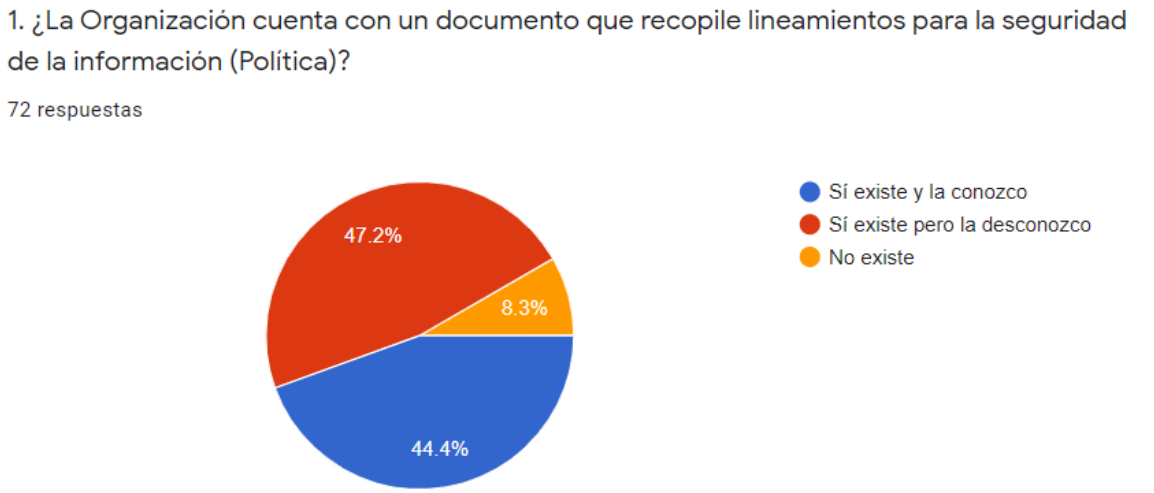
A.5 Política de seguridad de la información.

Objetivo: proporcionar dirección de la gestión y soporte para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.

- Políticas para la seguridad de la información:

La política de seguridad se desarrolla con el fin de preservar la información y los sistemas, garantizando la integridad, confidencialidad y disponibilidad de la información por ende la Dirección de la Financiera debe ser consciente de la necesidad de la gestión de la seguridad y hacer notar su compromiso y apoyo mediante un documento de políticas de seguridad que sea aprobado, publicado y comunicado a los colaboradores.

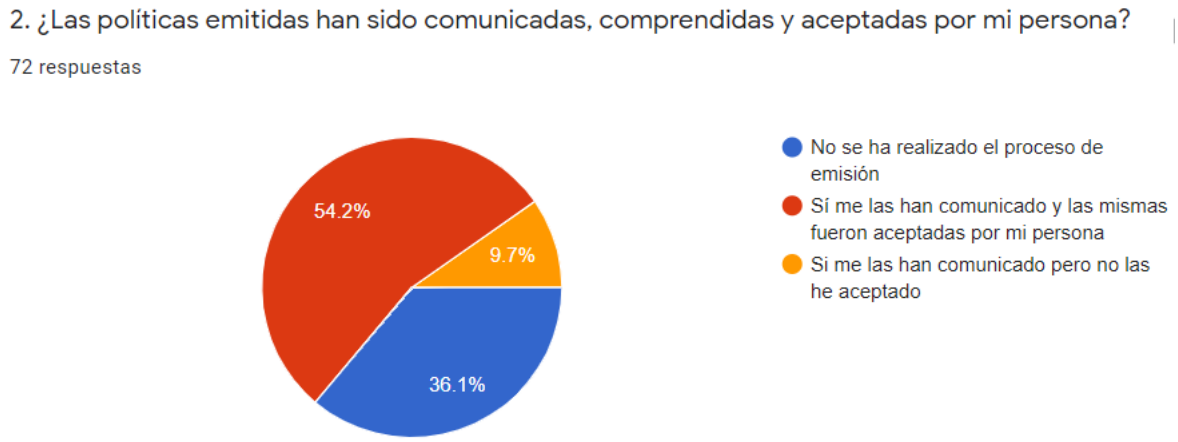
Gráfica 1. Pregunta 1 Política de Seguridad



Fuente: Elaboración propia.

Como respuesta ante la primera pregunta planteada en el cuestionario, se muestra que un 44.4% de los encuestados afirman conocer la política de seguridad, mientras que un 47.2% indican que sí existe, pero la desconocen y el 8.3% duda sobre la existencia de la política de seguridad. Mediante la indagación con Auditoría se valida que existe una política de seguridad, pero la misma se encuentra sin seguimiento desde el año 2014 y no está alineada a las necesidades de la Financiera lo cual puede provocar que los usuarios ejecuten actos que pongan en riesgo la seguridad de la información y no haya controles ni procedimientos para detectarlos, detenerlos ni sancionarlos.

Gráfica 2. Pregunta 2 Política de Seguridad



Fuente: Elaboración propia.

El gráfico de la pregunta dos, muestra la comunicación, comprensión y aceptación de las políticas emitidas, dando el resultado de 36.1% de los encuestados indicando que no se ha realizado el proceso de emisión, un 54.2% confirman que sí se las comunican y son aceptadas por los mismos y para un 9.7% las políticas emitidas fueron comunicadas, pero no han sido aceptadas. Mediante indagación y observación con el Departamento de Informática de la Financiera las políticas se encuentran en un repositorio de la Intranet y por medio de la página de la Financiera se logran visualizar; sin embargo, se resalta que no existe un proceso formal de comprensión y aceptación de las políticas.

- Revisión de las políticas para la seguridad de la información:

Cada política debería tener un propietario con responsabilidad de gestión aprobada para el desarrollo, la revisión y la evaluación de las políticas.

Gráfica 3. Pregunta 3 Política de Seguridad

Fuente: Elaboración propia

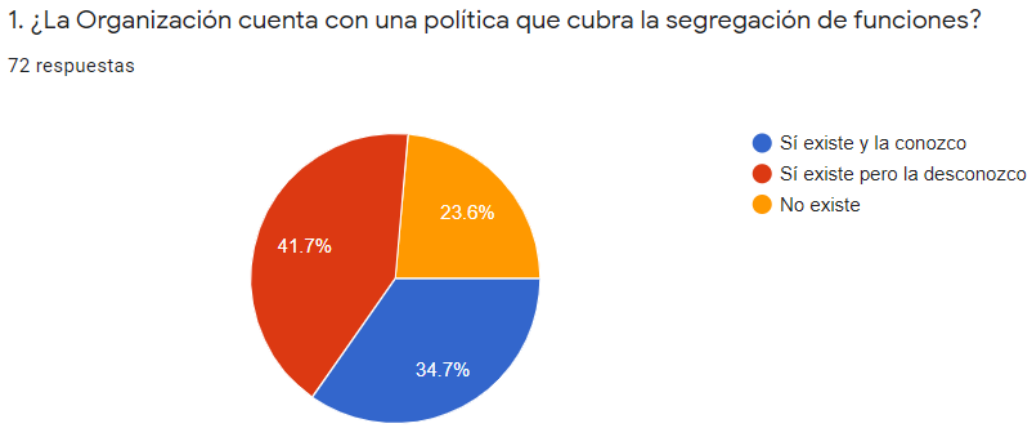
Como se identifica en la gráfica anterior, el 65.3% de los colaboradores afirman que las políticas poseen un formato y estilo consistente y el 34.7% indica que no, esta pregunta se formula debido a que la Financiera solo cuenta con el documento *Manual de Políticas* el cual incluye lineamientos básicos de la seguridad.

A.6 Organización de la seguridad de la información.

Objetivo: establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la organización.

Se debe establecer un marco de gestión para controlar el grado de aplicación de la seguridad de la información dentro de la Financiera, la asignación de las responsabilidades de seguridad de la información se hace de acuerdo con las políticas de seguridad de la información.

Gráfica 4. Pregunta 1 Organización de la Seguridad



Fuente: Elaboración propia

En relación con la pregunta formulada, el 34.7% confirma que sí existe y conoce sobre la política que cubre la segregación de funciones, el 41.7% responde que, sí existe, pero la desconoce, mientras que el 23.6% indica que no existe.

Mediante la indagación al Departamento de Auditoría Informática, se confirma que no existe un documento que cuente con los puntos para cubrir la segregación de funciones; sin embargo algunos colaboradores de la Financiera sí son informados del tema.

- Roles y responsabilidades de seguridad de la información:

Dentro de la Financiera se deben identificar las responsabilidades para la protección de los activos individuales y para la realización de procesos específicos de seguridad de la

información al mismo tiempo se deben definir las responsabilidades locales para la protección de activos y para llevar a cabo los procesos específicos de seguridad.

Gráfica 5. Pregunta 2 Organización de la Seguridad

Fuente: Elaboración propia

El 72.2% de los colaboradores dicen conocer que existe un encargado de la seguridad de la información, mientras que el 27.8% no saben de la existencia del responsable a cargo.

Por tanto, se puede entender que existe una figura que cumple parcialmente con el rol de responsable de seguridad de la información, el cual la mayoría se identificó con el Departamento de Informática, pero no está formalmente establecidas sus funciones, dando un control relativo dentro de la Financiera sobre sus actividades.

- Segregación de funciones:

La separación de funciones es un método para reducir el riesgo del mal uso accidental o deliberado de los activos de la organización.

Gráfica 6. Pregunta 3 Organización de la Seguridad

Fuente: Elaboración propia

En el gráfico se observa que el 66.7% de los encuestados señalan que sí están definidos y asignados los roles acordes al puesto de trabajo, mientras que el 33.3% indica que no. Es necesario analizar las funciones y roles de los colaboradores y segmentar las responsabilidades de cada colaborador con el fin de reducir las oportunidades de una modificación no autorizada o mal uso no intencional de los activos, pudiendo desarrollar que los colaboradores sepan, conozcan su función y rol dentro de la Financiera.

- Contacto con autoridades / Contacto con grupos de interés especial:

La Financiera debe tener procedimientos vigentes que especifiquen cuándo y qué autoridades (por ejemplo, cumplimiento de leyes, organismos reguladores y autoridades de supervisión) deberían contactarse, y cómo identificar los incidentes de seguridad de la información deberían reportarse en el momento oportuno (por ejemplo, si se sospecha que se está incumpliendo la ley), también tener contacto con grupos de interés especial para incrementar el conocimiento sobre las mejores prácticas y mantenerse al día con la información relevante sobre seguridad.

Gráfica 7. Pregunta 4 Organización de la Seguridad

Fuente: Elaboración propia

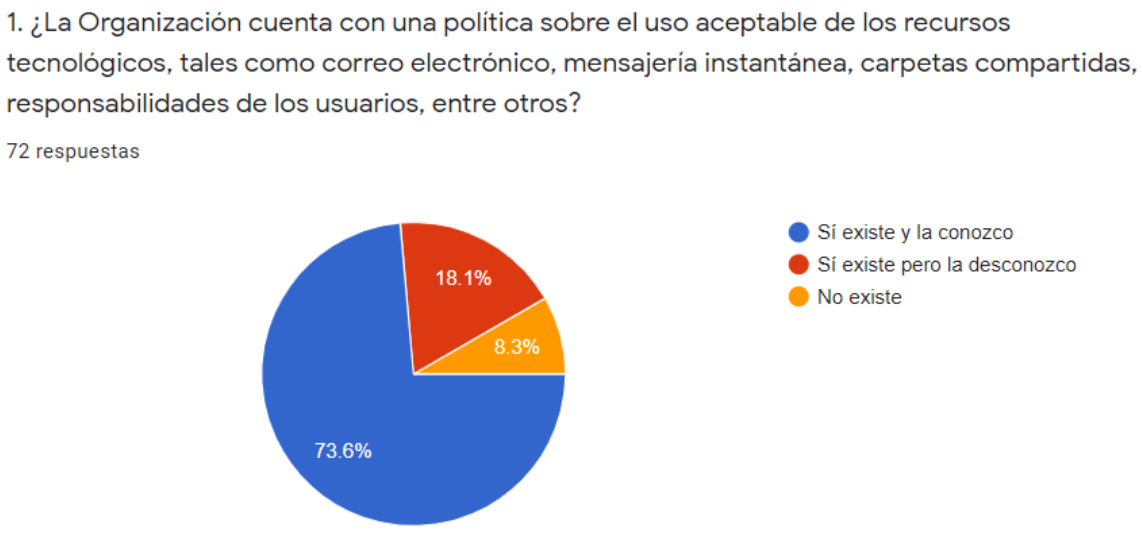
Se muestra que el 54.2% de los encuestados conocen sobre los contactos de grupos de interés y un 45.8% indican que no, esto es debido a una falta de comunicación, dado que la Financiera sí cuenta con los contactos de SUGEF, Cámara de Bancos, firmas auditoras.

A.8 Gestión de activos.

Objetivo: identificar los activos de la organización y definir las responsabilidades para la apropiada protección.

La Financiera debe identificar los activos relevantes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir la creación, elaboración, almacenamiento, transmisión, eliminación y destrucción. La documentación debería mantenerse en inventarios dedicados o existentes, según corresponda.

Gráfica 8. Pregunta 1 Gestión de Activos



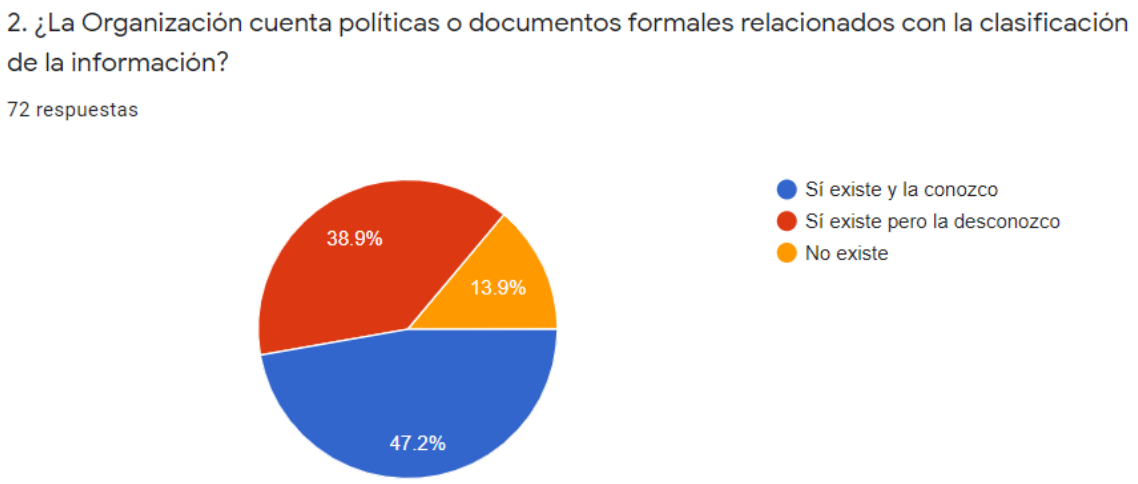
Fuente: Elaboración propia

Para el 73.6% la Financiera sí cuenta y conoce sobre la política del uso aceptable de los recursos tecnológicos, un 18.1% indica que sí existe, pero la desconoce, mientras que el 8.3% no saben si existe dicha política. Mediante la indagación al Departamento de Auditoría, se indica que existe un documento creado en enero del presente año el cual posee reglas sobre el uso aceptable de los recursos tecnológicos, pero no está formalmente establecida.

- Clasificación de la información.

La clasificación les ofrece a las personas que tratan con información, una indicación concisa de cómo manejarla y protegerla. La creación de grupos de información con necesidades de protección similares y la especificación de los procedimientos de seguridad de la información que se aplican a toda la información en cada grupo, facilitan esto. Este enfoque reduce la necesidad de una evaluación de riesgos caso por caso y el diseño personalizado de los controles.

Gráfica 9. Pregunta 2 Gestión de Activos



Fuente: Elaboración propia

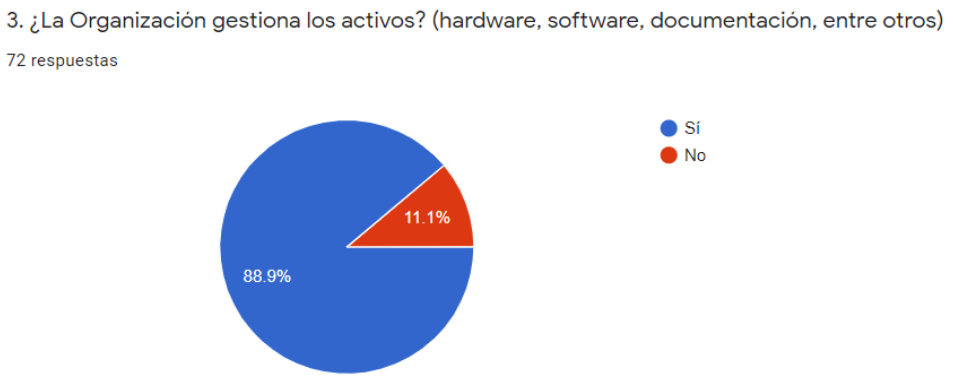
El 47.2% de los encuestados confirman la existencia y conocimiento de la clasificación de la información, el 38.9% indica que sí existe, pero la desconoce y para el 13.9% la Financiera no cuenta con un documento formal que clasifique la información.

Por medio de indagación con Auditoría TI de la Financiera, se confirma que muchos de los colaboradores en especial los más viejos, conocen sobre los lineamientos establecidos en la clasificación de la información, pero no existe una política formal que abarque el control.

- Inventario de Activos

Los inventarios de activos ayudan a garantizar que se logre la protección eficaz, pero también pueden ser requeridos para otros propósitos, como por ejemplo por razones de salud y seguridad, financieras o de seguros (gestión de activos).

Gráfica 10. Pregunta 3 Gestión de Activos



Fuente: Elaboración propia

Para los colaboradores encuestados, el 88.9% confirma sobre la existencia de la gestión de activos para la Financiera mientras que el 11.1% indican que no existe una gestión de activos.

Por medio de indagación con el Auditoría Informática de la Financiera, se evalúa que sí se lleva una correcta gestión de activos que comenzó a regir durante este año

- Eliminación de medios.

Se deben establecer procedimientos formales para la eliminación segura de los medios para minimizar el riesgo de fuga de información confidencial a personas no autorizadas. Los procedimientos para la eliminación segura de los medios que contienen información confidencial deben ser proporcional a la sensibilidad de esa información.

Gráfica 11. Pregunta 4 Gestión de Activos

Fuente: Elaboración propia

El gráfico detalla que el 17.1% de los encuestados indican que la Financiera sí cuenta y conocen sobre la política o documentación formal que regule la eliminación de los activos, para el 48.6% confirman que, sí existe, pero la desconocen y el 34.3% asegura que la Financiera no cuenta con la política o documentación para la eliminación de los activos.

Por medio de indagación con auditoría se comprueba que la Financiera no posee un documento o política que regule la eliminación de los activos.

- Transferencia de medios físicos.

La información puede ser vulnerable al acceso no autorizado, mal uso o corrupción durante el transporte físico, por ejemplo, al enviar los medios a través del servicio postal o por mensajería. En este control, los medios incluyen los documentos en papel.

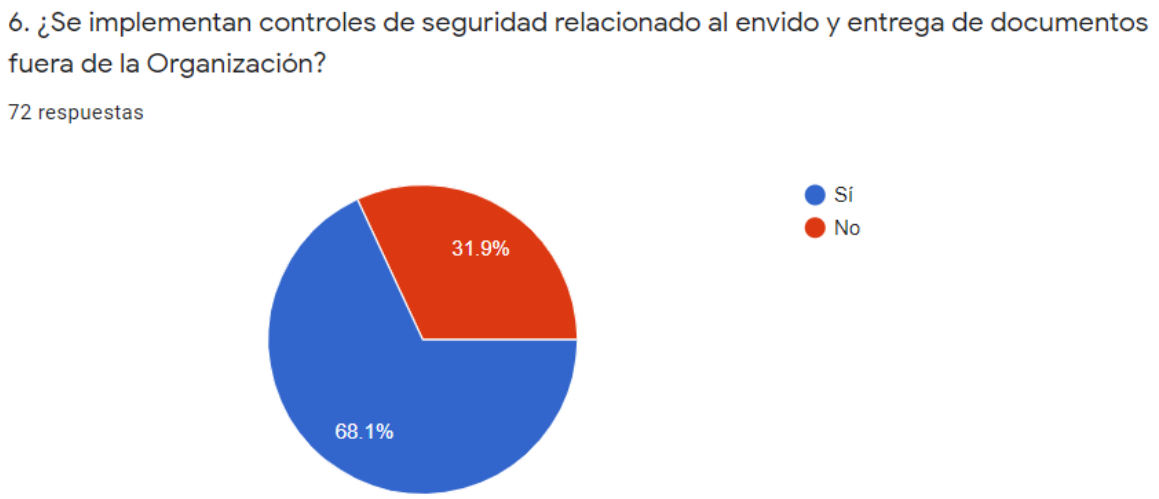
Gráfica 12. Pregunta 5 Gestión de Activos

Fuente: Elaboración propia

El 58.3% de los colaboradores encuestados indican que sí se cuenta con una política o documentación formal relacionada con el servicio de información enviada fuera de la Financiera; el 41.7% manifiestan que no se cuenta con política o documentación formal para este control.

Se realiza indagación con el Departamento de Auditoría de la Financiera y se valida que no existe una política o documento formal que cubra las necesidades dictadas por el control, muchos de los colaboradores conocen los lineamientos básicos para la información que es enviada fuera de la Financiera, pero no se encuentra documentada.

Gráfica 13. Pregunta 6 Gestión de Activos



Fuente: Elaboración propia

Cuando la información confidencial en los medios no se encuentra cifrada, debería considerarse la protección física adicional de los medios, aquí surge la última pregunta relacionada a la transferencia de los medios, se indaga si el envío y entrega de los documentos fuera de la Financiera poseen un tipo de control de seguridad y el 68.1% de los encuestados confirman que sí se cuentan bajo controles de seguridad y el 31.9% indican que no se cuenta con ningún tipo de seguridad.

Se realiza indagación con el Departamento de Auditoría de la Financiera y se valida que no existen controles de seguridad implementados al momento que la información es enviada o entregada fuera de las instalaciones de la Financiera.

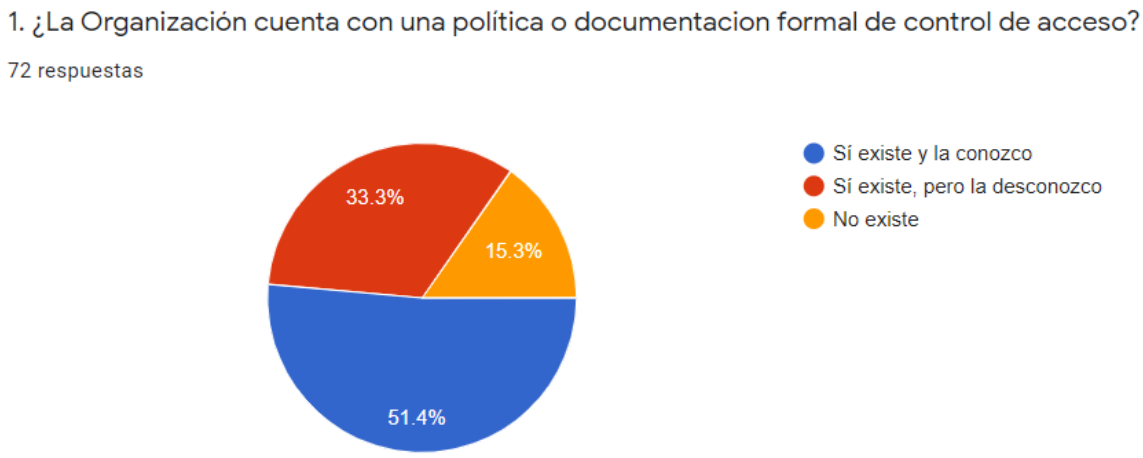
A.9 Control de accesos.

Objetivo: limitar el acceso a la información y a los recursos de procesamiento de la información.

Los propietarios de los activos deberían determinar las reglas de control de acceso, los derechos y las restricciones para las funciones específicas de los usuarios con respecto a sus activos con el nivel de detalle y el rigor de los controles que reflejan los riesgos asociados

de seguridad de la información; las reglas de control de acceso deberían ser soportadas por procedimientos formales y responsabilidades definidas.

Gráfica 14. Pregunta 1 Control de Acceso



Fuente: Elaboración propia

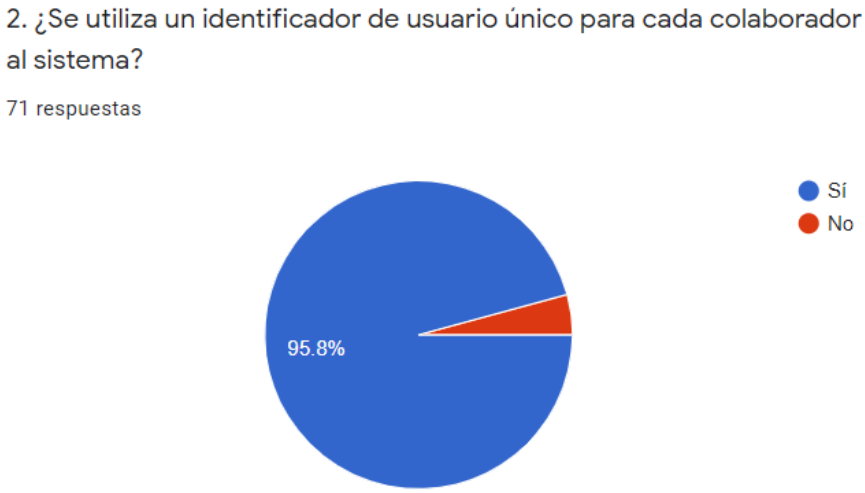
Con base en el gráfico anterior, se observa que un 51.4% indica que sí existe y conoce sobre la política o documento formal de control de acceso, mientras un 33.3% indica que sí existe una política o documento formal, pero la desconoce y el 15.3% señal que no existe política ni documento sobre gestión de acceso.

Se realiza una validación con el Departamento de Auditoría y se confirma que la Financiera no cuenta con un documento formal de control de acceso.

- Procedimientos de accesos seguros.

El procedimiento para iniciar sesión en un sistema o aplicación debería ser diseñado para minimizar la oportunidad de acceso no autorizado. Por lo tanto, el proceso de conexión debería divulgar el mínimo de información sobre el sistema o aplicación, de manera de evitar proveer a un usuario no autorizado con asistencia innecesaria.

Gráfica 15. Pregunta 2 Control de Acceso



Fuente: Elaboración propia

Se valida que el 95.8% de los colaboradores de la Financiera cuentan con un usuario único para el ingreso al sistema, mientras que el 4.2% indican que no, los tres colaboradores los cuales indican que tienen más de un usuario corresponden a los del Departamento de Informática y cuentan con los roles de súper usuarios del *Active Directory*.

- Registro y cancelación de registro de usuarios.

Proporcionar o revocar el acceso a la información o a las instalaciones de procesamiento de información es, por lo general, un procedimiento de dos pasos:

- Asignar y permitir, o revocar el ID de usuario.

- Proporcionar o revocar los derechos de acceso a dicho ID de usuario.

Gráfica 16. Pregunta 3 Control de Acceso

Fuente: Elaboración propia

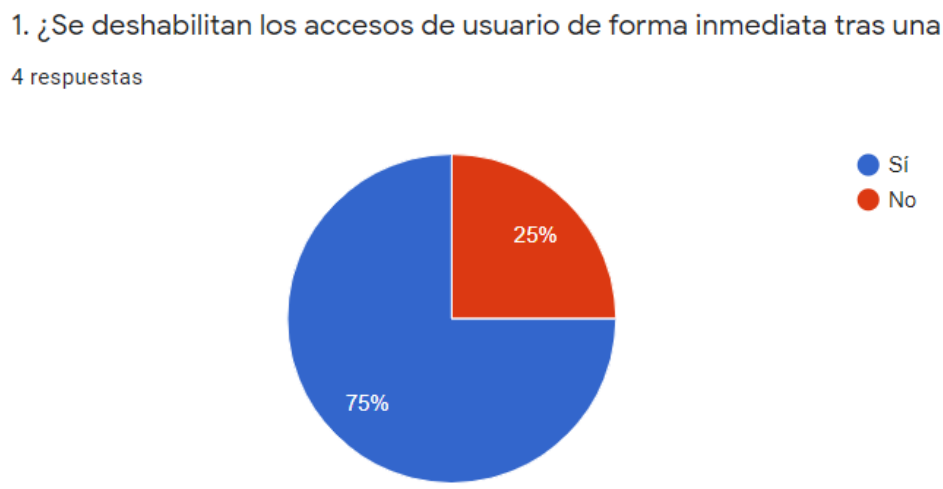
Se puede observar en el gráfico anterior, que el 76.1% afirma conocer el procedimiento formal para la gestión de acceso a los sistemas, mientras que el 21.1% indica que sí existe un procedimiento formal, pero, desconocen del mismo y el 2.8% manifiesta que no existe. Mediante indagación al Departamento de Auditoría Informática de la Financiera, se valida que no hay un documento formal, con lo que se cuenta son con directrices.

- Remoción o ajuste de los derechos de acceso.

Cuando ocurre la desvinculación, los derechos de acceso de un individuo a la información y los activos asociados con instalaciones de procesamiento de información y servicios deberían removerse o suspenderse.

En casos que la desvinculación sea iniciada por la dirección, los empleados o usuarios de terceras partes contrariados pueden deliberadamente dañar información o sabotear equipamiento de procesamiento de información. En casos de personas que renuncian o son despedidas, podrían estar tentados a recoger información para uso futuro.

Gráfica 17. Pregunta 1 TI - Control de Acceso



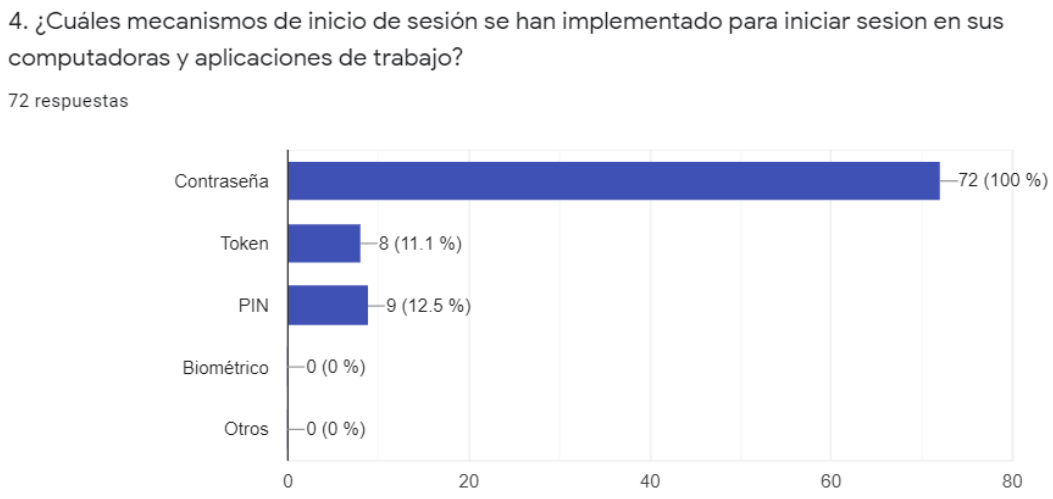
Fuente: Elaboración propia

La pregunta formulada en el gráfico anterior se realiza directamente al Comité de Informática el cual confirma que los accesos a los usuarios sí se deshabilitan de forma inmediata tras un despido, el mismo se realiza por orden directa del jefe del colaborador o Recursos Humanos.

- Sistema de gestión de contraseñas.

Cuando se requiere una fuerte autenticación y verificación de la identidad, deberían utilizarse métodos alternativos a las contraseñas, tales como medios criptográficos, tarjetas inteligentes, señales o medios biométricos.

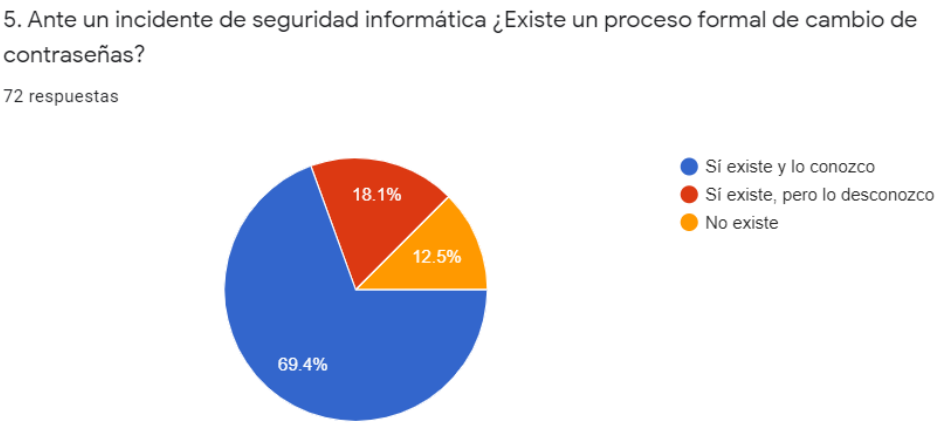
Gráfica 18. Pregunta 4 Control de Acceso



Fuente: Elaboración propia

A partir del gráfico anterior, se puede indicar que el mecanismo implementado para iniciar sesión a las computadoras y aplicaciones de trabajo dentro de la Financiera corresponde a la contraseña con un 100%, mientras que otros colaboradores utilizan también Token y PIN. Por tanto, Informática debe velar para que a los colaboradores se les brinde las herramientas adecuadas con el fin de que gestionen de una mejor manera la confección y uso de las contraseñas, sesiones desatendidas y el entorno de trabajo con el objetivo de que se realice una correcta gestión de la seguridad de la información dentro de la Financiera. Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas; las contraseñas son una forma común de proporcionar identificación y autenticación basada en un secreto que solo el usuario conoce. La fuerza de la autenticación del usuario debería ser adecuada a la clasificación de la información a ser accedida.

Gráfica 19. Pregunta 5 Control de Acceso



Fuente: Elaboración propia

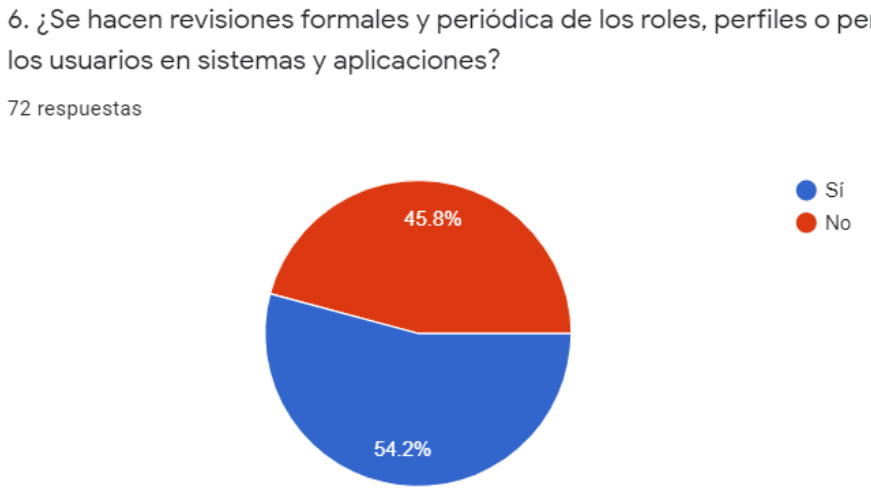
Como se muestra en la gráfica anterior, el 69.4% conoce sobre el proceso formal de cambio de contraseña, mientras un 18.1% desconoce cómo se realiza y el 12.5% afirma que no existe un proceso formal de cambio de contraseña en caso de un incidente de seguridad informática.

Se indaga con el Departamento de Auditoría y se comunica, que no existe un proceso formal de cambio de contraseña, lo que se posee son directrices y el año pasado se presentó un problema de seguridad por el cual los usuarios debieron realizar un cambio de contraseña guiado.

- Revisión de los derechos de acceso de los usuarios.

Los derechos de acceso de usuarios deberían revisarse a intervalos regulares, y luego de cualquier cambio, tal como una promoción, una degradación, o terminación del empleo.

Gráfica 20. Pregunta 6 Control de Acceso



Fuente: Elaboración propia

De acuerdo con el gráfico anterior, el 54.2% de los colaboradores afirman que sí se realizan revisiones formales a los usuarios para los accesos de sistemas y aplicaciones, mientras que un 45.8% indica que no se realizan estas revisiones. Se indaga con el Departamento de Auditoría Informática y se confirma que no se realizan una revisión formal de roles, perfiles o permisos a los aplicativos de la Financiera.

Para evidenciar la afirmación de falta de revisión de roles, perfiles o permisos, se realiza una pregunta directa al Comité de Informática referente a los roles con mayor privilegio debido a que el uso inapropiado de los privilegios de administración del sistema (cualquier característica o recurso de un sistema de información que habilite al usuario a hacer caso omiso de los controles del sistema o de la aplicación) puede ser un factor importante de contribución a las fallas o violaciones de los sistemas.

Gráfica 21. Pregunta 2 TI - Control de Acceso

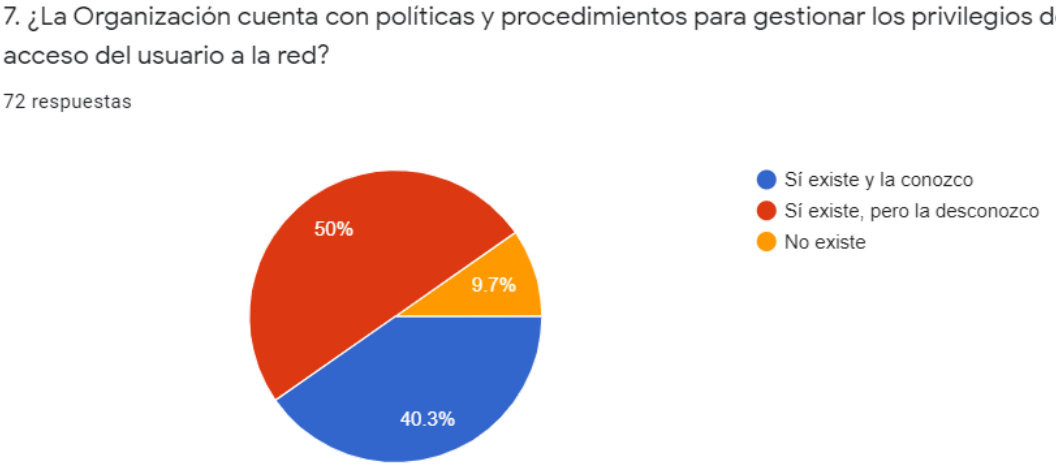
Fuente: Elaboración propia

Como se evidencia en el gráfico anterior, no se realiza una revisión de los derechos de usuarios con mayor privilegio por ende la Financiera está expuesta eventualmente a la sustitución de información, eliminación de datos importantes por error humano o de manera intencionada, desconocimiento de fraude, robo por accesos indebidos a datos sensibles.

- Acceso a redes y servicios de red.

La política sobre el uso de servicios de red debería ser coherente con la política de control de acceso de la organización, conexiones no autorizadas o inseguras a servicios de red pueden afectar a toda la organización.

Gráfica 22. Pregunta 7 Control de Acceso



Fuente: Elaboración propia

Como se observa en el gráfico anterior, el 50% de los colaboradores encuestados indican que sí existe una política y procedimiento para la gestión de privilegios de acceso a la red pero, desconocen de la misma, un 40.3% de los encuestados, dicen que existe y conocen sobre esta política y el 9.7% menciona que no se cuenta con política ni procedimiento para gestionar los privilegios de acceso del usuario a la red.

Se verifica con el Departamento de Auditoría Informática que no existe un documento formal, los colaboradores solo gestionan el caso e Informática lo atiende.

Este control es particularmente importante para conexiones de red a aplicaciones sensibles o críticas del negocio o de usuarios en ubicaciones de alto riesgo, por ejemplo, áreas públicas o externas que están fuera de la gestión de seguridad de la información y control de la organización.

Gráfica 23. Pregunta 3 TI - Control de Acceso

Fuente: Elaboración propia

Se evidencia que la Financiera cuenta con medidas para garantizar la seguridad en las redes. Sobre este tema se consulto al Comité de Informática arrojando un resultado positivo en las medidas de seguridad de redes.

- Control de acceso al código fuente de programas:

El acceso al código de programas fuente y artículos asociados (como diseños, especificaciones, proyectos de verificación y proyectos de validación) debería ser

estrictamente controlado, para prevenir la introducción de una funcionalidad no autorizada, evitar cambios involuntarios, así como a mantener la confidencialidad de la propiedad intelectual valiosa. Para el código de programas fuente, puede alcanzarse por almacenamiento centralizado controlando de dicho código, preferentemente en las bibliotecas de programas fuentes.

Gráfica 24. Pregunta 4 TI - Control de Acceso

Fuente: Elaboración propia

La gráfica anterior muestra que los códigos fuentes de programas si son almacenados en bibliotecas o repositorios, cabe señalar que el Departamento de Informática no desarrolla programas para la Financiera, pero sí tiene custodia del código de las aplicaciones.

A.11 Seguridad física y ambiental

Objetivo: Prevenir el acceso físico no autorizado, daños e interferencia a la información y a los recursos de procesamiento de la información de la organización.

- Perímetro de seguridad física.

La protección física puede ser alcanzada creando una o más barreras físicas alrededor de las premisas de la organización y de las instalaciones de procesamiento de la información. El

uso de múltiples barreras brinda protección adicional, mientras que la falta de una barrera no significa que la seguridad se vea comprometida inmediatamente.

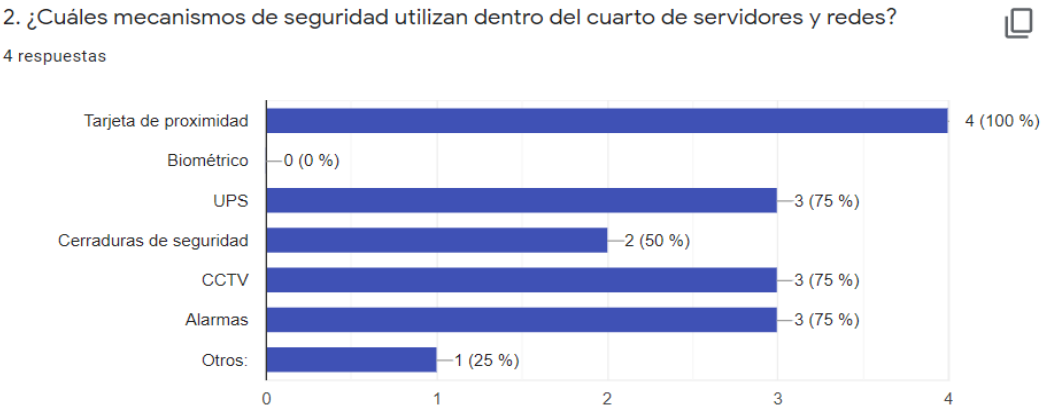
Gráfica 25. Pregunta 1 TI - Seguridad física y ambiental

Fuente: Elaboración propia

El gráfico anterior muestra que el acceso al cuarto de servidores y redes sí se encuentra restringido al personal respectivo de acuerdo con su rol dentro de la Financiera.

Deberían adoptarse controles para reducir al mínimo el riesgo de amenazas físicas potenciales, como ser: hurto, fuego, explosivos, humo, inundaciones (o falta de suministro de agua), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, interferencia de las comunicaciones, radiación electromagnética, y vandalismo.

Gráfica 26. Pregunta 2 TI - Seguridad física y ambiental



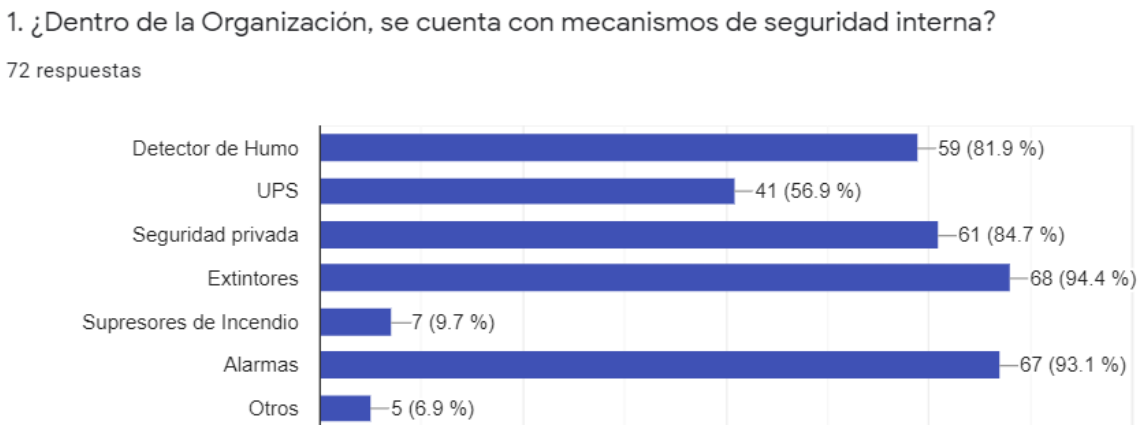
Fuente: Elaboración propia

Con base al gráfico anterior, la Financiera sí cuenta con mecanismos de seguridad dentro del cuarto de servidores y redes aportando elementos de protección especial para no verse afectado de manera negativa ante una eventualidad causada por una amenaza física.

- Trabajando en áreas seguras.

Los acuerdos para trabajar en áreas seguras incluyen controles para los empleados y los usuarios de terceras partes que trabajan en el área segura, así como otras actividades de terceros que ocurren allí.

Gráfica 27. Pregunta 1 - Seguridad física y ambiental

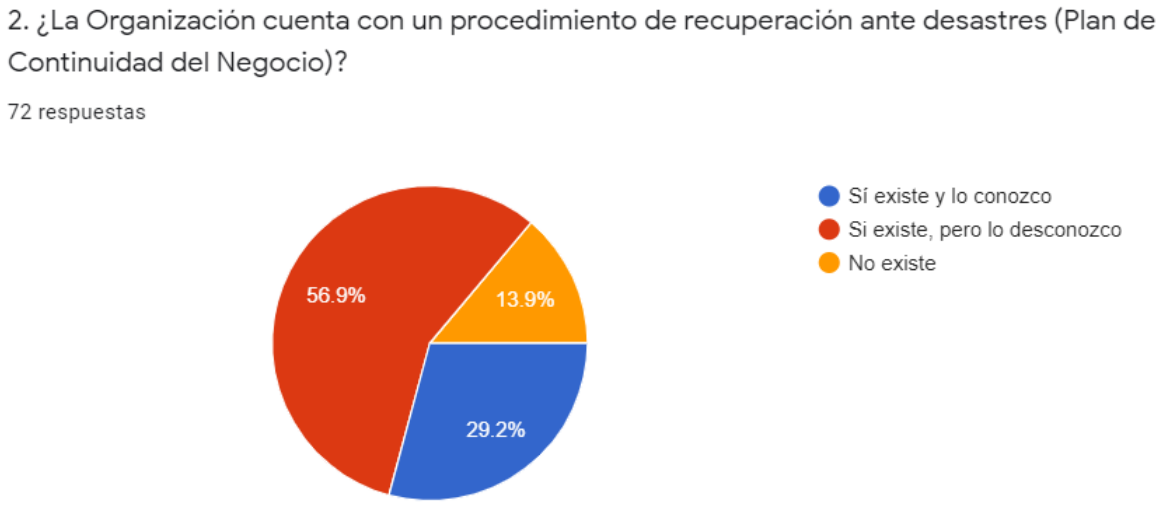


Fuente: Elaboración propia

La Financiera sí cuenta con mecanismos de seguridad interna para los colaboradores, aportando elementos de protección para no verse afectado de manera negativa ante una eventualidad causada por una amenaza física, dentro de otros elementos se destacan las cámaras de vigilancia, planta de respaldo, puertas de acceso por medio de gafete, entre otros.

Un Plan de Continuidad Empresarial es un documento que consta de la información crítica que necesita una empresa para continuar operando durante un evento no planificado. El Plan de Continuidad Empresarial debe establecer las funciones esenciales de la empresa, identificar qué sistemas y procesos deben mantenerse y detallar cómo mantenerlos. En él se debe tener en cuenta cualquier posible interrupción del negocio.

Gráfica 28. Pregunta 2 - Seguridad física y ambiental



Fuente: Elaboración propia

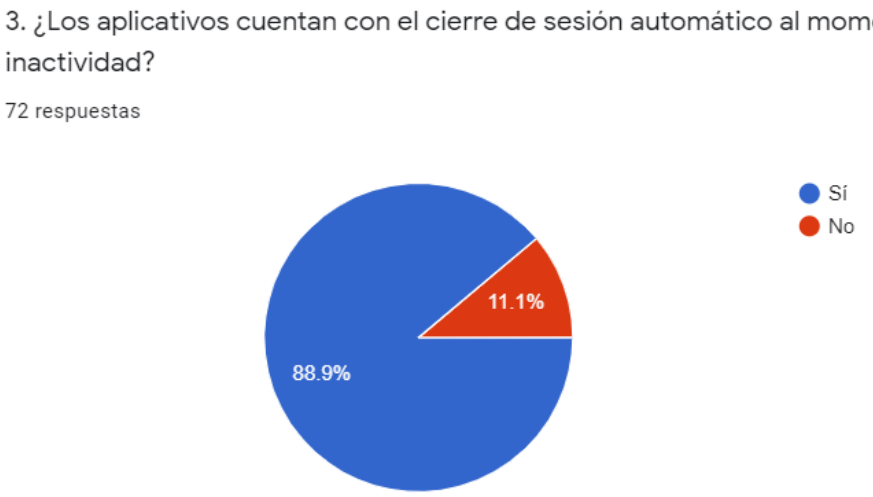
El 56.9% de los encuestados indican que sí existe un Plan de Continuidad del Negocio, pero lo desconocen, un 29.2% afirma la existencia y conocimiento del Plan de Continuidad del Negocio y un 13.9% indica que no existe un Plan de Continuidad del Negocio.

Mediante una indagación con el Departamento de Auditoría, se valida la existencia de un Plan de Continuidad del Negocio el cual es actualizado y solo es de conocimiento del personal que cumple el rol de ejecutor.

- Equipamiento desatendido por el usuario:

Todos los usuarios deberían ser advertidos de los requisitos y procedimientos de seguridad para proteger equipamiento desatendido, así como de su responsabilidad de implementar tal protección.

Gráfica 29. Pregunta 3 - Seguridad física y ambiental



Fuente: Elaboración propia

Como se muestra en el gráfico anterior, el 88.9% de los usuarios afirman que sí se cuenta con el cierre automático de las sesiones por un periodo de inactividad y el 11.1% indica que no.

Se realiza una indagación y observación a los aplicativos de la Financiera y se confirma que sí se cuenta con el cierre automático de sesión a los aplicativos utilizado por los usuarios.

- Política de escritorio y pantalla limpios:

Una política de escritorio y pantalla limpios reduce los riesgos de acceso no autorizado, pérdida o daño a la información durante y fuera de las horas normales de trabajo. Cofres u otras formas de almacenamiento seguro pueden también proteger información almacenada dentro de ellas contra desastres tales como incendios, terremotos, inundaciones o explosiones, se realiza la siguiente pregunta a los colaboradores debido a que por la emergencia actual del COVID 19 la Financiera recién comunicó una política de escritorio limpios a todos los colaboradores.

Gráfica 30. Pregunta 4 - Seguridad física y ambiental

Fuente: Elaboración propia

Se evidencia que el 90.3% de los colaboradores ya fueron informados por la política de zona de trabajo limpias y despejadas, el 6.9% sabe que existe, pero la desconoce y el 2.8% no conocen de la nueva política de escritorio y pantalla limpios.

Por ende se evidencia una mala comunicación de las políticas a los colaboradores de la Financiera, dado que se confirma que la política fue enviada por correo electrónico.

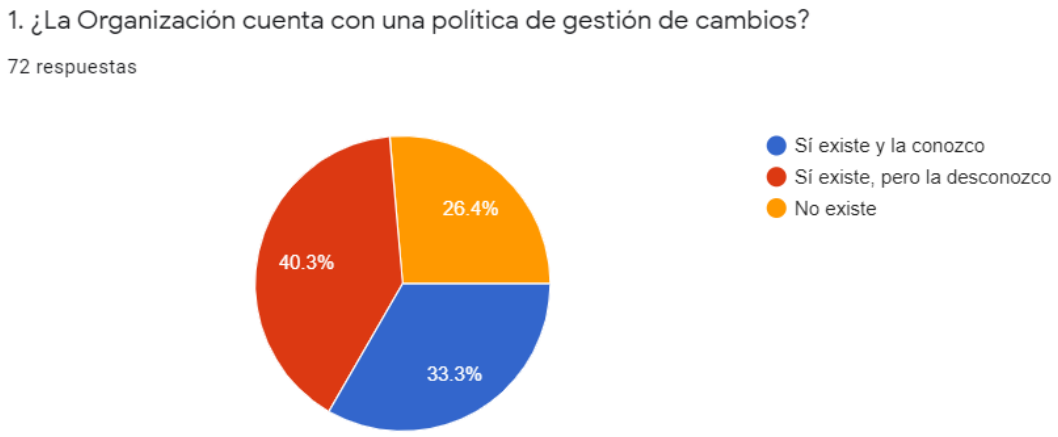
A.12 Seguridad de las operaciones

Objetivo: asegurarse de las operaciones correctas y seguras de los recursos de procesamiento de la información.

- Gestión de cambios:

Se deben establecer las responsabilidades y los procedimientos formales de gestión para asegurar el control satisfactorio de todos los cambios. Cuando se realizan los cambios, debería conservarse un registro de auditoría que contenga toda la información relevante.

Gráfica 31. Pregunta 1- Seguridad de las operaciones

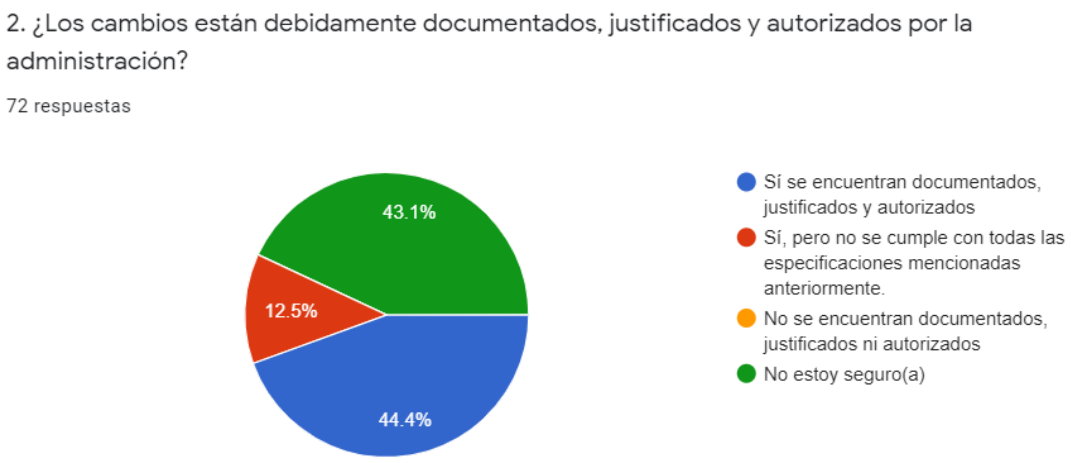


Fuente: Elaboración propia

En el gráfico anterior, un 33.3% sí conoce sobre la política de gestión de cambios, un 40.3% señala que sí existe, pero desconocen de la política y un 26.4% afirma que no existe una política de gestión de cambios. De acuerdo con las conversaciones con la Gerencia y analizando las encuestas, la administración debe crear un documento que incluya todos los procedimientos que correspondan y que se den a conocer a todos los usuarios de la organización.

El control inadecuado de cambios en las instalaciones y los sistemas de procesamiento de la información es una causa común de las fallas del sistema o de la seguridad. Cambios al ambiente operacional, especialmente al transferir un sistema en desarrollo al estado operacional, pueden afectar la confiabilidad de las aplicaciones.

Gráfica 32. Pregunta 2- Seguridad de las operaciones



Fuente: Elaboración propia

De acuerdo al gráfico anterior, se valida que un 43.1% de los usuarios no están seguros si los cambios son debidamente documentados, justificados y autorizados por la administración, mientras que un 12.5% afirman que no se cumplen con todas las especificaciones y el 44.4% menciona que sí se encuentran documentados, justificados y autorizados. Por medio de una indagación se confirma que muchos de los cambios recaen sobre el aplicativo SAP por lo que la especialista de la herramienta sigue un proceso al momento de ser solicitado un cambio, pero para otros aplicativos no se cuenta con un proceso formal de cambios.

- Instalación de *software* en los sistemas en operación:

El *software* de computador puede depender de *software* y módulos suministrados externamente, lo cual debería supervisarse y controlarse para evitar cambios no autorizados que puedan introducir debilidades de seguridad.

Gráfica 33.Pregunta 3- Seguridad de las operaciones

Fuente: Elaboración propia

Del gráfico anterior, el 61.1% afirma que sí existe una política sobre la instalación de *software*, pero desconocen de la misma, un 27.8% señala que conocen sobre la política y un 11.1% afirma que la Financiera no cuenta con una política de instalación de *software*. Por medio de la indagación al Departamento de Auditoría Informática, se valida que actualmente no se posee un documento formal que cumpla con este punto del control.

- Restricciones en la instalación de *software*:

La instalación descontrolada de *software* en los dispositivos informáticos puede conducir a la introducción de vulnerabilidades y luego a la fuga de información, pérdida de integridad o de otros incidentes de seguridad de la información, o de violación de los derechos de propiedad intelectual.

Gráfica 34. Pregunta 4 - Seguridad de las operaciones

Fuente: Elaboración propia

En la gráfica anterior, se valida que el 93.1% de los encuestados comprenden y entienden que quienes realizan las instalaciones de *software* a las computadoras de la Financiera corresponde al Departamento de Informática, mientras que el 6.9% no está seguro sobre si la instalación de *software* se encuentra limitada al personal autorizado. Se realiza una indagación a Informática y se valida que solo los usuarios con privilegios con rol de administrador de dominio pueden realizar instalaciones de *software* dentro de la Financiera.

- Separación de ambientes de desarrollo, pruebas y operación:

Si el personal de desarrollo y de prueba tiene acceso al sistema operacional y a su información, puede introducir código no autorizado y no comprobado o alterar datos operacionales. En algunos sistemas, esta capacidad podría ser utilizada para realizar fraude, o introducir código no comprobado o malicioso, que puede causar problemas operacionales serios.

Gráfica 35. Pregunta 5 TI - Seguridad de las operaciones

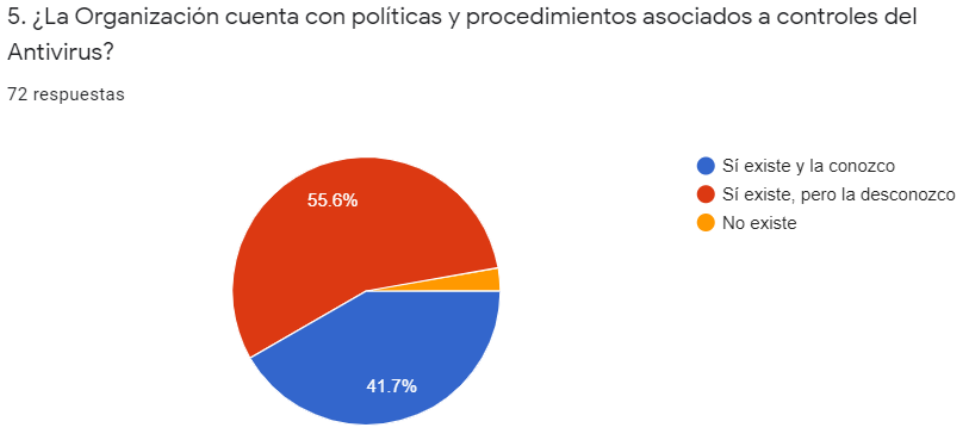
Fuente: Elaboración propia

Con base en el gráfico anterior, por medio de indagación y observación se valida que el único ambiente que maneja desarrollo dentro de la Financiera corresponde al aplicativo SAP y es por medio de un tercero: sin embargo, la aplicación sí cuenta con los tres ambientes los cuales son separados, independientes y correctamente identificados y solo la dueña de SAP tiene acceso a los tres ambientes.

- Controles contra el código malicioso:

El uso de la detección de *software* malicioso y *software* de la reparación solo como control de *software* malicioso no suele ser suficiente y normalmente debería acompañarse por procedimientos operativos que impidan la introducción del *software* malicioso.

Gráfica 36. Pregunta 5 - Seguridad de las operaciones



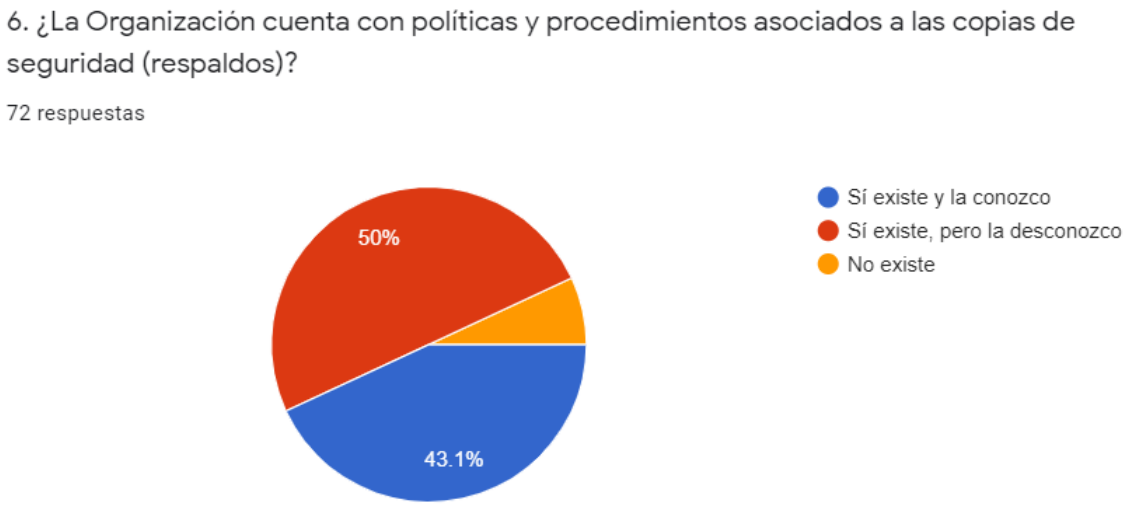
Fuente: Elaboración propia

Del gráfico anterior, se observa que el 55.6% indica que sí existe una política y procedimientos asociados a controles del antivirus, pero la desconocen; un 41.7% afirma conocer la política y el procedimiento y un 2.8% menciona que no existe una política, lo que posee la Financiera son directrices del uso del antivirus.

- Respaldo de la información:

La Financiera debe proporcionar instalaciones adecuadas de copias de respaldo de seguridad para garantizar que toda la información y *software* esenciales se pueden recuperar después de un desastre o falla en la comunicación.

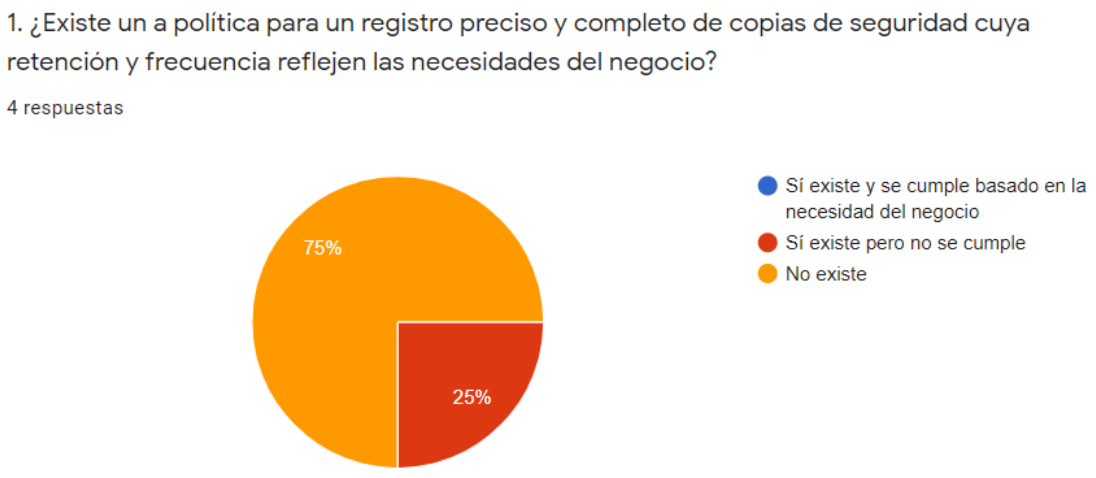
Gráfica 37. Pregunta 6 - Seguridad de las operaciones



Fuente: Elaboración propia

En la anterior gráfica se observa que un 50% indica desconocer la política de respaldos, pero afirma que sí existe, un 43.1% conoce sobre la política y un 6.9% señala que no existe. Por medio de una indagación se confirma que sí existe un documento escrito el cual menciona el tema de respaldos dentro de la Financiera, pero no se encuentra alineado a la necesidad del negocio, por lo que se formula una pregunta al Comité de Informática.

Gráfica 38. Pregunta 6 TI - Seguridad de las operaciones



Fuente: Elaboración propia

Como se muestra en la gráfica anterior, con el 75% se confirma que no existe una política para el registro preciso y completo de las copias de seguridad y que indique la retención y frecuencia de acuerdo con las necesidades de la Financiera. Por tanto, la administración debe realizar un esfuerzo importante para tener implementado al cien por ciento los temas con las copias de seguridad con el fin de que, si se presenta un desastre, se pueda realizar una recuperación puntual y así reducir el riesgo de pérdida de información.

- Controles de auditoría de sistemas de información:

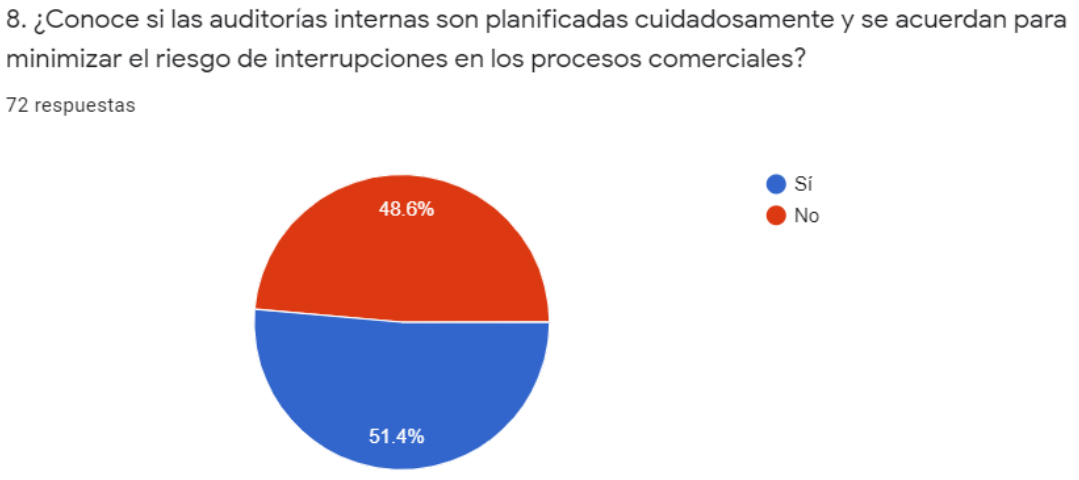
La auditoría informática busca analizar la información que es gestionada y almacenada dentro y fuera de los sistemas informáticos, con el objetivo de identificar, enumerar y evaluar, los controles que se tengan implementados para garantizar su confidencialidad, integridad y disponibilidad por lo que debe planificarse cuidadosamente y acordarse los requisitos y actividades de auditoría que impliquen verificaciones en los sistemas en producción, para minimizar el riesgo de interrupción de los procesos de negocio.

Gráfica 39. Pregunta 6 - Seguridad de las operaciones

Fuente: Elaboración propia

Por medio de indagación con el Departamento de Auditoría Informática se confirma que la Financiera sí se somete a un proceso de auditoría, por lo que el 86.1% lo afirman y el 13.9% indican que no se someten a un proceso de auditoría.

Gráfica 40. Pregunta 7 - Seguridad de las operaciones



Fuente: Elaboración propia

El proceso de auditoría si es planificado y se realiza para minimizar el riesgo de interrupciones en los procesos comerciales por lo que, en el gráfico anterior, el 51.4% comprende el proceso que lleva auditoría dentro de la Financiera y el 48.6% no.

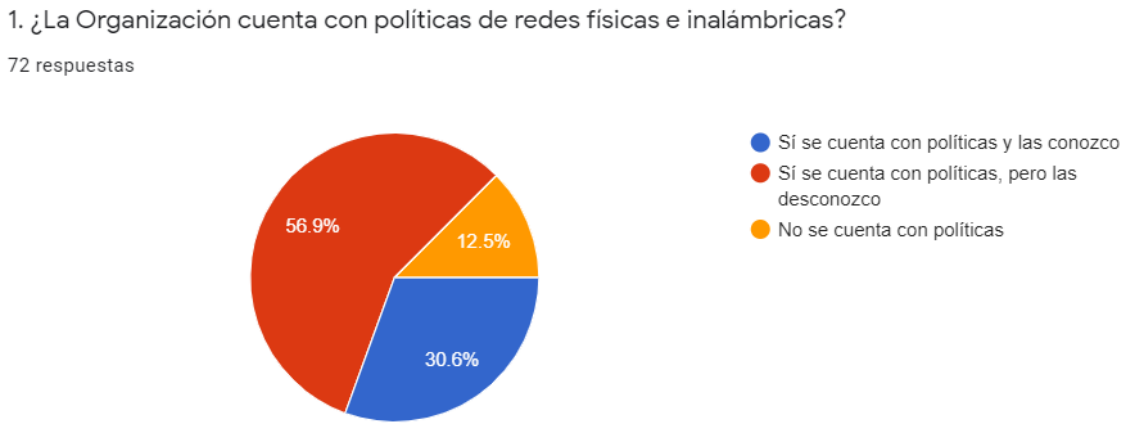
A.13 Seguridad de las comunicaciones

Objetivo: asegurar la protección de la información en las redes y sus recursos de soporte de procesamiento de información.

- Controles de red:

Los controles deberían implantarse para garantizar la seguridad de la información en las redes y la protección de los servicios conectados no autorizados.

Gráfica 41. Pregunta 1 - Seguridad de las comunicaciones



Fuente: Elaboración propia

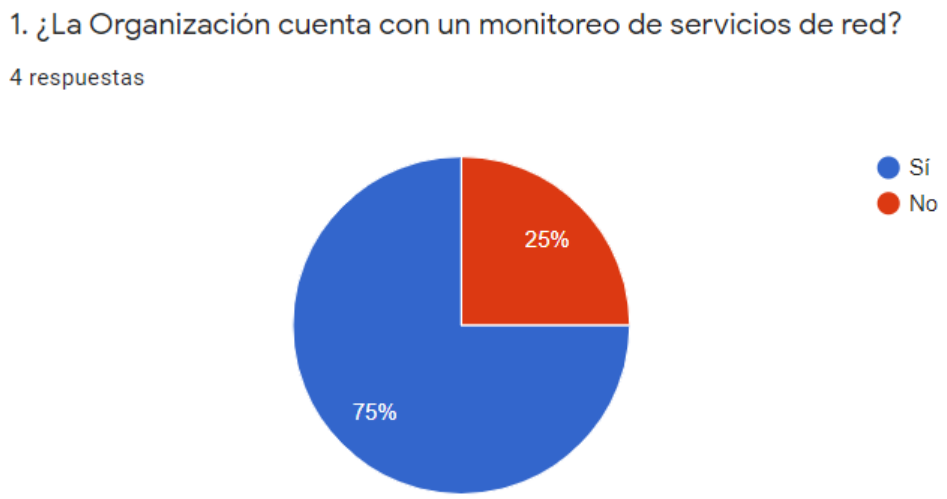
Con base en el gráfico anterior, se puede observar que el 56.9% afirma que se cuenta con una política de redes físicas e inalámbricas, pero la desconocen, un 30.6% indican que conoce sobre la política y un 12.5% señala que no se cuenta con una política que cubra este control.

De esta forma, la Financiera debe gestionar mejor la comunicación de políticas a los colaboradores debido a que actualmente no existe un documento que cubra el control.

- Seguridad de los servicios de red:

Los servicios de red incluyen la provisión de conexiones, los servicios de red privados, y las redes con valor agregado, así como soluciones de seguridad para la red tales como cortafuegos (firewalls) y sistemas de detección de intrusos.

Gráfica 42. Pregunta 1 TI - Seguridad de las comunicaciones



Fuente: Elaboración propia

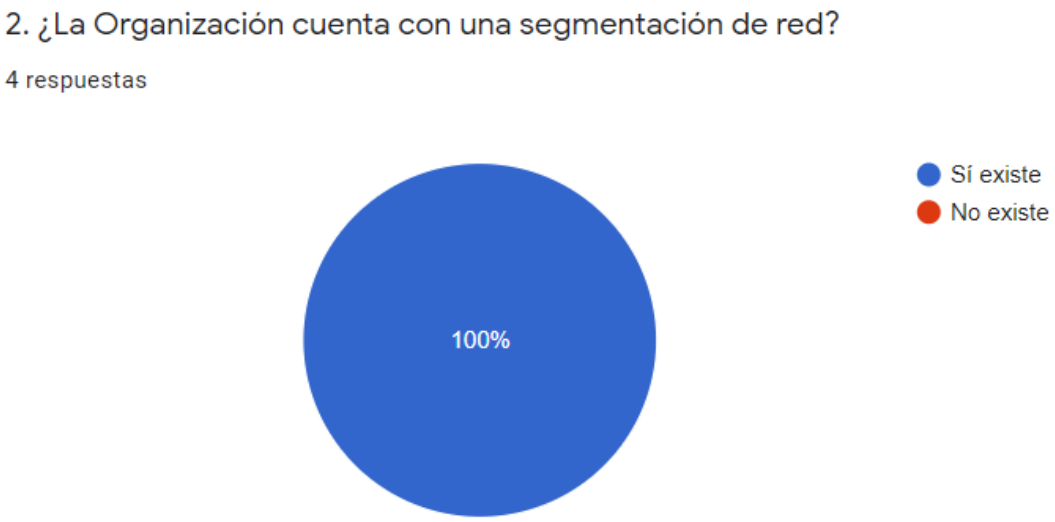
De acuerdo al gráfico anterior, el 75% de los compañeros del Comité de Informática afirman que sí existe un monitoreo de red dentro de la Financiera, sin embargo, sí se posee un monitoreo de la red, pero no se han realizado auditorías de *hacking* ético para evaluar el estado de las mismas, por eso el 25% indica que no.

- Segregación en las redes:

Las tecnologías de control de autenticación, cifrado y control de acceso de red del nivel usuario de redes inalámbricas modernas, basadas en normas, pueden ser suficientes para la conexión directa a la red interna de la organización.

Un método para controlar la seguridad de grandes redes es dividirlas en dominios de red separados. Los dominios pueden ser elegidos con base en los niveles de confianza (por ejemplo, dominio de acceso público, dominio del escritorio, dominio del servidor), en unidades de la organización (por ejemplo, recursos humanos, finanzas, *marketing*) o una combinación (por ejemplo, dominio del servidor conectado a varias unidades de la organización). La separación se puede hacer ya sea utilizando redes físicamente diferentes o utilizando diferentes redes lógicas (por ejemplo, redes virtuales privadas).

Gráfica 43. Pregunta 2 TI - Seguridad de las comunicaciones



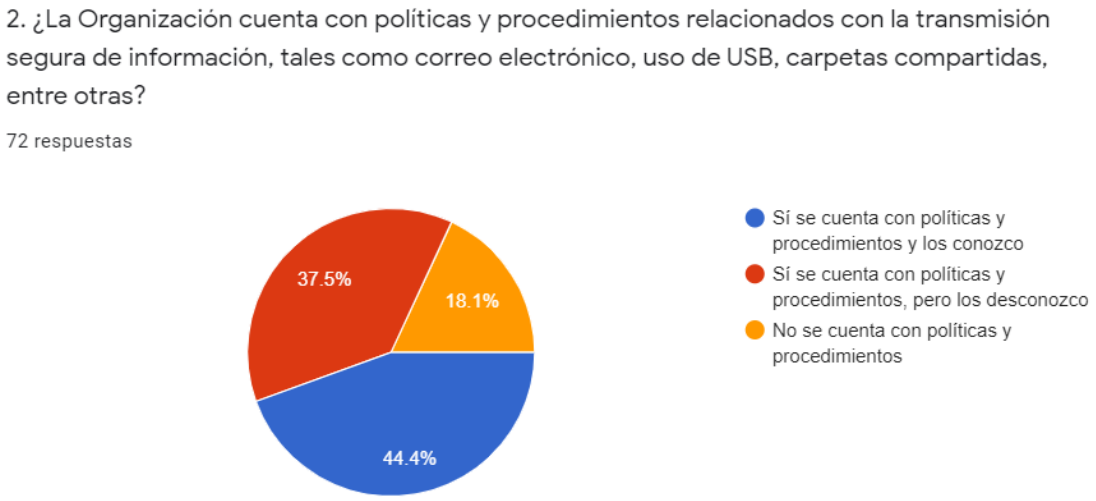
Fuente: Elaboración propia

El gráfico anterior se confirma que el Comité de Informática afirma que en la Financiera sí se cuenta con la segmentación adecuada de la red.

- Políticas y procedimientos de transferencia de información:

Se deben considerar las implicaciones de negocios, legales y de seguridad asociadas con el intercambio de datos electrónico, comercio electrónico y comunicaciones electrónicas y los requisitos de controles.

Gráfica 44. Pregunta 2 - Seguridad de las comunicaciones



Fuente: Elaboración propia

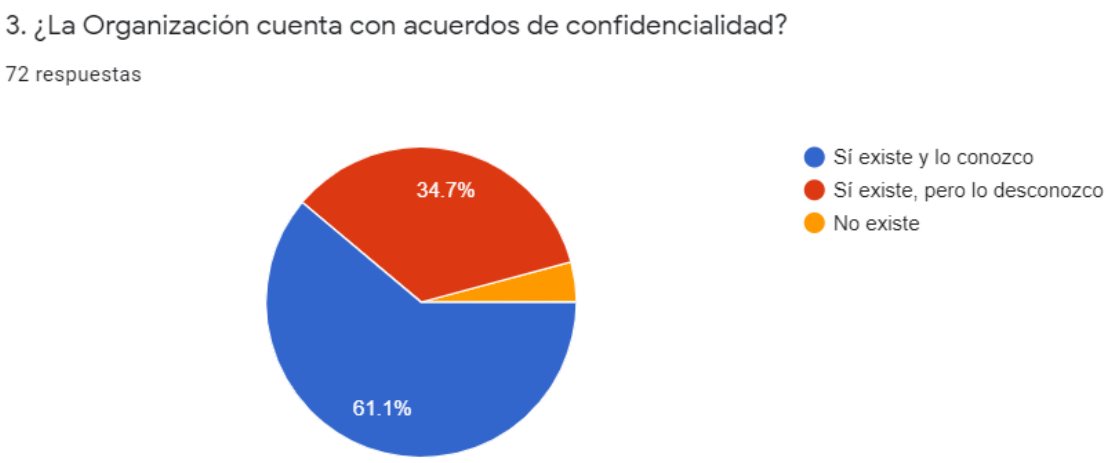
El gráfico anterior describe que, el 44.4% de los encuestados conocen y afirman que la Financiera cuenta con una política y procedimiento relacionados con la transmisión segura de información, un 37.5% indica que sí existe, pero desconoce de la política y un 18.1% opina que no existe política ni procedimiento. Por medio de indagación, se valida que la Financiera cuenta con parte de lo solicitado en el control, pero hace falta que la política cubra todos los aspectos relacionados al intercambio de la información.

- Acuerdos de confidencialidad o no divulgación:

Los acuerdos de confidencialidad y no divulgación protegen la información de la organización e informan a los signatarios de su responsabilidad para proteger, utilizar, y divulgar la información de forma responsable y autorizada.

Puede haber necesidad por parte de una organización de utilizar diversas formas de acuerdos de confidencialidad o no divulgación en diferentes circunstancias.

Gráfica 45. Pregunta 3 - Seguridad de las comunicaciones



Fuente: Elaboración propia

Los acuerdos de confidencialidad o de no divulgación deberían tratar el requisito de proteger la información confidencial usando términos que puedan hacerse cumplir legalmente.

Con base en la gráfica anterior, el 61.1% afirma la existencia y conocimiento de los acuerdos de confidencialidad dentro de la Financiera, el 34.7% indican que sí existen, pero desconocen y el 4.2% dice que no existe tales acuerdos. Por indagación con el Departamento de Auditoría, se confirma que si existen acuerdos de confidencialidad en los contratos con RH.

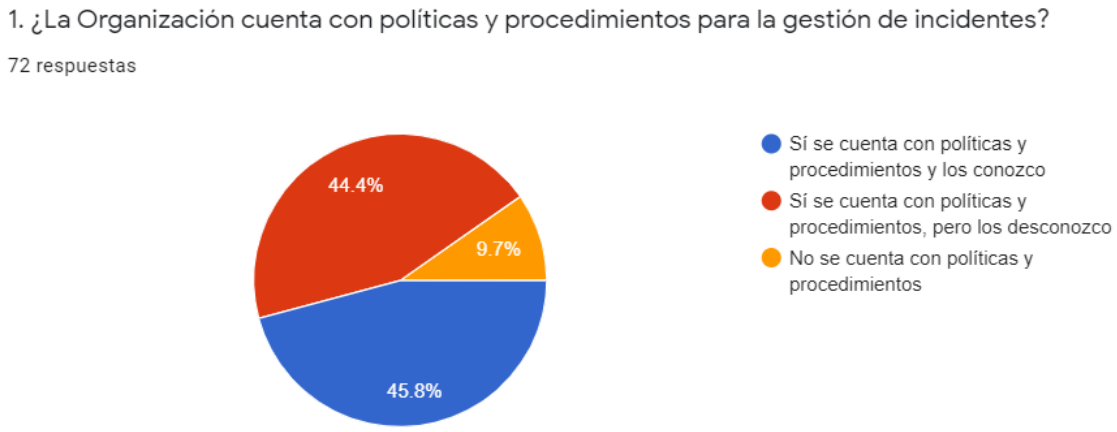
A.16 Gestión de incidentes de seguridad

Objetivo: garantizar un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades.

- Responsabilidades y procedimientos:

Los objetivos para la gestión de incidentes de seguridad de la información deberían acordarse con la dirección, y debería asegurarse que aquellos responsables de esta gestión entienden las prioridades de la organización para manejar incidentes de seguridad de la información.

Gráfica 46. Pregunta 1- Gestión de incidentes de seguridad



Fuente: Elaboración propia

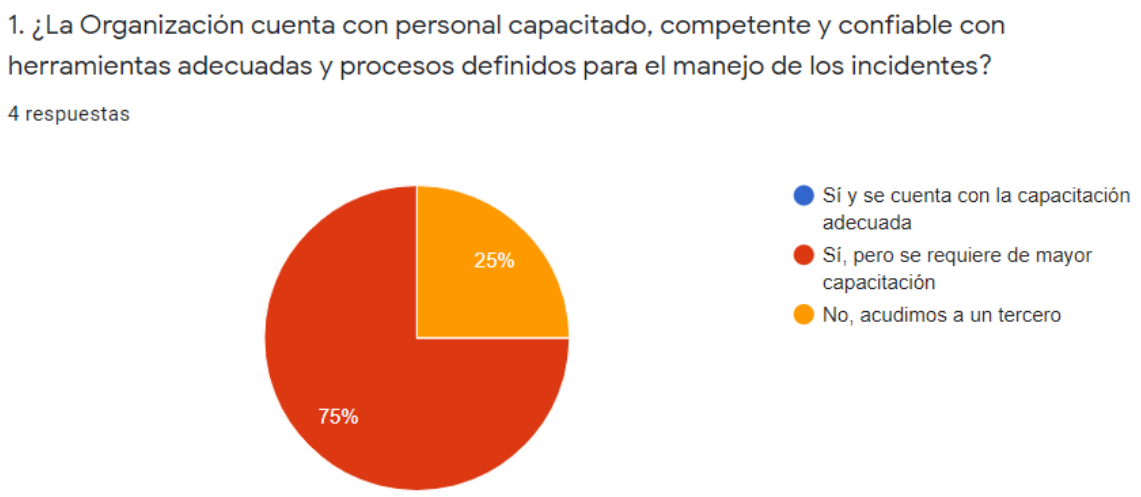
El 45.8% de los encuestados afirman la existencia e indican que conoce la política y procedimiento de la gestión de incidentes, un 44.4% dice desconocer la política o procedimiento, pero afirma que sí existe y un 9.7% cree que no se cuenta con política y procedimiento para la gestión de incidentes; sin embargo, los incidentes sí son atendidos, pero no hay política o documentación formal de cómo gestionar ante un incidente.

- Aprendiendo de los incidentes de seguridad de la información:

La evaluación de incidentes de seguridad de la información puede indicar la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de futuras ocurrencias, o para ser tomada en cuenta en el proceso de revisión de la política de seguridad.

Con el debido cuidado de los aspectos de confidencialidad, se pueden utilizar anécdotas de incidentes actuales de seguridad de la información en la capacitación de la sensibilización del usuario como ejemplos de lo que podría suceder, cómo responder a estos incidentes y cómo evitarlos en el futuro.

Gráfica 47. Pregunta 1 TI - Gestión de incidentes de seguridad



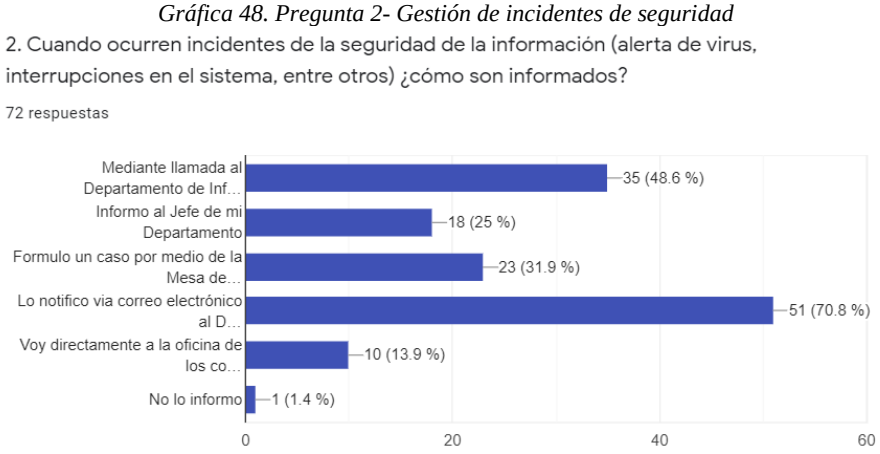
Fuente: Elaboración propia

El gráfico anterior muestra que el personal del Departamento de Informática requiere apoyo de alta gerencia para realizar mejoras en la capacitación relacionadas a temas de manejos de incidentes de la seguridad de la información.

- Reporte de eventos de seguridad de la información:

Todos los colaboradores y contratistas deben ser advertidos de su responsabilidad de reportar cualquier evento de seguridad de la información lo más rápidamente posible. Deberían también conocer el procedimiento para reportar los eventos de seguridad de la información y el punto de contacto al que los eventos deberían reportarse.

Gráfica 48. Pregunta 2- Gestión de incidentes de seguridad

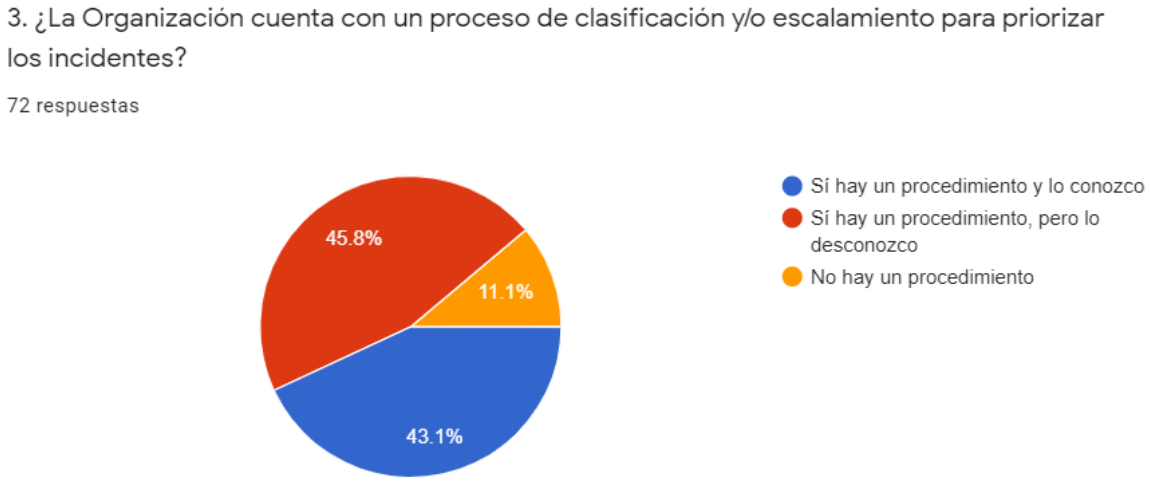


Fuente: Elaboración propia

El gráfico mostrado indica que no existe un proceso formal de reporte de incidentes de la seguridad de la información, cada colaborador maneja distintos canales para la comunicación al momento en que ocurre un incidente dentro de la Financiera.

Los desperfectos u otros comportamientos anómalos del sistema pueden ser un indicador de un ataque a la seguridad o de una violación real a la seguridad y, por lo tanto, debería siempre reportarse como un evento de seguridad de la información.

Gráfica 49. Pregunta 3 - Gestión de incidentes de seguridad



Fuente: Elaboración propia

Se valida con el Departamento de Auditoría la falta de un proceso de clasificación y/o escalamiento de incidentes, quien realizan este trabajo es Informática por lo que el 11.1% de los encuestados afirman de forma correcta, el resto siguen lineamientos no formales.

Causas de la problemática

Los problemas identificados dentro de la Financiera Desyfin obedecen a una serie de situaciones que interfieren con la atención de los mismo. A continuación, se describen nuevos problemas identificados que ocasionan que las áreas de estudio no estén alineadas con las mejores prácticas ni estándares para la gestión de la seguridad de la información, las mismas están ordenadas según su peso e importancia.

Administración del riesgo.

De parte de la Financiera actualmente no ha habido gestión para la identificación y análisis de los riesgos, motivo por el cual no hay una base para la determinación de cómo deben administrarse para que sean capaces de afrontarlos exitosamente.

Deficiencia en el manejo de respaldos.

Los respaldos realizados a los sistemas de la Financiera no llevan un correcto proceso de retención y frecuencia, por lo que ante una falla en los sistemas se pueden ver afectados ante pérdida de información no recuperable.

Exceso de confianza.

Se puede mencionar el alto grado de confianza que se tiene respecto a la infraestructura y recurso humano por parte de la Financiera, producto de que para los altos mandos el personal ya debe saber las responsabilidades, lo bueno y lo incorrecto. Esto ha hecho sentir que no se requiere contar con un sistema para la gestión de la seguridad de la información.

Poca información y capacitación.

No se realiza una oportuna divulgación para dar a conocer la situación de las diferentes áreas en cuanto a planes, políticas o mejores prácticas en cuestiones de seguridad de la información que sirvan de orientación a los colaboradores; tampoco se brindan capacitaciones relacionadas en cuanto a la seguridad de la información con el fin de que los colaboradores tengan un poco más de conocimiento y la importancia que posee la seguridad en la actualidad.

Cambios a programas.

La Financiera no cuenta con políticas o procedimientos para la gestión de cambios, en consecuencia, los cambios realizados a los sistemas carecen de documentación formal,

aprobación y un flujo de implementación que valide los cambios realizados,al mismo tiempo que dificulta la forma de verificar la información en procesos de auditoría debido que no se puede identificar la trazabilidad de los cambios realizados en los sistemas.

Roles y responsabilidades.

No existe una delegación formal de funciones o tareas en un colaborador en relación con la seguridad de la información, igualmente de la asignación de la autoridad necesaria con el propósito de que este funcionario pueda tomar las decisiones y emprender las acciones más oportunas para ejecutar su cometido de manera expedita y eficaz.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

Conclusiones

De acuerdo con el estudio y análisis realizado, se puede llegar a las siguientes conclusiones para lograr implementar una adecuada gestión en el uso de la seguridad de la información por parte de los colaboradores de la Financiera:

1. Se determinó que la Financiera Desyfin, carece de políticas formales que funcionan como herramientas principales para asegurar la implementación, operación, seguimiento, revisión y mejoramiento de la seguridad de la información.

2. Se han detectado una serie de riesgos que pueden afectar tanto las operaciones de Informática como las de la Financiera.

3. Se debe mejorar el proceso de capacitación con respecto al sistema de gestión de seguridad de la información de la Financiera para poder ser más efectivos en la consecución de un esquema de trabajo basado en buenas prácticas.

4. Al incluir la norma ISO27001:2013 la Financiera tendrá una ventaja competitiva en mediano plazo ya que no es requerido gastar tiempo y recursos en implementar un programa completo de seguridad de la información y el nivel de implantación de la norma aumentará drásticamente si se llega a implementar.

5. Lo más efectivo seguirá siendo la utilización de metodología comprobada que oriente en el diseño del programa de seguridad con base en las necesidades y objetivos; no sirve invertir en *hardware* de primera línea si el personal de la Financiera no está consciente de su papel protagónico en un sistema de gestión de la seguridad de la información.
6. Al momento en que se desee desarrollar con éxito un sistema de gestión de la seguridad de la información la clave es tener presente que las políticas y procedimientos de seguridad de la información son un grupo de documentos interrelacionados.

7. El correcto uso de las políticas de seguridad de la información desarrolladas durante la propuesta dará grandes beneficios que permitan incrementar la eficacia y eficiencia de los servicios que ofrece la Financiera, permitiéndoles garantizar altos niveles de seguridad para sus sistemas de gestión de la información.

Recomendaciones

Con base en los hallazgos identificados al momento de tratar de aplicar los diferentes requerimientos de la norma ISO 27001:2013, se recomienda a la Finaciera:

1. Dar uso, mantenimiento y actualización a la propuesta de solución desarrollada para el Departamento de Informática de la Financiera; debido que interrumpir o no aplicar el proceso de mejora continua en gestión de seguridad provocaría una desactualización de las políticas y con ello afectar las labores y desempeño de la unidad; se estima un período no mayor a 6 meses para implementar la propuesta indicada por parte del Departamento de Informática y una vez implementado, las políticas deben hacerlas conocer a todo el personal que labora en la Financiera.

2. Luego de haber realizado el primer análisis FODA, se aconseja realizar sucesivos análisis de forma periódica teniendo como referencia el primero, con el propósito de conocer si se están cumpliendo con los objetivos planteados en la formulación estratégica. Esto es aconsejable dado que las condiciones externas e internas son dinámicas y algunos factores cambian con el paso del tiempo, mientras que otros sufren modificaciones mínimas.

3. El mantenimiento, operación y control del sistema de gestión de seguridad de la información no puede ser tarea que realice una única persona ya que limitaría la capacidad de esta por conseguir todos los objetivos planteados, se debe realizar una revisión independiente contratada por parte de la Gerencia, esta revisión es necesaria para asegurar la continua idoneidad, eficiencia y efectividad del enfoque de la Financiera para manejar la seguridad de la información.

4. Realizar una adecuada segregación de las funciones y responsabilidades en cuanto al uso de los diferentes medios de para reducir las oportunidades de una modificación no autorizada o mal uso no intencional del uso los activos de la Financiera. Se recomienda que cada dueño de procesos asigne las diferentes responsabilidades y las mismas se den a conocer a la Gerencia General, en un tiempo de dos meses.

5. Apoyarse en criterios externos, firmas auditoras, SUGEF, ISACA, entre otras, otorga mayor credibilidad al trabajo realizado en la Financiera en relación con el sistema de gestión de seguridad de la información. Este apoyo es necesaria para asegurar la continua idoneidad, eficiencia y efectividad del enfoque de la Financiera para manejar la seguridad de la información. El apoyo debe incluir las oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el enfoque por seguridad, incluyendo políticas y objetivos de control.

6. Se debe mejorar el proceso de capacitación con respecto al sistema de gestión de seguridad de la información de la financiera para poder ser más efectivos en la obtención de un esquema de trabajo basado en buenas prácticas. De manera semestral impartir por parte de Informática o Auditoría charlas a los colaboradores con temas de seguridad de la información y por medio de correo electrónico, difundir mensajes de buenas prácticas de seguridad, aportando una mejor cultura dentro de la Financiera.

7. Implementar de forma inmediata un plan de respaldos de la información para salvaguardar la debida continuidad de la Financiera, documentar el proceso de respaldos, revisar y verificar las copias de respaldo una vez al mes por parte del encargado de las copias de seguridad de la Financiera o por parte de algún funcionario designado por el área de Informática.

8. Constituir un comité de riesgo para la evaluación, inspección y tratamiento de los riesgos identificados. De esta manera la Financiera puede implementar una gestión de la vulnerabilidad técnica de una manera efectiva, sistemática y respetable, tomando

mediciones para confirmar su efectividad. Estas consideraciones deben incluir a los sistemas de operación y cualquier otra aplicación en uso.

9. La Financiera debe considerar el uso de metodologías y estándares internacionales; con el fin de establecer proyectos relacionados con la gestión de seguridad de la información como parte de las tareas del Departamento de Informática, que a su vez conformen el Plan Estratégico y con ello delimitar las fechas de cada implementación.

10. Se recomienda contratar nuevos colaboradores que apoye en el ámbito de informática que brinde apoyo en tareas relacionadas a la seguridad de la informacion y así equilibrar las cargas laborales. Para ejecutar la propuesta se recomienda contar con un comité de seguridad y un oficial de seguridad de la información e invertir más recurso humano ya que actualmente con el recurso que se cuenta no es lo suficiente para realizar todas las tareas encomendadas. Se sugiere que la Gerencia General en conjunto con el Departamento de Informática, en un lapso de dos meses analicen que cantidad de personas se necesitan contratar para ejecutar todo el proceso de establecer un Sistema de Gestión de Tecnologías de Información.

CAPÍTULO VI: PROPUESTA

Diagnóstico de la compañía

En la normativa ISO27001:2013 se cita en el punto 4.1 “comprender la organización y su contexto ” lo siguiente: la organización debe determinar los asuntos externos e internos que son relevantes para su propósito y que afectan su capacidad para lograr el (los) resultado(s) deseado(s) de su sistema de gestión de seguridad de la información.

Una de la forma de abordar estos requisitos puede ser realizar un análisis FODA, es decir, un análisis de la situación real en que se encuentra una organización, analizando sus características internas (debilidades y fortalezas) y su situación externa (amenazas y oportunidades) cuyo objetivo primario consiste en obtener conclusiones sobre la forma en que la Financiera será capaz de afrontar los cambios y las turbulencias en el contexto, (oportunidades y amenazas) a partir de sus fortalezas y debilidades internas.

Al iniciar todos los factores que intervienen en la Financiera, estos pueden ser clasificados como positivos o negativos, en función de un análisis de factores críticos positivos con los que se cuentan en otras palabras las fortalezas, aspectos positivos que podemos aprovechar utilizando nuestras fortalezas para el caso de las oportunidades, las debilidades corresponden a factores críticos negativos que se deben eliminar o reducir y las amenazas son aspectos negativos externos que podrían obstaculizar el logro de nuestros objetivos.

Por medio de una reunión con el personal del Departamento de Informática y con el Departamento de Auditoría Interna se realiza el análisis FODA producto a los objetivos planteados en la propuesta del trabajo de graduación.

Análisis FODA

El análisis FODA debe enfocarse solamente hacia los factores claves para el éxito del negocio. Debe resaltar las fortalezas y las debilidades diferenciales internas al compararlo de manera objetiva y realista con la competencia, y con las oportunidades y amenazas claves del entorno.

Fortalezas.

- Personal estable dentro en la institución.
- Personal con conocimiento de la operativa y procesos de la entidad.
- Infraestructura tecnológica adecuada para soportar la operativa del negocio.
- Continuidad del negocio.
- La mayoría de los sistemas se adquieren de proveedores externos, y son sistemas maduros que presentan un alto grado de estabilidad.

Oportunidades.

- Buenas relaciones con proveedores y otras entidades.
- Teletrabajo.
- Conexiones remotas.
- Avances tecnológicos que nos van a permitir incluso la conexión desde nuestros móviles.
- Ampliar conocimiento en cada proyecto.
- Relaciones con diferentes consultores.
- Implementar nuevas tecnologías para reforzar seguridad y control de acceso a datos.

Debilidades.

- Pocos recursos.
- Concentración del conocimiento y habilidades.
- Falta de planes para retención del personal.
- Capacitaciones al personal.
- Falta programación de las áreas en proyectos.
- La capacitación técnica para administrar las tecnologías no se percibe como inversión necesaria.
- No se cuenta con contratos de soporte que garanticen tiempos de respuesta para atención de incidentes.
- Escasez de recurso humano técnico.

Amenazas.

- Costos altos.
- Baja contratación personal no técnico, pero que conozca el negocio.
- Dependencia de los proveedores.
- Se está retomando el antiguo modelo de implementar sistemas colaterales al sistema principal para satisfacer sus faltantes. Esto alimenta un ambiente heterogéneo en sistemas, el cual dificulta la fluidez de procesos porque la operativa depende de un número cada vez mayor de actores (proveedores, sistemas, equipos, tareas de sincronización, etc.)

Tendencias de tecnologías de información

Realizando un análisis de las tecnologías que utilizan las instituciones en la industria financiera local, se encuentran las siguientes características:

- En un principio se hablaba de *hardware*, pero ahora la mejor solución es una estrategia definida por *software* de virtualización, lo que se traduce en un aumento considerable de la eficiencia y reducción de recursos, permitiendo que los servicios de TI virtualizados y la administración de operaciones automatizadas, ofrecen nuevos niveles de utilización de recursos y productividad del personal.
- La computación en la nube sigue siendo una de las tendencias más importantes en tecnologías de información.
- Centros de datos definidos por *software*, el cual consiste en un centro de datos donde la infraestructura está virtualizada y es entregada como un servicio. El control de estos centros de datos es totalmente automatizado mediante *software*, en contraste con los centros de datos tradicionales, donde la infraestructura se define por *hardware*.
- Computación en todas partes, ya que, si la tecnología de los dispositivos móviles inteligentes continúa progresando, deberá darse un especial énfasis en atender las necesidades de los usuarios en diversos contextos y entornos, en lugar de centrarse en los dispositivos que utilizan los usuarios.

- Seguridad informática basada en riesgos, ya que las organizaciones reconocerán que no es posible brindar un entorno seguro al 100%, por lo tanto, al aceptar esto, aplicarán herramientas más sofisticadas de evaluación y prevención de riesgos.

Matriz de riesgo

Se trata de una herramienta ampliamente utilizada en diversas actividades que deben ponderar y gestionar riesgos. Desde su concepción metodológica las matrices se componen de dos vectores, uno de impacto y otro de probabilidad, cuya combinación define el riesgo de un factor en particular; para Wolinsky (2003), "la matriz de riesgo es un elemento que posibilita cuantificar los riesgos disminuyendo el nivel de subjetividad al momento de su evaluación, siempre que la parametrización y asignación de valores a los indicadores esté debidamente fundamentada" (p.110).

Se utiliza la matriz de riesgos como herramienta de análisis y determinación del nivel de los mismos, en términos de alto, medio o bajo, para gestionar las acciones a tomar y en consecuencia, darles respuesta e incluso diseñar controles internos que permitan cubrirlos, minimizarlos o eliminarlos.

Los riesgos se pueden clasificar, según Lara (2012), como financieros, operativos y de cumplimiento. Adicionalmente, Ernst & Young incluye los riesgos estratégicos. Los riesgos financieros surgen por la volatilidad en los mercados y en la economía real; los riesgos operativos surgen de los procesos, de los sistemas, de la gente y de la cadena de valor general de un negocio. Los riesgos de cumplimiento se originan por situaciones de políticas, leyes, reglamentación del marco legal o del gobierno corporativo; los estratégicos se originan por la relación con los clientes, competidores e inversionistas.

Toda entidad a efectos de gestionar o administrar los riesgos debe identificar los factores que los generan y crear su propia jerarquía de riesgos, con esto se buscar establecer las prioridades de atención sobre los cuales se implementarán los mecanismos de cobertura sustentados en adecuados controles internos que contribuyan a la mitigación, transferencia o eliminación de los niveles de riesgos existentes.

Después de evaluar las diferentes áreas con las entrevistas y encuesta realizada, se identificaron 25 riesgos a las que se exponen las áreas de estudio, algún daño o pérdida de

la información, comprometiendo la disponibilidad, integridad y confidencialidad. Seguidamente, se presenta una matriz de riesgos identificados, en donde se documentan los riesgos a los que se exponen las áreas al no contar con los controles requeridos según la

Imagen 4. Amenazas y vulnerabilidades

Amenazas y Vulnerabilidades

	Amenaza	Describición
Hardware	A1	Daños en los equipos Informáticos
	A2	Adquirir y mantener infraesctructura tecnológica
	A3	Perdida por robo/ hurto de información
Software	A4	Daños en software
	A5	Infección de Virus
	A6	Bitácoras de los eventos
	A7	Perdida de información
	A8	Uso de software en forma no autorizada
	A9	Uso de software por usuarios no autorizados
	A10	Software desarrollado por terceros
	A11	Entregables del software no cumplen expectativas
Comunicaciones	A12	No complimiento de las políticas del manejo de la información
	A13	Interrupción de acceso a la red
	A14	Fallas en el acceso a recursos compartidos dentro de la Financiera
	A15	Intromisión por parte de personas y/o elementos inoportunos a la red de datos interna de la Financiera
	A16	Información que se envía por medios electrónicos.
	A17	Descontrol en el recibo y envío de información
Seguridad	A18	Derechos de acceso del usuario
	A19	No implementar copias de seguridad en forma periódica.
	A20	Exceso de confianza
	A21	Manejo de riesgos informáticos
	A22	Manejo de los cambios a sistemas
Colaboradores	A23	Educar y capacitar a los colaborades
	A24	Contratos de Confidencialidad
	A25	Inexperiencia del personal informático

	Vulnerabilidad	Describción
Hardware	V1	Uso continuo e inadecuado de los equipos Informáticos
	V2	No se prevé la necesidad de adquirir nuevos equipos
	V3	Las copias de seguridad no se disponen en lugar fuera de la Financiera
Software	V4	Daños en los equipos de cómputo
	V5	Falta de protección contra virus y código malicioso
	V6	Definición o ausencia de un registro de evento que contemple todas las necesidades de trazabilidad
	V7	No establecimiento de políticas de administración de seguridad de la información
	V8	Uso impropio/no controlado
	V9	Control de acceso inadecuado
	V10	Los recursos de desarrollo del proyecto en la Financiera eran insuficientes o inadecuados
	V11	Levantamiento de requerimiento inadecuado o cambios producto de nuevas necesidades no actualizadas.
Comunicaciones	V12	Carencia de políticas
	V13	No diagnosticar en tiempo oportuno la causa de no tener acceso a la red
	V14	No diagnosticar en tiempo oportuno la causa de no tener disponibles los recuros funcionado de manera óptima
	V15	No contar con los recuros para el manejo óptimo de la seguridad de los sistemas.
	V16	Falta de herramientas de inspección de contenido para correo electrónico
	V17	La carencia del procedimiento que norme el envío y recibido de información
Seguridad	V18	Acceso indebidos por parte de los usuarios ante la presencia de perfiles inadecuados
	V19	Se corre el riesgo de perder la información de los periodos de nomina almacenados en el programa.
	V20	Falta de concientización de los colaboradores
	V21	Ausencia de adminitración de los riesgos informáticos
	V22	Falta de participación desde el principio, perdida de interes, cambio de dirección o prioridades
Colaboradores	V23	Poca capacitación y no aplicabilidad de procesos de inducción y reinducción a los funcionarios en materia de seguridad informática
	V24	Salvaguardar los intereses intitucionales con el personal (interno y externo) sobre la confidencialidad de la información que costodian
	V25	Personal no cuenta con las competencia ni las herramientas para salvaguardar eficazmente los recursos de la Financiera

norma ISO 27001:2013. Esta matriz es una herramienta sencilla que permite efectuar un diagnóstico objetivo de la situación global del riesgo de las diferentes áreas de estudio desde dos perspectivas: la probabilidad de que suceda y el impacto sobre las áreas u Financiera si llegase a suceder.

Fuente: Elaboración propia

Se ejecuta la identificación de las amenazas y vulnerabilidades relacionadas con los activos y funciones que soportan los procesos de la Financiera tomando en cuenta los siguientes: *hardware, software,* comunicaciones, seguridad y colaboradores.

Una vez identificadas las amenazas y vulnerabilidades se identifican los riesgos potenciales que podrían causar impacto a nivel de confidencialidad, exactitud y disponibilidad sobre la información dentro de la Financiera.

Imagen 5 Riesgos pontenciales

Riesgos Potenciales						
	Amenaza	Vulnerabilidad	Riesgo	Descipción	Causa	Efecto
Hardware	A1	V1	R1	Falta de mantenimiento preventivo y/o correctivos de los equipos existentes.	Carencia de mantenimiento en los equipos existentes.	Baja en la calidad de prestación del servicio.
	A2	V2	R2	Dificultad en la contratación y mantenimiento de la infraestructura tecnológica.	No se contemplan equipos nuevos y necesarios para la seguridad de las operaciones.	No se adquieran todas los elementos que conforman la solución.
	A3	V3	R3	Si el equipo servidor tiene un fallo catastrófico es posible la perdida total de información.	No establecimiento de políticas de administración de seguridad de la información.	Atraso en las labores de los colaboradores o no ejecución de tareas en tiempos oportunos.
Software	A4	V4	R4	Fallas de progamación que se presenta en el software.	Mal manejo en el control de cambios a programas.	Pérdida de continuidad del servicio.
	A5	V5	R5	Infección y propagación de virus a los equipos.	Falta de monitoreo de los equipos conectados a la red.	Caidas y degradación del sistema.
	A6	V6	R6	Ausencia de un registro apropiodo de los eventos del sistema que permita la trazabilidad de de las actividades que se desarrollan en el mismo.	Ausencia de un registro de evento que contemple todas las necesidades de trazabilidad.	Dificultad para analizar incidente ante de ausencia de bitácoras eficientes
	A7	V7	R7	Si el equipo servidor tiene un fallo catastrófico es posible que se perdida información de orden institucional.	No establecimiento de políticas de respaldos que se adecuden a las necesidades de la Financiera.	Atraso en las labores de los colaboradores o no ejecución de tareas en tiempos oportunos.
	A8	V8	R8	Accesos indebidos de usuarios a programas o funciones dentro del sistema.	Falta de revisión de los usuarios con mayor privilegión dentro de los sistemas de la Financiera.	Robo, eliminación o alteración de la información almacenada en los sistemas.
	A9	V9	R9	Acceso no removidos oportunamente.	La no eliminación del acceso ante un despido o renuncia del colaborador.	Robo, eliminación o alteración de la información.
	A10	V10	R10	Software desarrollado por terceros no tiene contratos adecuados para su cumplimiento	Los recursos de desarrollo del Proyecto en la Financiera eran insuficientes o inadecuados	Incremento en los costos del proyectos y la necesidad de mayores controles técnicos y legales.
	A11	V11	R11	Software no cumplen expectativas de la Finanicera	Levantamiento de requerimiento inadecuado o cambios producto de nuevas necesidades no actualizadas.	No se cuenta con avances reales del sistema, con el costo que implica su retraso.
Comunicaciones	A12	V12	R12	Falta políticas referentes al cumplimiento de directrices y sobre la responsabilidad de la información contenida en los sistemas.	Demoras en la generación de la información.	Incumplimiento en cuanto a las directrices relacionadas con Gobierno de TI
	A13	V13	R13	Dificultad para acceder a los servicios de internet e intranet	Falta de herramientas para diagnosticar en tiempo oportuno la causa de no tener acceso a Internet	Atraso en las labores de los colaboradores o no ejecución de tareas en tiempos oportunos.
	A14	V14	R14	No tener disponibilidad de recursos en momentos determinados	Falta de herramienta para diagnosticar en tiempo oportuno la causa de no tener disponibles los recuros funcionado de manera óptima	Atraso en las labores de los colaboradores o no ejecución de tareas en tiempos oportunos.
	A15	V15	R15	Pérdida de información financiera, por intromisión de entes externos y/o inescrupulosos, los cuales pueden generar daño y pérdida de información institucional	No tener establecida e implementada políticas de seguridad a los equipos informáticos, sistemas de información institucional.	Robo, eliminación o alteración de la información almacenada en los sistemas.
	A16	V16	R16	Uso indebido del correo electrónico.	Falta de controles adecuados para la información que envía los usuarios por correo electrónico	Fuga o suplantación de información por medio de correo electrónico.
	A17	V17	R17	Inadecuado manejo de envío y recibido de información tanto dentro como fuera de la Financiera	Falta de definición, revisión y control interno	Dificultad en la toma de decisiones y reclamaciones legales.
Seguridad	A18	V18	R18	Posible acceso indebido de terceros en los perfiles de los derechos de acceso del usuario	Falta de validación de perfiles y permisos correspondientes a los asignados a cada colaborador	Acceso indebidos por parte de los usuarios ante la presencia de perfiles inadecuados
	A19	V19	R19	Falta de coordinación para producir copias de seguridad de los archivos existentes en forma periódica	Perdida de archivos en el sistema por mal manejo y operatividad del mismo.	Expone a la Financiera a problemas administrativos y legales.
	A20	V20	R20	Falta de un sistema para la gestión de la seguridad de la información	Alto grado de confianza que se tiene respecto a la infraestructura y recurso humano por parte de la Financiera	Manejo erroneo de la seguridad de la informacón.
	A21	V21	R21	No se realiza una gestión ni análisis de los riesgos	Falta de una identificación y análisis de los riesgos.	Exposición ante riesgos sin un debido tratamiento.
	A22	V22	R22	Los cambios no se realice de forma apropiada para evitar problemas posteriores.	Ausencia de políticas y procedimientos necesarios para el control de cambios	Se realizan prácticas inadecuadas, por lo que se pueden presentar diversos tipos de problemas del sistema estando en producción.
Colaboradores	A23	V23	R23	Ausencia de capacitación para los colaboradores	Poca capacitación y no aplicabilidad de procesos de inducción y reinducción a los colaboradores	Problemas de implantación, apropiación y aceptación de un buen modelo de seguridad informática.
	A24	V24	R24	Falta de conocimiento sobre los contratos de confidencialidad.	Salvaguardas los intereses intitucionales con el personal (interno y externo) sobre la confidencialidad de la información que costodian.	Fugas de información, uso indebido de los sistemas, entre otros
	A25	V25	R25	Falta de herramientas y capacitación del personal informático para contar con las capacidades necesarias.	Ausencia de capacitaciones para el personal informático y adquisición de nuevos herramientas.	Desmotivación para el desarrollo de la labor, gestión ineficiente.

Fuente: Elaboración propia

Se realiza la descripción del riesgo acorde a las amenazas y vulnerabilidades encontradas, asimismo la causa y el posible efecto que podría tener el riesgo si llega a materializarse dentro de la Financiera.

Basado en los riesgos anteriores, se implementa el análisis de evaluación de los riesgos basado en la probabilidad e impacto.

Imagen 6 Probabilidad

Probabilidad		
5	Frecuente	Una vez por semana
4	Probable	Una vez por mes
3	Ocasional	Una vez por semestre
2	Posible	Una vez por año
1	Improbable	Cada cinco años

Fuente: Elaboración propia

Se utiliza la escala de uno (1) a cinco (5) para medir la probabilidad que el riesgo llegue a ocurrir, para ello se realiza la entrevista con el Departamento de Auditoría de la Financiera y se plantean los resultados de la evaluación obtenida.

Imagen 7 Impacto

Impacto		
5	Catastrófico	De suceder las consecuencias sería catastróficas.
4	Mayor	De suceder tendría altas consecuencias sobre la Financiera.
3	Moderado	De presentarse el hecho tendría medianas consecuencias sobre la Finanicera o área.
2	Menor	De suceder habría un bajo impacto sobre la Financiera o área.
1	Insignificante	Si llegara a presentarse su impacto sería mínimo.

Fuente: Elaboración propia

Se emplea la escala de uno (1) a cinco (5) para medir el impacto sobre la ocurrencia del riesgo, para ello se realiza la entrevista con Auditoría de la Financiera y se plantea los resultados de la evaluación obtenida.

Imagen 8 Evaluación de riesgo

Identificación		Análisis		Evaluación
Nº	Descipción	Probabilidad	Impacto	
R1	Falta de mantenimiento preventivo y/o correctivos de los equipos existentes.	2	1	2
R2	Dificultad en la contratación y mantenimiento de la infraestructura tecnológica.	2	3	6
R3	Si el equipo servidor tiene un fallo catastrófico es posible la perdida total de información.	2	5	10
R4	Fallas de progamación que se presenta en el software.	3	3	9
R5	Infección y propagación de virus a los equipos.	3	3	9
R6	Ausencia de un registro apropiodo de los eventos del sistema que permita la trazabilidad de de las actividades que se desarrollan en el mismo.	3	3	9
R7	Si el equipo servidor tiene un fallo catastrófico es posible que se perdida información de orden institucional.	2	5	10
R8	Accesos indebidos de usuarios a programas o funciones dentro del sistema.	2	4	8
R9	Acceso no removidos oportunamente.	2	3	6
R10	Software desarrollado por terceros no tiene contratos adecuados para su cumplimiento	2	3	6
R11	Software no cumplen expectativas de la Finanicera	2	4	8
R12	Falta políticas referentes al cumplimiento de directrices y sobre la responsabilidad de la información contenida en los sistemas.	4	3	12
R13	Dificultad para acceder a los servicios de internet e intranet	3	4	12
R14	No tener disponibilidad de recursos en momentos determinados	3	2	6
R15	Pérdida de información financiera, por intromisión de entes externos y/o inescrupulosos, los cuales pueden generar daño y pérdida de información institucional	2	5	10
R16	Uso indebido del correo electrónico.	2	2	4
R17	Inadecuado manejo de envío y recibido de información tanto dentro como fuera de la Financiera	2	3	6
R18	Posible acceso indebido de terceros en los perfiles de los derechos de acceso del usuario	3	5	15
R19	Falta de coordinación para producir copias de seguridad de los archivos existentes en forma periódica	3	4	12
R20	Falta de un sistema para la gestión de la seguridad de la información	3	4	12
R21	No se realiza una gestión ni análisis de los riesgos	4	3	12
R22	Los cambios no se realice de forma propiada para evitar problemas posteriores.	3	5	15
R23	Ausencia de capacitación para los colaboradores	3	2	6
R24	Falta de conocimiento sobre los contratos de confidencialidad.	3	4	12
R25	Falta de herramientas y capacitación del personal informático para contar con las capacidades necesarias.	4	4	16

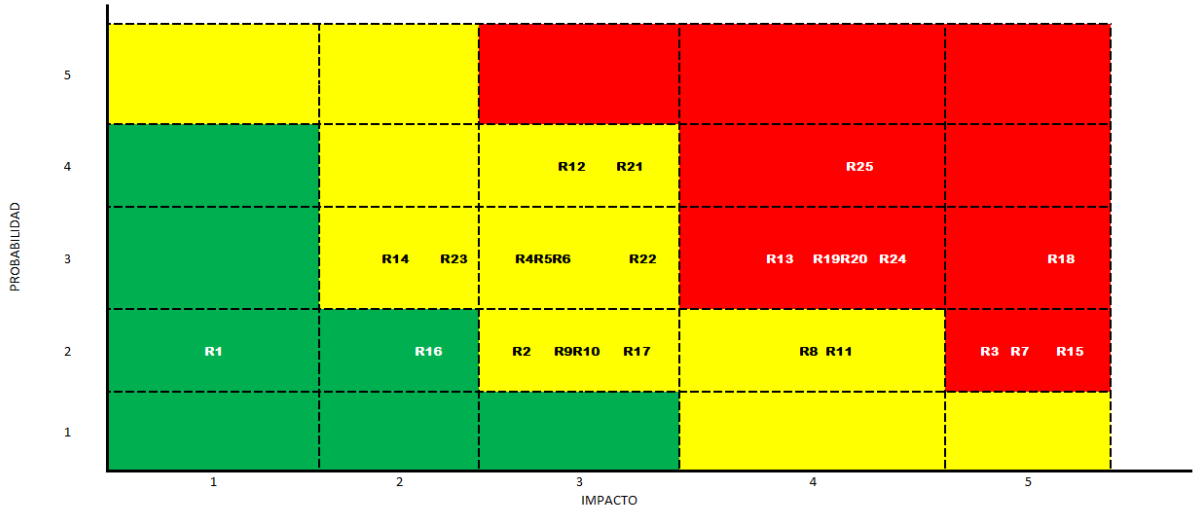
Fuente: Elaboración propia

A partir de las amenazas y vulnerabilidades identificadas, se efectúa el análisis de la probabilidad e impacto para los riesgos planteados y los mismos fueron sometidos a la evaluación bajo la siguiente fórmula:

$$Evaluación\ riesgo = Probabilidad * Impacto$$

El mapa de calor permite representar de forma gráfica un plano conformado por zonas donde se ubican los riesgos de acuerdo con su probabilidad y su impacto. Cada zona dentro del mapa de calor corresponde a un tipo de riesgo, el cual indica las acciones que se deben realizar para el tratamiento del riesgo.

Imagen 9. Matriz de riesgo



Fuente: Elaboración propia

La matriz de riesgos refleja que las áreas en estudio están expuestas a riesgos cuya probabilidad de que ocurran se encuentran en los puntos medios (baja, media y alta); sin embargo, el impacto para la Financiera es muy alto debido a que la información manejada por parte de ellos es sensible y vital para la continuidad del negocio.

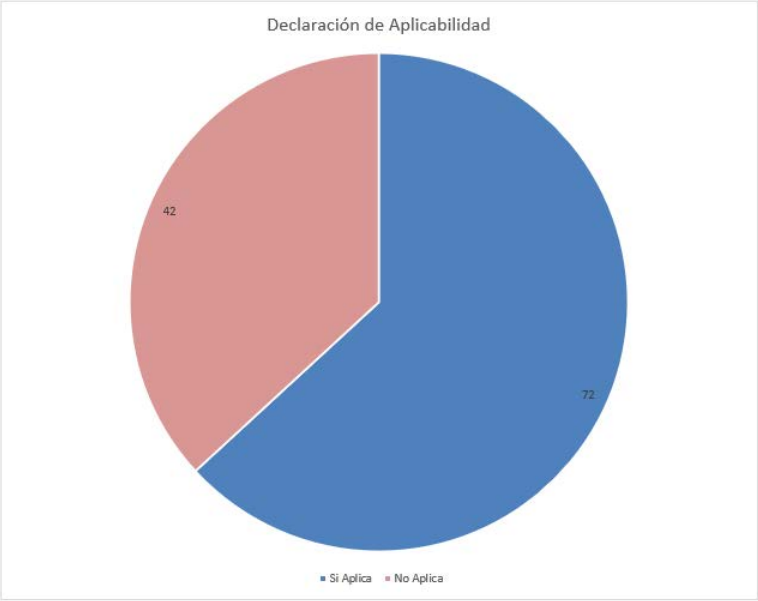
Actualmente la Financiera no cuenta con un apetito de riesgo por lo que no es posible realizar un cálculo del riesgo residual por ende no se logra identificar la cantidad de riesgo que la Financiera está dispuesta en asumir para el logro de sus objetivos.

Declaración de aplicabilidad

La declaración de aplicabilidad, como lo exige la ISO27001:2013 en la cláusula 6.1.3 (d), contiene los controles necesarios y una justificación para incluirlos, ya sea que estos hayan sido implementados o no, y la justificación para la exclusión de controles del Anexo A.

Una declaración de aplicabilidad es una parte fundamental de un SGSI, lo anterior debido a que es en esta sección donde se establecerán que controles y políticas serán implementados por Financiera Desyfin, los cuales se detallan.

Gráfica 50. Declaración de Aplicabilidad

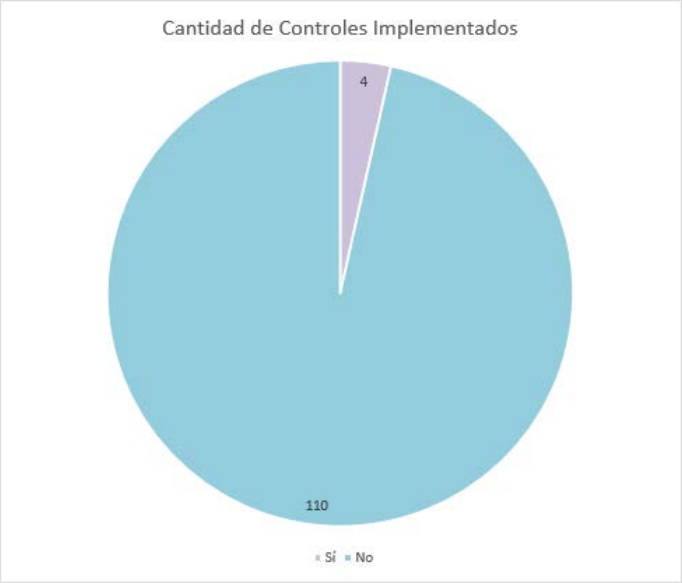


Fuente: Elaboración propia.

En el gráfico anterior muestra cómo será la aplicabilidad de la norma ISO 27001:2013 en el desarrollo del manual de políticas y procedimientos de la seguridad de la información para la Financiera Desyfin. En el mismo se observa que del total de controles 114, únicamente 42 de ellos no serán aplicados en el proyecto, correspondiente a 72 controles que sí están dentro del alcance definido para la presente investigación.

Al mismo tiempo se realiza una validación de los controles que se encuentran actualmente implementados por parte de la Financiera y este fue el resultado obtenido:

Gráfica 51. Controles Implementados



Fuente: Elaboración propia.

Como se puede observar en la gráfico anterior, 110 controles no se encuentran implementados ya que carecen de políticas, procedimientos y controles que permitan la total aplicabilidad de un sistema de gestión de seguridad de la información, también un porcentaje del mismo actualmente se encuentra en un estado parcial de aplicabilidad, solo 4 de los controles han sido implementados en su totalidad dado que cuentan con las políticas y los procesos documentados y se lleva a cabo conforme lo indica la norma.

La propuesta para un adecuado manejo de la seguridad de la información es un conjunto de mecanismos que determinan lo que se debe establecer para salvaguardar los sistemas y la información que se encuentran contenida en cada uno de ellos. El presente conjunto de políticas están fundamentadas con el estándar internacional ISO27001:2013 el cual de forma global contiene las estrategias para proteger y mantener la disponibilidad de los recursos.

Creación de políticas

Las organizaciones han desarrollado documentos, directrices y recomendaciones que guían el uso adecuado de las nuevas tecnologías para maximizar los beneficios y evitar su uso inapropiado, lo que puede conducir a graves problemas en los bienes y servicios de las empresas en todo el mundo.

En este sentido, las políticas de seguridad informática resultan ser una herramienta organizativa para crear conciencia sobre la importancia y la sensibilidad de la información y los servicios críticos para los miembros de una organización. Esto permite a la empresa desarrollarse y permanecer en su área de negocios. De acuerdo con lo anterior, proponer o identificar una política de seguridad requiere un alto nivel de compromiso organizacional, agudeza técnica para identificar errores, debilidades y persistencia para renovar y actualizar esta política basada en el entorno dinámico que rodea a las organizaciones modernas.

El propósito de las políticas de seguridad informática es proporcionar a todos los colaboradores de la compañía y a los usuarios que tienen acceso a sus recursos de tecnología e información los requisitos y pautas para las medidas de protección requeridas mientras que los procedimientos son un método de ejecución o pasos a seguir, en forma secuenciada y sistemática, en la obtención de un fin. Además, estas políticas son útiles al examinar los sistemas de información de una empresa durante un proceso de auditoría.

Todas las buenas políticas de seguridad informática tienen en común estas características:

- Concretas: tienen que poderse implementar a través de procedimientos, reglas y pautas claras.
- Claras: tienen que definir de forma clara las responsabilidades y obligaciones de los distintos tipos de usuarios: personal, administradores y dirección.
- Obligatorias: su cumplimiento tiene que hacerse respetar, mediante herramientas de seguridad o sanciones.

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
	1.0		Elaboración del primer documento

1. OBJETIVO

Formalizar el marco normativo y de gobierno corporativo que permita controlar el entorno lógico y físico de la información teniendo en cuenta los criterios de confidencialidad, disponibilidad, autenticidad e integridad de la información almacenada, transmitida o intercambiada en la Financiera Desyfin S.A, entre áreas internas o con entidades externas.

2. ALCANCE

Las políticas definidas en el presente documento aplican a todos los colaboradores, personal temporal y practicantes de Financiera Desyfin S.A, Costa Rica, así como otras personas relacionadas con terceras partes que utilicen recursos tecnológicos e informáticos que tengan que ver con la Financiera.

3. DESCRIPCIÓN

3.1 Estructura del documento

- Organización de la Seguridad de la Información (3.2)
  - Roles y responsabilidades (3.2.1)
  - Segregación de funciones (3.2.2)
  - Contacto con autoridades (3.2.3)
  - Contacto con grupos de interés (3.2.4)
- Gestión de activos (3.3)
  - Responsabilidad de los activos (3.3.1)
  - Clasificación de información (3.3.2)
  - Manejo de los medios (3.3.3)
- Control de acceso (3.4)
  - Administración de cuentas de usuarios y contraseñas (3.4.1)
  - Acceso a internet- Uso de correo electrónico (3.4.2)
  - Acceso código fuente de programas (3.4.3)
- Acceso físico (3.5)
- Seguridad de las operaciones (3.6)
  - Procedimientos y responsabilidades operacionales (3.6.1)
  - Protección contra código malicioso (3.6.2)
  - Respaldos (3.6.3)
- Seguridad de las comunicaciones (3.7)
  - Seguridad de los servicios de red (3.7.1)
  - Acuerdos de transferencia de información (3.7.2)
- Gestión de incidentes de seguridad de la información. (3.8)
  - Responsabilidades y procedimientos (3.8.1)
  - Reporte de eventos de seguridad de la información (3.8.2)
  - Evaluación sobre los eventos de seguridad de la información (3.8.3)

3.2 Organización de la seguridad de la información

3.2.1 Roles y responsabilidades

Se deberán definir, asignar y mantener los roles y responsabilidades de la seguridad de la información al personal de la Financiera que estará a cargo de la ejecución del marco de seguridad de la información

3.2.2 Segregación de funciones

Se deberán implementar controles y lineamientos que permitan una división de roles y responsabilidad es que reduzca la posibilidad de que un solo individuo afecte un proceso crítico dentro de la Financiera.

3.2.3 Contacto con autoridades

Se deberán mantener y diseñar planes de respuesta a las amenazas del entorno, los cuales deberán establecer y mantener actualizados contactos con las principales organizaciones: bomberos, policía, entes reguladores y cualquier otro contacto importante para la Financiera.

3.2.4 Contacto con grupos de interés

Se deberán establecer lineamientos que permitan a los responsables de seguridad de la información a participar en foros especializados en seguridad con el fin de incrementar el conocimiento sobre las mejores prácticas y mantenerse al día con la información relevante sobre seguridad de la información, así como recibir advertencias oportunas de alertas, avisos y parches sobre ataques o vulnerabilidades.

3.3 Gestión de activos

3.3.1 Responsabilidad por los activos

Se deberán establecer y comunicar las directrices mínimas necesarias para garantizar el uso aceptable de los activos por parte de los colaboradores de la Financiera, así como los controles y medidas que permitan garantizar la seguridad y continuidad del servicio que apoyan esos activos.

3.3.2 Clasificación de la información

Se deberán implementar y establecer los lineamientos y controles mínimos que permitan a la Financiera clasificar y etiquetar la información y sus sistemas, así como asegurar que la información y los activos que los resguardan dispone de un nivel de protección apropiado de acuerdo a la clasificación otorgada.

La clasificación deberá considerar al menos los niveles de clasificación siguientes:

Información pública

Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea colaborador de la Financiera o no; no obstante, se deberá implementar controles que eviten la autorización no autorizada de la misma.

Esta información en caso de ser conocida o utilizada por personas, sin la debida autorización, no impactaría de manera significativa a los clientes, sistemas o procesos de la Financiera; no obstante, la modificación de la misma sí representa un riesgo para la Financiera.

Información interna

Información que puede ser conocida y utilizada únicamente por los colaboradores de la Financiera y es necesaria para realizar su trabajo, y cuya divulgación, uso o modificación no autorizada podría significar un riesgo para la Financiera.

Información confidencial

Información cuyo acceso, uso o modificación estará restringido a un grupo definido de personas. Los accesos a terceros, uso o modificaciones no autorizadas representan un riesgo de alto impacto a la Financiera.

Toda copia de información clasificada como confidencial deberá ser destruida luego de que no requiera ser utilizada.

3.3.3 Manejo de los medios

Se deberán establecer controles que prevengan la divulgación, modificación, extracción o destrucción no autorizada de la información almacenada en medios de almacenamiento, tales como, pero no limitado a: cintas de respaldo y memorias externas – USB, discos duros (Externo e Interno), CDs, DVDs.

Para ello se deberán considerar al menos lo siguiente:

a. Gestión de medios removibles

Se deberán establecer lineamientos con el fin de restringir el uso medios de almacenamiento removibles unicamente al personal autorizado de la Financiera, el cual por sus funciones desempeñadas deba hacer uso de esos medios de almacenamiento.

Adicionalmente, se deberán establecer controles a los medios removibles con el fin de prevenir accesos no autorizados a la información que se almacena. Esos controles deberán

estar de acuerdo con el esquema de clasificación establecido en la Financiera; adicionalmente, el medio deberá ser clasificado según el nivel más alto de información que contengan.

b. Destrucción o eliminación de la información y medios

Se deberán establecer los lineamientos y controles necesarios que garanticen que la información confidencial sea eliminada y los medios que la almacenaban sean destruidos cuando los mismos no sean requeridos por los procesos de negocio. Lo anterior respentando y considerando los periodos mínimos de retención de información que debe respetar la Financiera.

c. Traslados de la información

Se debe implementar los controles a los medios de almacenamiento que son transportados fuera de la Financiera con el fin de protegerlos contra accesos, uso o modificaciones no autorizados durante su transporte.

3.4 Control de acceso

3.4.1 Administración de cuentas de usuarios y contraseñas

Se deberá implementar los procedimientos necesarios que permitan controlar la creación, modificación, desactivación y eliminación de usuarios, administración de contraseñas y permisos de acceso a los recursos tecnológicos y a la información de la Financiera.

Todo acceso a la información de la Financiera debe ser provisto basado en el puesto desempeñado y durante el periodo establecido, de manera que la información solo sea utilizada por aquellas personas que tienen una necesidad legítima con la información.

Se deberán de implementar controles que garanticen que terceros, los cuales realicen trabajos a la Financiera, solo tengan los accesos necesarios para desempeñar sus funciones y durante el periodo establecido para ejecutar esas labores.

3.4.2 Acceso a internet – uso correo electrónico

Se deberán establecer los lineamientos mínimos necesarios que delimiten el uso de las herramientas de internet y correo electrónico a únicamente asuntos laborales relacionados a la Financiera.

3.4.3 Acceso código fuente de programas

Se deberán establecer controles que resguarden el acceso a archivos ejecutables, código fuente, librerías y otra documentación o recursos asociados al diseño de una aplicación o sistema. Asimismo, el acceso a estos deberá ser otorgado únicamente al personal que, para desempeñar sus funciones, requieran del acceso.

3.5 Acceso físico

Se deberán de implementar controles y lineamientos que prevengan el acceso físico no autorizado, daños e interferencias a los activos y recursos de procesamiento de la información de la Financiera.

3.6 Seguridad de las operaciones

3.6.1 Procedimientos y responsabilidades operacionales

Se deberán implementar los lineamientos necesarios que garanticen que la información es procesada de manera correcta y segura, y que se dispone de la documentación necesaria para los usuarios

3.6.2 Protección contra código malicioso

Se deberán establecer los controles necesarios que permitan asegurar que el equipo de cómputo, así como las instalaciones de procesamiento de la información se encuentran protegidas contra código malicioso (*Malware*, virus, entre otros)

3.6.3 Respaldos

Se deberán establecer los lineamientos necesarios que permitan definir la periodicidad y la información que deberá ser respaldada con el fin de minimizar el impacto de perder esa información, así mismo el cronograma definido de respaldos no deberá afectar la operativa diaria de la Financiera

3.6.4 Control de software operativo

Se deberá establecer los lineamientos de prohibición para la descarga, instalación, implementación o uso de *software* no autorizado y/o sin licenciamiento.

3.6.5 Controles de auditoría de sistemas de información

La planificación de auditorías y monitoreo de la Financiera deben enfocarse en la evaluación y aplicación de los sistemas, los equipos relacionados con la infraestructura de red, servidores y equipo de cómputo en general.

3.7 Seguridad de las comunicaciones

3.7.1 Seguridad de los servicios de red.

Se debe implementar controles de seguridad y procedimientos de administración asociados, por ejemplo, *firewalls*, dispositivos de seguridad, segmentación de redes y

detección de intrusos, para autorizar acceso y controlar los flujos de información desde y hacia las redes de la Financiera.

3.7.2 Acuerdos de transferencia de información.

Se deberán establecer acuerdos formales con los colaboradores, los cuales establezcan las prohibiciones y/o autorizaciones respecto a copiar, transferir, almacenar, transferir y/o reenviar información que le pertenece a la Financiera, como por ejemplo: información de clientes, otros colaboradores y/o proveedores, a personas externas no autorizadas.

3.8 Gestión de incidentes de seguridad de la información

3.8.1 Responsabilidades y procedimientos.

Se deberán definir, asignar y mantener los roles y responsabilidades, así los lineamientos necesarios que permitan gestionar los incidentes de seguridad de la información. Esos lineamientos deberán considerar al menos un proceso de comunicación, un proceso de resolución y un proceso de evaluación de impacto asociado al incidente.

3.8.2 Reporte de eventos de seguridad de la información.

Se debe establecer un procedimiento formal de comunicación de eventos de seguridad de la información, junto con un procedimiento de respuesta y escalado de incidentes, que permitan una pronta respuesta a los eventos.

3.8.3 Evaluación y decisión sobre los eventos de seguridad de la información

Se deberán establecer lineamientos que permitan evaluar cada evento y que permitan determinar si se debe clasificar como incidentes de seguridad.

4. REFERENCIAS

Documento	Descripción del Documento
ISO 27001	Estándar para la seguridad de la información.
COBIT 2019	Marco de mejores prácticas a nivel de tecnologías.

5. DEFINICIONES

Términos	Definición
Activo	Es cualquier dato, dispositivo u otro componente del entorno que apoya actividades relacionadas con la información. Los activos incluyen generalmente hardware (servidores y *switches*), *software* (por ejemplo, aplicaciones de misión crítica y sistemas de apoyo) e información confidencial.
Auditoría	Disciplina incluida en el campo de la auditoría que se refiere al análisis de las condiciones de una instalación informática por un auditor externo e independiente que realiza un dictamen sobre diferentes aspectos.
Código fuente	Es el texto que contiene las instrucciones del programa, escritas en el lenguaje de programación. Se trata de un archivo de texto legible que se puede copiar, modificar e imprimir sin dificultad.
Contraseña	Medida de seguridad para restringir los nombres de inicio de sesión a cuentas de usuario y el acceso a los sistemas y recursos.
Correo electrónico	Permiten la interconexión de ordenadores para el intercambio de mensajes, documentos, informaciones, etc.
Cuenta	Una cuenta de usuario nos permite autenticarnos a los servicios de un sistema. A una cuenta se le identifica por un nombre de usuario (comúnmente conocido como login) y una contraseña (o password).
Firewall	Mecanismo que permite que las comunicaciones entre una red local e Internet se realicen conforme a las políticas de seguridad de quien los instala.
Impacto	Una medida del efecto de una incidencia, problema o cambio en los procesos de negocio.
Incidente	Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción de este o una reducción de la calidad de dicho servicio
Lineamientos	Enfoque y la dirección de un conjunto de ideas

Malware	Es un *software* que tiene como objetivo infiltrarse en o dañar una computadora sin el conocimiento de su dueño y con finalidades muy diversas ya que en esta categoría encontramos desde un troyano hasta un *spyware*.
Riesgo	Posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufra perjuicio o daño.
Roles	Función o papel que cumple alguien o algo.
Seguridad de la información	Persigue la protección de la información y de los sistemas de información del acceso, de utilización, divulgación o destrucción no autorizada.
Sistema	Es un conjunto de partes o elementos organizados y relacionados que interactúan entre sí para lograr un objetivo. Los sistemas reciben (entrada) datos, energía o materia del ambiente y proveen (salida) información, energía o materia.
Software	Es un término genérico que designa al conjunto de programas de distinto tipo (sistema operativo y aplicaciones diversas) que hacen posible operar con el ordenador.
Virus	Es un programa informático que se ejecuta en el ordenador sin previo aviso y que puede corromper el resto de los programas, ficheros de datos e, incluso el mismo sistema operativo.
Vulnerabilidad	La vulnerabilidad es la potencialidad o la posibilidad de que se materialice una amenaza sobre el activo de información.

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
	1.0		Elaboración del primer documento

1. OBJETIVO

Alcanzar y mantener una protección adecuada de los activos e información de la Financiera Desyfin S.A.

2. ALCANCE

Los rubros en la presente política aplican a todos los colaboradores, personal temporal y practicantes de Financiera Desyfin S.A, Costa Rica, así como otras personas relacionadas con terceras partes que utilicen recursos tecnológicos e informáticos que tengan que ver con la Financiera.

3. DESCRIPCIÓN

3.1 Estructura del documento

- **Gestión de Activos. (3.2)**
  - Responsabilidad por los activos. (3.2.1)
  - Clasificación de la información. (3.2.2)
  - Etiquetado de la información (3.2.3)
  - Manejo de los activos (3.2.4)
- **Manejo de los medios. (3.3)**
  - Gestión de medios removibles. (3.3.1)
  - Destrucción o eliminación de la información. (3.3.2)
  - Traslados de la información (3.3.3)

3.2 Gestión de activos

3.2.1. Responsabilidad por los activos.

- ✓ Departamento de Informática:

- Custodiará todos los activos informáticos de la Financiera.
- Asignará los equipos informáticos a todos los usuarios, de acuerdo con los requerimientos de las áreas.
- Verificará que no le sea asignado un mismo activo informático a más de un colaborador.
- Verificará que los usuarios sean empleados regulares de la Financiera, así como contratistas externos, consultores, practicantes, etc.
- Llevará el control de los equipos asignados al personal.

- ✓ Responsabilidades de los usuarios:

- Será responsable de la custodia de los equipos informáticos asignados (Pc, monitores, teclados, impresoras, USB, etc.)
- Notificará, por medio de la mesa de ayuda los inconvenientes o anomalías presentada con los equipos, accesorios, impresoras, sistemas, entre otros.

3.2.2. Clasificación de la información.

- ✓ Información pública

Esta es información general como cierta información técnica o información utilizada por los empleados, proveedores de servicios o practicantes de la Financiera, la cual puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la Financiera o no.
Esta información en caso de ser conocida, utilizada o modificada por personas, sin la debida autorización, no impactaría de manera significativa a los clientes, sistemas o procesos de la Financiera.

- ✓ Información interna

Información que puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y entidades externas debidamente autorizadas, y cuya

divulgación o uso no autorizados podría incrementar el riesgos o derivar en pérdidas leves a la Financiera o terceros.

- ✓ Información confidencial

Información con un alto nivel de sensibilidad y que se requiere su uso estricto y exclusivo por un grupo muy reducido de empleados, generalmente de la alta dirección, custodio y dueño.
La distribución no autorizada de esta información puede impactar significativamente los resultados operativos de la organización, a sus accionistas, socios estratégicos de negocio o a sus clientes.
Toda la información confidencial, desde el momento de su creación hasta el momento que es destruida o desclasificada, debe estar marcada con la designación apropiada.

3.2.3 Etiquetado de la información.

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y etiquetados en función a ello, con el objetivo de señalar cómo han de ser tratados y protegidos.

- Documentos en papel: se indica el nivel de confidencialidad en la esquina superior derecha de cada página del documento; también se indica en la portada o en el sobre que contiene dicho documento, como también en la carpeta de archivo en la que se guarda el documento.

- Documentos electrónicos: se indica el nivel de confidencialidad en la esquina superior derecha de cada página del documento.

- Sistemas de información: el acceso a niveles de confidencialidad en aplicaciones y bases de datos debe ser otorgado solo al personal respectivo por medio de roles.

- Correo electrónico: se indica el nivel de confidencialidad en el asunto del correo y en el pie del mensaje inscrito deberá llevar la marca de agua utilizado.

- Carpetas compartidas: se otorgará acceso a la información a las carpetas solo con la autorización del dueño de la información almacenada en dicha carpeta.

- En los casos que aplique deben estar firmados digitalmente.

3.2.4 Manejo de los activos.

- El tratamiento de la información se debe realizar a través de los procedimientos y estándares definidos para la misma, con el objetivo de proteger esta información de la divulgación no autorizada o del mal uso.

- Todo activo dentro de la Financiera debe estar etiquetado e inventariado.

- Usar los servicios de almacenamiento en la nube autorizados por la Financiera.

- Registro de usuarios y dispositivos: se deberá mantener un registro de dispositivos detallando los privilegios de acceso asignados a cada usuario que los necesite.

- Utilizar repositorios comunes para el intercambio de información, que sean propios de la Financiera.

3.3 Manejo de los medios

3.3.1. Gestión de medios removibles.

- El uso de medios de almacenamiento removibles tales como, pero no limitado a: discos duros externos y memorias externas – USB, por parte de los colaboradores de la Financiera está restringido.

- Los medios de almacenamiento removibles aceptados, deberán contar con la encriptación realizada por el Departamento de Informática para el uso autorizado, de esta medida quedan excentos los medios de los cuales Informática no cuenten con las herramientas para su encriptación.

- Las excepciones deben estar aprobadas por el gerente de departamento según corresponda.

- En caso de una eventualidad, se deberá solicitar el cambio de contraseña de acceso al dispositivo.

- Desactivar la opción de autoarranque en los equipos para no permitir posibles ejecuciones automáticas no deseadas cuando los dispositivos extraíbles son enchufados.

- Deshabilitar por defecto los puertos USB y habilitarlos para el personal que necesite dicha funcionalidad de manera periódica o gestione ficheros de gran tamaño.

3.3.2. Destrucción o eliminación de la información.

- La información de la Financiera puede ser destruida o eliminada cuando no sea requerida por los procesos de negocio, considerando los límites de retención establecidos por las leyes, regulaciones nacionales o internacionales que aplique a la Financiera.

- Documentos físicos y electrónicos que contengan información clasificada como confidencial por la Financiera, deberán ser destruidos o eliminados garantizando que la información no pueda ser reconstruida posterior a su destrucción. Para ello se puede utilizar un formateo de bajo nivel o destrucción física dejando su evidencia.

- Se deberán implementar controles que prevengan la destrucción o eliminación no autorizada de información, por parte de colaboradores o terceros.

3.3.3. Traslado de la información.

- Se debe tomar las medidas de seguridad necesarias para el traslado de los medios de respaldo a la bóveda de seguridad o lugar de resguardo: sobre con cintas de seguridad, boleta de envío y recibido.

- Todo medio de almacenamiento removibles tales como, pero no limitado a: discos duros externos y memorias externas – USB, deberán contar con su debida autorización y encriptación para ser trasladada.

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
	1.0		Elaboración del primer documento

1. OBJETIVO

Administrar adecuadamente las cuentas de usuarios y contraseñas de acceso a los sistemas y aplicaciones por parte de los colaboradores y terceros en la Financiera.

2. ALCANCE

Los rubros en la presente política aplican a todos los colaboradores, personal temporal y practicantes de Financiera Desyfin S.A, Costa Rica, así como otras personas relacionadas con terceras partes que utilicen recursos tecnológicos e informáticos que tengan que ver con la Financiera.

3. DESCRIPCIÓN

3.1 Estructura del documento

- Control de acceso y gestión de contraseñas. (3.2)
  - ID de usuarios (3.2.1)
  - Características de seguridad de las contraseñas, longitud y frecuencia de cambios. (3.2.2)
  - Usuarios funcionales (3.2.3)
  - Usuarios administradores (3.2.4)
  - Manipulaciones de la contraseña – prohibiciones. (3.2.5)

3.2 Control de acceso y gestión de contraseñas.

3.2.1. ID de usuarios.

- La Financiera requiere que cada colaborador que accede a los sistemas computacionales posea un ID de usuario único y una contraseña privada, de su exclusivo conocimiento.

- Todos los accesos a los sistemas deben ser por medio de ID de usuarios que sean claramente identificables, utilizando la nomenclatura siguiente:
  a. El nombre de usuario se creará considerando el primer nombre acompañado de un guion y las iniciales de los dos apellidos.

  b. En caso de que el nombre de usuario ya esté registrado se procederá a utilizar el primer nombre acompañado de la primera letra del segundo nombre, un guion y las iniciales de los dos apellidos.

  c. En los casos donde se siga detectando que el usuario ya existe, se deberán seguir agregando letras del segundo nombre y apellidos hasta que se logre un usuario único.

  Por ejemplo: “Santiago José Bermúdez Salazar” se registraría como “santiago-bs”, si existiera otra persona con el mismo nombre e iniciales de sus apellidos, su nombre de usuario quedaría como “santiagoj-bs”.

- Los ID de usuarios deben ser usados para otorgar y restringir los privilegios de acceso al sistema basado en perfiles laborales, responsabilidades y otras actividades de negocios.

- Cada colaborador es personalmente responsable por el uso que se le dé a su ID de usuario y contraseña.

- El Departamento de Informática es responsable de ejecutar la creación, modificación y suspensión de las cuentas de usuario de red o dominio, las cuales deberán ser solicitadas por las Jefaturas, Responsables del Departamentos o Gerencias, por medio del sistema de soporte.

- El Departamento de Auditoría, así como cada jefatura, responsable del departamento o gerencias, serán responsables de las revisiones periódicas de cuentas inactivas para tomar las acciones respectivas sobre ellas.

- Las sesiones de usuario deberán tener configurados los tiempos de inactividad, lo cual permita el cierre automático de las sesiones después de un período de inactividad definido. El tiempo configurado no podrá exceder un rango 15 minutos.

- Se deberán crear restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo. Ese tiempo deberá considerar únicamente el tiempo en el que el colaborador desempeñe sus funciones, si el mismo requiere trabajar fuera de horario laboral deberá tramitarse por medio del sistema de soporte con la autorización de la Jefatura o de la Gerencia de Operaciones.

3.2.2. Características de seguridad de las contraseñas, longitud y frecuencia de cambios.

- Las contraseñas predeterminadas por el proveedor se deben cambiar inmediatamente después de la instalación de los sistemas, *software* o *hardware*.

- En lo posible las aplicaciones que sean utilizadas por la Financiera deberán estar integradas con el Directorio Activo (AD).

- Si los sistemas no pueden ser integrados con el Directorio Activo, los usuarios deben elegir sus contraseñas en cumplimiento con los estándares de seguridad definidos para cada sistema, como en longitud, según la configuración específica, cambios periódicamente, según este definido para cada sistema, deber ser alfanuméricos y contener caracteres especiales.

- Una contraseña segura deberá cumplir con las siguientes características:

  - ✓ La longitud debe ser al menos de 8 caracteres.
  - ✓ Contener caracteres tanto en mayúsculas como en minúsculas.
  - ✓ Puede tener dígitos y caracteres especiales como _, -, /, *, $, ¡, ¿, =, +
  - ✓ No debe ser una palabra por sí sola.
  - ✓ No debe ser basada en información personal, nombres de familia, palabras específicas del diccionario, entre otras etc.

- Ejemplos de contraseñas no seguras:

  - ☒ Nombres de familiares, mascotas, amigos, compañeros de trabajo, personajes, etc
  - ☒ Cumpleaños, aniversarios, información personal, teléfonos, códigos postales, etc.
  - ☒ Patrones como 1234?, aaabbb, qwerty, zyxwvuts, etc.
  - ☒ Composiciones simples como: MINOMBRE1, 2minombre, etc

- La frecuencia del cambio de contraseña para los sistemas no deberá exceder los 90 días.

- Cuando un usuario sospeche que su contraseña ha sido descubierta por cualquier otra persona, deberá de informar de la situación al Departamento de Informática y solicitar o realizar el cambio de contraseña de manera inmediata

- La contraseña puede ser conocida por otro usuario, únicamente cuando se emite por primera vez, y estas contraseñas temporales deben ser cambiadas la primera vez que el usuario ingresa al sistema.

3.2.3 Usuarios administradores de sistemas.

- Los usuarios de mayor privilegio deberán estar restringidos a los colaboradores que por funciones requieran el uso de los mismos; no obstante, estos colaboradores deberan tener dos usuarios, uno con los permisos restringidos para sus labores del día a día y el usuario administrador el cual deberá ser utilizado solo cuando las labores lo requieran.

- Todo ID administrador de sistema que incluyen los sistemas por defecto, deben ser deshabilitados y crear los de uso interno.

- Cada administrador del sistema será responsable de generar un documento con las contraseñas vigentes de cada sistema a su cargo, y entregarlas en un sobre sellado a la Gerencia de Operaciones para su custodia. Ese sobre será abierto solo bajo circunstancias de emergencia, en cuyo caso, la primera acción, una vez que se logre ingresa, será cambiar de nuevo todas las claves, generar un nuevo documento y entregarlo en sobre sellado a la Gerencia nuevamente.

- El Departamento de Informática debe mantener actualizada una lista con los sistemas y sus usuarios administradores.

- Toda acción generada por los IDs administradores deben quedar registradas dentro de los sistemas de la Financiera para garantizar que se mantiene la seguridad de los activos de información y se monitorean los registros con fines de cumplimiento normativo.

3.2.4 Usuarios funcionales del sistema.

- La Financiera administrará una lista con las transacciones sensitivas de los sistemas junto con los roles que se utilizan para ejecutar estas funciones.

- Para cada sistema dentro de la Financiera se definirán usuarios los cuales tendrán acceso a realizar transacciones sensitivas dentro de cada aplicación.

- Cada Jefatura deberá solicitar la asignación de los roles a los usuarios al Departamento de Informática por medio del sistema de soporte de usuarios.

- Deben ser verificadas periódicamente las actividades de los usuarios con mayores privilegios en los recursos informáticos de la Financiera para garantizar sus debidas funciones.

- En lo posible las aplicaciones toda transacción que se realice en el sistema se deberá grabar el ID del usuario, la fecha y la hora en que se realizó

3.2.5 Manipulaciones de los usuarios y contraseña - prohibiciones

- La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.

- En lo posible las aplicaciones se desactivará el uso de la utilidad de: ¿Recordar Contraseña? de los sistemas y aplicaciones.

- Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlas en un lugar donde personas no autorizadas puedan acceso y consultarlas.

- Aunque los ID de usuarios puedan ser compartidos por razones de intercambio de información, como correo electrónico y otros usos, las contraseñas jamás deben ser reveladas o compartidas a otros usuarios.

- Los administradores de sistemas, encargados de informática y cualquier otro personal de la Financiera, nunca deben pedirle a un colaborador que revele su contraseña personal.

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
	1.0		Elaboración del primer documento

1. OBJETIVO

Mantener la seguridad física y ambiental en las áreas sensibles de la Financiera, así como la protección de la infraestructura ubicada en el edificio principal y sedes.

2. ALCANCE

Los rubros en la presente política aplican a todos los colaboradores, personal temporal y practicantes de Financiera Desyfin S.A, Costa Rica, así como otras personas relacionadas con terceras partes que utilicen recursos tecnológicos e informáticos que tengan que ver con la Financiera.

3. DESCRIPCIÓN

3.1 Estructura del documento

- **Seguridad del Data Center. (3.2)**
  - Acceso al data center. (3.2.1)
  - Controles ambientales y de seguridad (3.2.2)
- **Aseguramiento de oficinas, salas e instalaciones (3.3)**
  - Administración de la seguridad del personal (3.3.1)
- **Aseguramiento de equipos de cómputos (3.4)**
  - Colocación y protección del equipo (3.4.1)
  - Pantalla y escritorios limpios (3.4.2)

3.2 Seguridad del Data Center.

3.2.1 Acceso al Data Center

- La administración del acceso al Data Center es regulada por la Jefatura de Informática, todo ingreso de personas no autorizadas deberá quedar tramitada por el sistema de soporte de la Financiera.

- El acceso a externos será concedido solo para propósitos específicos y autorizados, proporcionándoles instrucciones sobre los requisitos de seguridad del área.

- La fecha, hora de entrada y salida de visitantes debe ser registrada, Toda esta información debe registrarse en la bitácora física del centro de datos.

- Todos los visitantes deben ser supervisados todo el tiempo que se encuentren en las instalaciones del Data Center y estos deben estar acompañados por personal responsable de Informática.

- La puerta de ingreso al Data Center deberá ser regulada, garantizando que solo el personal autorizado previamente por la Financiera tenga aceso.

3.2.2 Controles ambientales y de seguridad

- Se deberán de implementar controles ambientales en el Data Center de la Financiera así como lugar que se considere necesario, por ejemplo:

  - Dispositivos mínimos del DataCenter:
    - Sensores de temperatura y humedad
    - Aire acondicionado
    - Detectores de humo
    - Cámaras de seguridad
    - Extintores o supresores de fuego
    - Piso elevado o falso
    - UPS

  - Dispositivos mínimos en otras áreas que se considere necesario
    - Cámaras de seguridad
    - Sensores de humo
    - Extintores o supresores de fuego

- En los casos que sea posible se deberá monitorear de manera periódica los controles ambientales; adicionalmente, se deberán de realizar mantenimientos preventivos de manera periódica con el fin de garantizar el funcionamiento.

- Las instalaciones deben estar protegidas de riesgos como robo, hurto o daño; adicionalmente, se deberán implementar los controles ambientales mencionados anteriormente y garantizar aspectos tales como: suministro de energía y cableado.

- Todos los incidentes relacionados con el entorno del Data Center deben ser ingresados a la mesa de ayuda para su debida atención.

- Se prohíbe el consumo de alimentos, bebidas, fumado y almacenamiento de documentos en áreas consideradas seguras, como por ejemplo el Data Center. La Bitácora del Data Center deberá contar con una leyenda que indique estas restricciones, la cual deberá ser firmada por terceros con el fin de garantizar el conocimiento y el cumplimiento de estas por parte de terceros.

- El Departamento de Informática debe brindar la seguridad necesaria para el cableado de telecomunicaciones para evitar interrupciones dentro de la Financiera.

3.3 Aseguramiento de oficinas, salas e instalaciones

3.3.1 Administración de la seguridad del personal.

- Se deben identificar las áreas seguras dentro de la Financiera, en los casos que la financiera considere necesario podrá identificarlas utilizando rótulos, señales y placas, entre otros mecanismos que se consideren apropiados.

- Toda visita, que no sea cliente de cajas o plataforma de servicio, deberá identificarse en la recepción y se le deberá asignar un gafete de visita. La visita deberá esperar en la recepción a que un colaborador, el cual será el responsable de la visita y deberá acompañarlo durante toda la estadía en las instalaciones de Desyfin.

- Para las visitas que deban ingresar a áreas definidas como seguras por la Financiera, se deberá tramitar el permiso de ingreso de previo y siguiendo los lineamientos para dicha solicitud según el área a visitar.

- Todo funcionario, personas y empresas que prestan servicios profesionales y técnicos a la Financiera deben portar el carnet asignado en un lugar visible.

- El personal de Seguridad debe revisar el contenido de toda maleta, bolsa, caja u otro que presente sospechas para prevenir la sustracción de componentes de equipos de cómputo o de información en medios magnéticos o físicos.

- Se debe desarrollar los controles necesarios para proteger a sus funcionarios contra amenazas naturales o producidas por el hombre.

3.4 Aseguramiento de equipos de cómputos

3.4.1 Colocación y protección del equipo.

- La Financiera debe brindar a sus colaboradores los equipos de cómputo y recursos tecnológicos necesarios para el cumplimiento de sus funciones. Dichos equipos no podrán utilizarse para funciones ajenas a las de la Financiera.

- El Departamento de Informática debe definir los requerimientos para el mantenimiento preventivo y correctivo de los equipos tecnológicos, así como de los controles para su implementación y velar por su cumplimiento.

- Está prohibida la descarga, instalación, implementación o uso de *software* no autorizado y/o sin licenciamiento.

- Los colaboradores que dispongan de computadoras portátiles deben tomar todas las medidas adecuadas para la protección de estas, así como sacar el equipo de la Financiera solo cuando sea necesario y con previa autorización de la Jefatura inmediata.

- En caso de personal externo, que por sus labores necesiten hacer uso de la red o recursos tecnológicos de la Financiera con equipos de su propiedad, la Jefatura responsable de los trabajos a realizar debe solicitar al Departamento de Informática la revisión de las herramientas de antivirus y sistema operativo debidamente parchado, antes de que dicho funcionario tenga acceso a la red o recursos requeridos.

- Es responsabilidad de cada colaborador apagar los equipos tecnológicos asignados al finalizar su jornada laboral o durante periodos de inactividad, salvo casos en los que sea estrictamente necesario mantenerlos funcionando.

3.4.2 Pantalla y escritorios limpios.

- Los puestos de trabajo deben permanecer limpios y ordenados.

- Al levantarse del puesto de trabajo y al finalizar la jornada laboral, los escritorios deben permanecer despejados y libres de documentos físicos y/o medios extraíbles, estos deben guardarse en un lugar seguro y bajo llave.

- Al no estar en el puesto de trabajo, se debe bloquear la sesión de los equipos de cómputo para proteger el acceso a las aplicaciones y servicios de la Financiera.

- Cuando se imprima o digitalice documentos con información interna o confidencial, estos deben retirarse inmediatamente de dichos dispositivos.

- Los dispositivos de impresión y digitalización deben permanecer limpios de documentos.

- Los gabinetes, cajones y archivadores de contengan documentos y/o medios extraíbles con información deben quedar cerrados durante la hora de almuerzo y al finalizar la jornada laboral.

- Los basureros de cada escritorio son exclusivamente para depositar basura NO biodegradable, lo que quiere decir que no se debe tirar residuos de comida, tampoco debe depositarse cajitas de refrescos, vasos de café, etc., lo anterior debido a que los basureros no tienen bolsa de basura y sería muy poco higiénico tirar otro tipo de basura que no sean desechos de oficina.

- Sobre los escritorios solamente deben tener lo siguiente:

- ✓ Teléfono.
- ✓ Monitor.
- ✓ Impresora (en los cubículos necesarios).
- ✓ Calendario de escritorio de Financiera Desyfin.
- ✓ *Mousepad* de Financiera Desyfin.
- ✓ Se prohíbe cualquier otro tipo de decoración personal o elemento de trabajo distinto al citado anteriormente.
- ✓ Todos los documentos y/o expedientes necesarios para el trabajo diario deberán estar debidamente almacenados en sus gavetas archivos designados para ello. Ningún documento o papel puede quedar encima de los escritorios.
- ✓ Mantenga solo los documentos o papeles necesarios.
- ✓ Archive diariamente todo aquello que no debe permanecer en el escritorio.
- ✓ Retire de su cubículo matas, fotos, muñecos de colección u otros.
- ✓ No aglomere sacos, zapatos, bolsos en las áreas de trabajo.
- ✓ No mantenga comida ni recipientes sobre su escritorio.
  Recicle todos los documentos que no son necesarios y que se encuentran sobre su escritorio.

- ✓ El escritorio y área de trabajo debe de permanecer con la menor cantidad de artículos posibles y mantener solo lo estrictamente necesario.

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
	1.0		Elaboración del primer documento

1. OBJETIVO

Establecer los lineamientos y responsabilidades para recibir, catalogar y resolver solicitudes de nuevas aplicaciones o de modificaciones a las existentes.

2. ALCANCE

Aplica única y exclusivamente para los cambios a los sistemas provistos por el Departamento de Informática a la Financiera Desyfin S.A.

3. DESCRIPCIÓN

3.1 Estructura del documento

- **Administración del cambio (3.2)**
  - Cambios normales (3.2.1)
  - Cambios estandar – frecuentes (3.2.2)
  - Cambios de emergencia (3.2.3)
  - Priorización de los cambios (3.2.4)

3.2 Administración del cambio

3.2.1. Cambios normales.

- Todos los cambios deben ser registrados y documentados por medio del sistema de soporte de la Financiera; adicionalmente, esos cambios deberán estar ingresado o aprobados al menos por el *Key User* del módulo de SAP afectado.

- Todos los cambios solicitados deben ser evaluados, autorizados, aceptados, documentados, probados y cerrados sin excepción, con la finalidad de evitar impactos negativos en la calidad, confidencialidad, integridad, disponibilidad y funcionalidad de los sistemas y servicios.

- Todo cambio debe ser valorado por la encargada de SAP y los *Key Users* de los módulos de SAP afectados, los cuales deberán realizar evaluaciones de impacto, priorización para todas las solicitudes de cambio, y la Gerencia de Operaciones debe dar las autorizaciones respectivas.

- Cada vez que se efectúen cambios a nivel de sistema operativo, las aplicaciones críticas para el negocio deben ser revisadas y probadas de manera que se aseguren que no habrá un impacto adverso en la operación o en la seguridad.

- Todos los cambios en *software* y *hardware* deben ser desarrollados en un ambiente de prueba, validados y certificados antes de pasar al ambiente de producción. Se excluye de este lineamiento el *hardware* que por sus características no pueda ser certificado antes de ponerlo a producción.

- Se deben establecer los planes de reversión de forma tal que se mitigue cualquier situación adversa a la hora de implementar el cambio.

- Se debe establecer un plan de liberación del cambio, considerando la construcción del cambio, la documentación de las pruebas, la implementación, fechas y horas para la liberación, situaciones de aceptación y no aceptación.

3.2.2. Cambios estándares – frecuentes

- Los cambios estándar deben ser formalmente documentados y aprobados por la Jefatura de Informática.

- La lista de cambios estándar debe ser revisada periódicamente por el Departamento de Informática y los líderes del producto, para asegurar su actualización, completitud y alineación con las necesidades de la Financiera.

- Los cambios frecuentes han sido preaprobados por la Jefatura de Informática y por lo tanto no necesitan pasar por nuevas aprobaciones durante el proceso de administración de cambios, por ejemplo (cambios de contraseña).

3.2.3. Cambios de emergencia.

- Es considerado cambio de emergencia, cuando el impacto afecta de manera inmediata y critica la operativa en la Financiera.

- Para la implementación de los cambios de emergencia debe ser autorizada por la Gerencia de Operaciones.

- Todo cambio de emergencia se debe implementar lo más pronto posible.

- La documentación de los cambios de emergencia puede realizarse posterior a su implementación en el mínimo tiempo posible después de que el cambio fue implementado al mismo tiempo se le debe dar seguimiento al cambio.

3.2.3. Priorización de los cambios.

- La prioridad de los cambios se compondrá de dos factores:

    - **Impacto**: se estima por el grado o cantidad de daño a la Financiera.
    - **Urgencia**: se estima el tiempo y disponibilidad de los recursos de la Financiera para su implementación.

  Para catalogar el impacto se consideran aspectos como:

    - ¿Cuál es la cantidad de clientes/usuarios afectados?
    - ¿Cuál es impacto monetario causado por el incidente?
    - ¿Cuál es la cantidad de sistemas / elementos involucrados?

Para la clasificación de la urgencia se consideran los niveles:

- Bajo: 7 días
- Medio: 5 días
- Alto: 8 horas

El valor final de priorización del cambio corresponde a la siguiente matriz:

		Impacto		
	Prioridad	**Baja**	**Media**	**Alta**
URGENCIA	**Baja**	Baja	Baja	Media
	Media	Baja	Media	Alta
	Alta	Media	Alta	Alta

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
	1.0		Elaboración del primer documento

1. OBJETIVO

Asegurar que operaciones que rigen del uso de la Internet sean relacionadas con las actividades de la Financiera.

2. ALCANCE

Los rubros en la presente política aplican a todos los colaboradores, personal temporal y practicantes de Financiera Desyfin S.A, Costa Rica, así como otras personas relacionadas con terceras partes que utilicen recursos tecnológicos e informáticos que tengan que ver con la Financiera.

3. DESCRIPCIÓN

3.1 Estructura del documento

- **Restricciones a las comunicaiones (3.2)**
  - Control de acceso (3.2.1)
  - Uso de Internet (3.2.2)
  - Intercambio de información (3.2.3)
  - Requerimientos para la conexión de equipo de terceros (3.2.4)

3.2 Restricciones a las comunicaciones

3.2.1. Control de acceso.

- El acceso a la Internet será otorgado según las funciones que se desempaña en cada puesto, este será solicitado únicamente por la Jefatura del colaborador.

- No todos los colaboradores deben tener acceso a navegación por Internet en el equipo asignado para ejercer sus labores.

- La conexión a Internet debe realizarse por los medios autorizados por el Departamento de Informática.

- Toda conexión por parte del colaborador desde y hacia la Internet, será llevada a cabo a través de un servidor interno. Este servidor tendrá los controles de acceso, muros protectores (*firewalls*) y sistemas que monitorea para salvaguardar la integridad y seguridad de los datos y comunicaciones.

- Solamente los clientes debidamente autorizadas podrán contar con el acceso a internet para visitantes. Esto incluye también el acceso a Internet mediante una red inalámbrica – WiFi.

3.2.2 Uso de Internet

- Está estrictamente prohibido el acceso a páginas web con contenidos ilícitos, material pornográfico, de contenido racista, homofobia o cualquier material que atente contra la dignidad y principios morales.

- De igual forma, queda prohibido a cualquier colaborador utilizar el tiempo laboral para accesar a redes sociales, correos personales o páginas de interés propio, através de la red de la Financiera.

- Se prohíbe terminantemente bajar música, películas, programas, juegos o cualquier otra aplicación que no tengan relación con las labores de la Financiera y que además perjudiquen el funcionamiento de la red y capacidad de almacenamiento de las máquinas.

- La Financiera prohíbe el uso de servicios de radio y televisión por Internet, participar de videojuegos, apuestas o casinos en línea y sitios web similares.

- De manera semestral, el Departamento de Informática monitoreará el servicio de Internet, generando un reporte con el detalle del uso de este servicio. De existir cualquier anomalía se reportará a los miembros del Comité de TI.

3.2.3 Intercambio de información

- Los colaboradores de la Financiera no divulgarán a través de la Internet información interna que pudiera afectar adversamente las operaciones, negociaciones, relaciones con los clientes o imagen pública de la misma, salvo que cuenten con la aprobación previa y escrita de la Gerencia.

- En caso de que alguna información interna o confidencial, de la Financiera se pierda o se divulgue a terceros no autorizadas a través de la Internet, o cuando se sospeche dicha pérdida o divulgación, la persona que lo detecte debe informar al Departamento de Informática de inmediato por medio del sistema de soporte.

3.2.4 Requerimientos para la conexión de equipo de terceros

- Debe contar con la versión actualizada del *software* de antivirus que esté soportada por el fabricante con su respectiva licencia original.

- El sistema operativo debe contar con los últimos parches de seguridad, cabe destacar que el sistema operativo debe ser licenciado y cumplir con su respectivo mantenimiento.

- Protección *anti-spyware* debidamente actualizada.

- En cuyo caso que los equipos no cuenten con lo estipulado, se puede realizar una excepción siempre y cuando se le comunique al tercero que va hacer monitoreado por parte del Departamento de Informática al momento de estar conectado a la red.

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
	1.0		Elaboración del primer documento

1. OBJETIVO

Establecer las pautas y lineamientos en relación con respaldo y la recuperación de los datos propios de la Financiera asegurando su confidencialidad, integridad y disponibilidad.

2. ALCANCE

Aplica única y exclusivamente para los respaldos provistos por el Departamento de Informática a la Financiera Desyfin S.A.

3. DESCRIPCIÓN

3.1 Estructura del documento

- **Administración de respaldos (3.2)**
  - Componentes necesarios de respaldar (3.2.1)
  - Lineamientos de respaldos y recuperación (3.2.2)

3.2 Administración de respaldos.

3.2.1. Componentes a respaldar

- Máquinas virtuales.
- Servidores (dominio, base de datos, archivos, aplicaciones).
- Datos y estructura de la base de datos.
- Archivos de usuarios acorde a prioridad de clasificación.

3.2.2. Lineamientos de respaldos y recuperación

- Informática debe tener claramente definido el personal que tendrá la responsabilidad de realizar los distintos tipos de respaldos.

- El personal no solo debe ser capaz de generar el respaldo, sino estar capacitado para la recuperación de la información en caso de ser necesario, a partir de los distintos tipos de respaldo.

- Debe crearse una programación formal de respaldo. Además, se debe contar con procedimientos de verificación y supervisión de los procesos y del contenido de los respaldos.

- Todos los procesos de respaldo y recuperación deben proveer los elementos que evidencien la ejecución del proceso, detalle el contenido de los mismos, así como errores o inconsistencias en caso de existir.

- Los medios de respaldo deben disponer de etiquetas internas y externas, así como una identificación permanente, que permita determinar fácil y confiablemente su contenido.

- Antes de proceder a la restauración de datos sensitivos o críticos a partir de un respaldo se debe realizar una copia de los mismos para minimizar efectos de corrupción o daños de los datos originalmente respaldados.

- Los respaldos mensualmente se envían a una sucursal, que cumpla y dispongan de condiciones de acceso restringido y de medio ambiente y físicos apropiados que los protejan de cualquier contingencia.

- Se debe tomar las medidas de seguridad necesarias para el traslado de los medios de respaldo a la sucursal.

- La frecuencia de las copias de seguridad se realizará acorde a:

  - ✓ La variación de los datos generados.

  - ✓ El coste de almacenamiento.

- ✓ Los límites de retención de establecidos por las leyes o regulaciones nacionales o internacionales que le apliquen a la Financiera.

- El tipo de respaldo apropiado, se realizará acorde a los recursos y tiempo necesarios para llevarlos a cabo.

  - ✓ Completa: se copia todos los datos a una cinta.

  - ✓ Incremental: solo se graban los datos que han cambiado desde la última copia completa.

  - ✓ Diferencial: se copian los datos que han cambiado desde la última copia completa.

- Se fijará una periodicidad para realizar pruebas de restauración para garantizar que la información necesaria para la continuidad de negocio puede ser recuperada en caso de desastre.

- En caso de ser posible, la información respaldad será cifrada, de esta manera se protege en caso de robo de información o acceso no autorizado.

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
	1.0		Elaboración del primer documento

1. OBJETIVO

Establecer los lineamientos y responsabilidades la administración de incidentes y problemas en los sistemas de información de la Financiera.

2. ALCANCE

Aplica única y exclusivamente para los incidentes o problemas relacionados a los sistemas provistos por el Departamento de Informática a la Financiera Desyfin S.A.

3. DESCRIPCIÓN

3.1 Estructura del documento

- **Administración del problema o incidente (3.2)**
    - Lineamientos (3.2.1)

3.2 Administración del problema o incidente.

3.2.1. Lineamientos

- Todos los funcionarios de la Financiera son responsables de notificar, en el menor tiempo posible a su jefatura inmediata o a Informática, cualquier anomalía en torno a los sistemas informáticos o plataforma tecnológica para iniciar la respectiva investigación y tomar las medidas correctivas pertinentes, esto se llevará a cabo por medio de la mesa de ayuda "SysAid".

- Es responsabilidad del personal de Informática detectar problemas de manera proactiva y reactiva, adicionalmente se debe clasificar el problema de acuerdo a su naturaleza (*software*, infraestructura, recurso humano, proveedores).

- Se deben establecer los parámetros y lineamientos que rijan el proceso de administración de incidentes y problemas, donde se definan los procedimientos necesarios para el reporte de incidentes y problemas, identificación y respuesta, el escalamiento en los casos más críticos y el seguimiento necesario para la adecuada solución, considerando niveles de servicio establecidos.

- Se deben emitir reportes de incidentes y problemas para todos los casos que se presenten. Estos deben ser generados por los funcionarios que atendieron y dieron respuesta a dichos incidentes o problemas.

- Los incidentes y problemas deben ser registrados en un sistema de gestión “SysAid” que permita establecer registros de auditoría y dar el seguimiento apropiado a los casos abiertos, reabiertos, en curso y cerrados.

- En caso que se requiera, se deben realizar estudios de costo-beneficio para la implementación de la resolución de problemas.

- En los casos cuando el costo y el esfuerzo no justifique el beneficio de la resolución del problema o cuando se ha resuelto definitivamente el problema de raíz y se ha validado con el usuario o áreas afectadas, se debe ejecutar el cierre del problema.

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
	1.0		Elaboración del primer documento

1. OBJETIVO

Describir las actividades para la administración de problemas que logren minimizar los impactos adversos de incidentes que son causados por errores en las aplicaciones o infraestructura TI y prevenir incidentes recurrentes relacionados con estos errores.

2. REFERENCIA

- Procedimiento de administración de problemas

3. DEFINICIONES

- **Problema:** Es una condición generalmente identificada como resultado de múltiples incidentes que comparten síntomas comunes. Los problemas pueden ser identificados a partir de único incidente, pero cuya causa es desconocida y el impacto es significativo.

- **Incidente:** Es cualquier evento que no es parte del estándar de operación de un servicio, el cual podría causar interrupción o reducción en la calidad del servicio.

- **Causa raíz:** Es el diagnóstico de la situación que causó el problema o incidente.

4. PROCEDIMIENTO DE ADMINISTRACIÓN DE PROBLEMAS

- **Identificación y clasificación de problemas**

▪ Usuario final ▪ Asistente de TI	1	Identifica la existencia de un problema en *hardware* o *software* de la Financiera.
	2	Ingresa el problema detectado en la herramienta SysAid.
	3	Clasifica la urgencia del problema: ▪ Baja ▪ Normal ▪ Alta ▪ Inmediata
	4	Clasifica el problema según las siguientes categorías: ▪ Archivos ▪ Equipos ▪ Permisos ▪ Programas/Sistemas ▪ SAP
	5	Envía el problema identificado.

- **Gestión de problemas**

▪ Asistente de TI ▪ Especialista SAP	6	Recibe el problema identificado
	7	Identifica la causa-raíz del problema. Para identificar la causa raíz se pueden realizar las siguientes actividades: Revisar el problema y su descripción. Revisar las soluciones

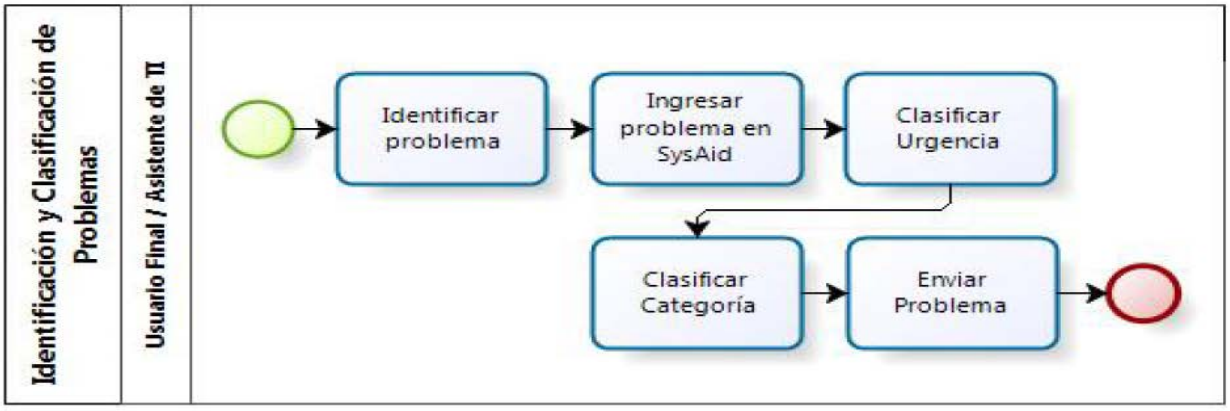
▪ Asistente de TI ▪ Especialista SAP		provisionales dadas. Verificar que la investigación responda las siguientes preguntas: ¿Cuál parte no funciona bien? ¿Dónde ocurre el incidente? ¿Con qué frecuencia ocurren los incidentes? ¿Por qué vuelven a ocurrir los incidentes? ¿Qué otros temas han afectado? Establecer posibles causas del problema. Probar la causa más probable. Verificar la causa real.
	8	Busca en la base de datos de conocimiento en SysAid (Knowledgebase) si se ha documentado algún problema similar. Si se trata de un problema conocido continuar en paso 9, si no en paso 11.
	9	Ejecuta la solución presente en la base de datos de conocimiento.

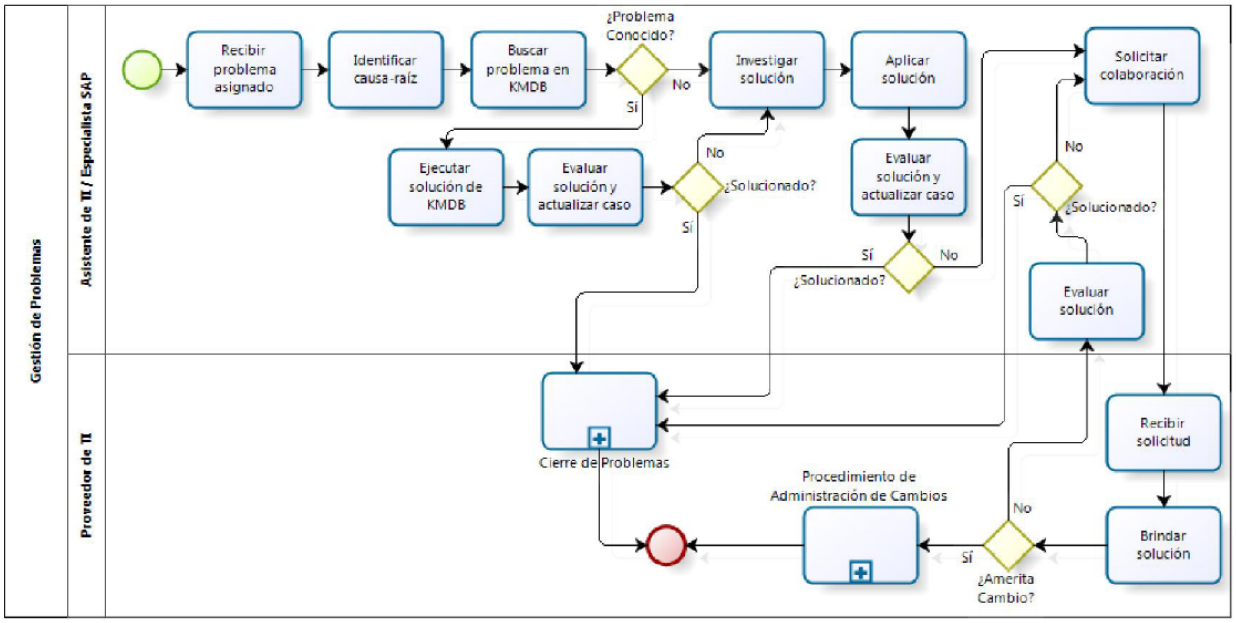
▪ Asistente de TI ▪ Especialista SAP	10	Evalúa si lo ejecutado solucionó el problema y actualiza el estado de la resolución en la herramienta SysAid. Si se logró subsanar continuar en paso 18, de lo contrario en paso 11.
	11	Investiga en el sitio web del proveedor o documentación confiable de resolución del problema
	12	Aplica la solución determinada luego de la investigación efectuada.
	13	Evalúa si se logra resolver el problema y actualiza el estado de la resolución en la herramienta SysAid. Si se resuelve continuar en paso 18, si no en paso 14.
	14	Solicita al proveedor la colaboración para la resolución del problema.
▪ Proveedor de TI	15	Recibe la solicitud de resolución del problema identificado por los colaboradores de la Financiera.
	16	Suministra al personal de

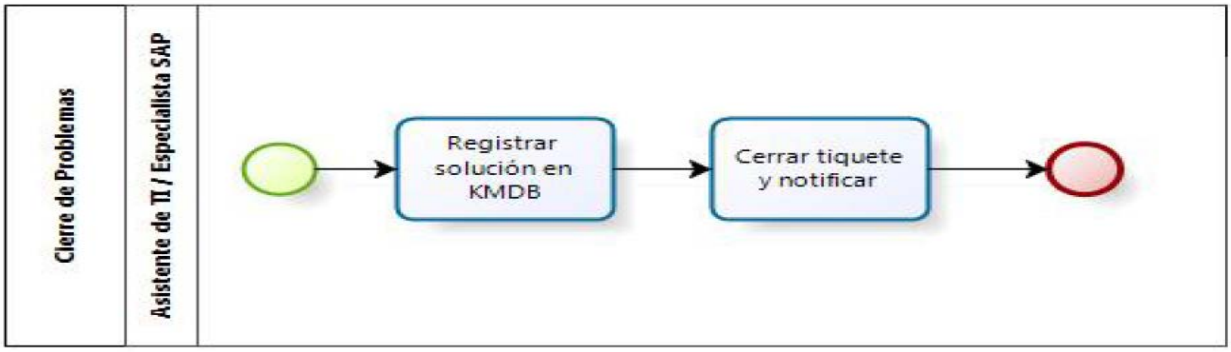
		TI o Especialista SAP las tareas que se deben ejecutar para resolver el problema o bien realizar los cambios necesarios para tratar el mismo. Si se deben realizar cambios pasar al procedimiento de administración de cambios, si no continuar en paso 17.
▪ Asistente de TI ▪ Especialista SAP	17	Evalúa si lo realizado solventó el problema. Si se resolvió continuar en paso 18, caso contrario en paso 14.

- **Cierre de problemas**

▪ Asistente de TI ▪ Especialista SAP	18	Una vez evaluada satisfactoriamente la solución, se evalúa si es de utilidad registrar la solución en la Base de Datos de Conocimientos para referencia futura
▪ Asistente de TI ▪ Especialista SAP	19	Cierra el tiquete en la herramienta SysAid y notifica al usuario que ingresó el problema. Fin del Procedimiento.


Identificación y Clasificación de Problemas
Usuario Final / Asistente de TI
Identificar problema
Ingresar problema en SysAid
Clasificar Urgencia
Clasificar Categoría
Enviar Problema


Gestión de Problemas
Asistente de TI / Especialista SAP
Proveedor de TI
Recibir problema asignado
Identificar causa-raíz
Buscar problema en KMDB
¿Problema Conocido?
No
Sí
Investigar solución
Aplicar solución
Solicitar colaboración
Ejecutar solución de KMDB
Evaluar solución y actualizar caso
¿Solucionado?
Evaluar solución y actualizar caso
¿Solucionado?
Evaluar solución
Cierre de Problemas
Recibir solicitud
Procedimiento de Administración de Cambios
Brindar solución
¿Amerita Cambio?


Cierre de Problemas
Asistente de TI / Especialista SAP
Registrar solución en KMDB
Cerrar tiquete y notificar

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
	1.0		Elaboración del primer documento

1. OBJETIVO

Desarrollar un estándar para gestionar el control de cambios en el área de tecnología de información.

2. ALCANCE

El presente documento coordina las actividades asociadas con los requerimientos de cambios del Área de TI:

- Cambios en aplicaciones.
- Cambios en procedimientos.
- Cambios en parámetros de sistema o configuración.
- Cambios en infraestructura.
- Cambios de emergencia.

3. REFERENCIAS

- Procedimiento de administración de cambios de TI.

4. SEGUIMIENTO Y REPORTE DEL ESTADO DEL CAMBIO

Con el fin de establecer un mecanismo estándar de control centralizado para administrar las solicitudes de cambio, y contar con información actualizada del estado de avance para solicitantes e interesados, se utilizará la herramienta de HelpDesk SYSAID.

5. PREAUTORIZACIÓN DE CAMBIOS ESTÁNDARES O DE RUTINARIOS

La Gerencia de Operaciones autorizará una lista de cambios que, debido a sus características de baja complejidad y bajo riesgo, serán implementados sin la necesidad de seguir este procedimiento.

6. PROCEDIMIENTO DE ADMINISTRACIÓN DE CAMBIOS TI

- **Solicitud de cambios**

Responsable	Número Actividad	Procedimiento
▪ Jefatura de Área ▪ Gerencias ▪ Usuario Final	1	Registra o actualiza la solicitud de cambio mediante correo electrónico, o mediante la herramienta SysAid.
▪ Jefatura de Informática	2	Recibe la solicitud de cambio registrada o actualizada.
	3	Clasifica la solicitud de cambio en las siguientes categorías: ▪ Aplicaciones ▪ Procedimientos (Documentación) ▪ Parámetros de sistema o configuración ▪ Plataforma o infraestructura. ▪ Cambio de Emergencia ▪ Si corresponde a un cambio de emergencia continuar en paso 29, de lo contrario en paso 4.
▪ Jefatura de Informática ▪ Especialista SAP ▪ Dueño del Sistema	4	Evalúa el impacto del cambio en el sistema operacional, así como su funcionalidad, estableciendo en una de las siguientes categorías de impacto: ▪ Crítico, alto, moderado, bajo o muy bajo Esto de acuerdo con los procesos equipos, sistemas, programas o procesos que resulten afectados en forma directa o indirecta por el cambio.
		De acuerdo con la evaluación obtenida del impacto, prioriza el

	5	cambio en uno de los siguientes niveles de urgencia: ▪ inmediato, alto, normal o bajo. Si corresponde a documentación de cambio de emergencia, Fin del Procedimiento; si no, paso 6.

- **Aprobación y asignación del cambio**

▪ Gerencia de ▪ Operaciones ▪ Jefatura de ▪ Informática	6	De acuerdo con lo especificado en la solicitud de cambio, determina si el cambio requerido es aprobado o rechazado. Si el cambio es aprobado continuar en paso 7; si no, Fin del Procedimiento.
	7	Asigna la ejecución del cambio al encargado respectivo. Si corresponde a Aplicaciones continuar en paso 8, Procedimientos, Parámetros o Infraestructura en paso 18.

- **Cambios en las aplicaciones**

▪ Gerencia de Operaciones	8	Analiza el sistema para el cual se solicita el cambio. Si corresponde a SAP continuar en paso 9, de lo contrario en paso 15.
▪ Especialista SAP	9	Recibe la petición de cambio y analiza lo solicitado, para establecer los requerimientos, los cuales van a ser solicitados a la empresa consultora.
	10	Coordina la solicitud de cambio con el especialista de la empresa consultora.
▪ Proveedor SAP	11	Implementa el requerimiento según lo solicitado por la especialista SAP, y solicita probar los cambios realizar para determinar si se desempeñan según lo esperado.
▪ Jefatura de Área ▪ Gerencias ▪ Usuario Final	12	Prueba los cambios realizados por el proveedor y certifica si cumplen lo deseado. Si el cambio es satisfactorio continuar en paso 13, si no en paso 9.
		Si es posible, crea un punto de restauración en el

▪ Proveedor SAP	13	sistema, el cual permita realizar un *rollback* del cambio en caso de presentarse problemas a la hora de ejecutar el cambio en el servidor de producción.
	14	Ejecuta el cambio en el servidor de producción y documenta lo realizado. Continuar en paso 26.
▪ Dueño del sistema	15	Coordina con el proveedor del sistema la solicitud de cambio.
▪ Proveedor de TI	16	Desarrolla y prueba el requerimiento efectuado por los colaboradores de la Financiera.
	17	Implementa el cambio en el ambiente de producción. Continuar en paso 26.

- **Cambios en procedimientos, parámetros e infraestructura**

▪ Jefatura de Informática	18	Identifica los procedimientos, parámetros e infraestructura que se solicita modificar.
	19	Establece los escenarios de prueba necesarios para evitar que la ejecución del

		cambio afecte las operaciones de la Financiera.
	20	Realiza las pruebas necesarias para corroborar que el cambio no afecte las operaciones. En caso de que las pruebas demuestren la afectación de las operaciones continuar en paso 21; si no, en paso 22.
▪ Jefatura de Informática	21	Comunica al solicitante del cambio lo identificado en las pruebas. Continuar en paso 1.
	22	Solicita la aprobación para migrar el cambio a producción
▪ Jefatura de Área ▪ Gerencias ▪ Usuario final	23	Aprueba la migración del cambio a producción. En caso de no aprobar continuar en paso 1.
▪ Jefatura de Informática	24	Realiza el cambio en los procedimientos, parámetros e infraestructura.
	25	Actualiza toda la documentación

		relacionada con los procedimientos, parámetros e infraestructura. Continuar en paso 26.

- **Evaluación y cierre de cambios**

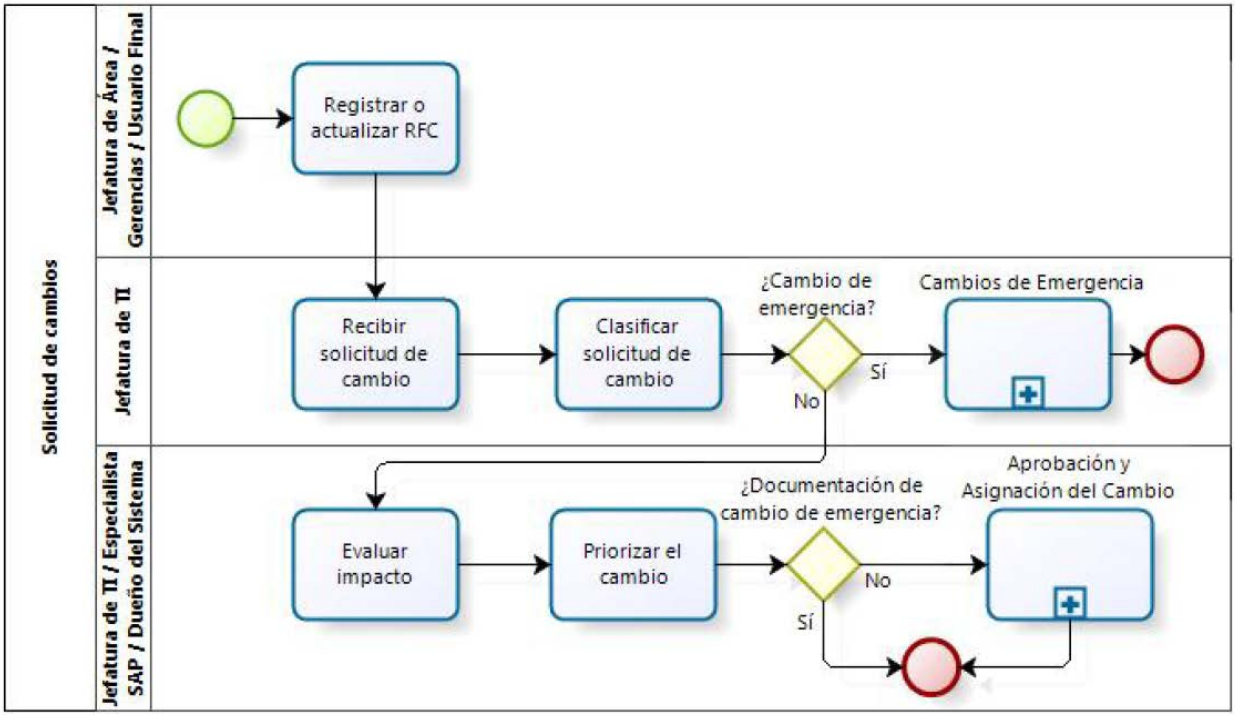
▪ Proveedor ▪ Jefatura de Informática ▪ Especialista SAP	26	Solicita al responsable de haber efectuado la petición de cambio, realizar una evaluación del cambio ejecutado.

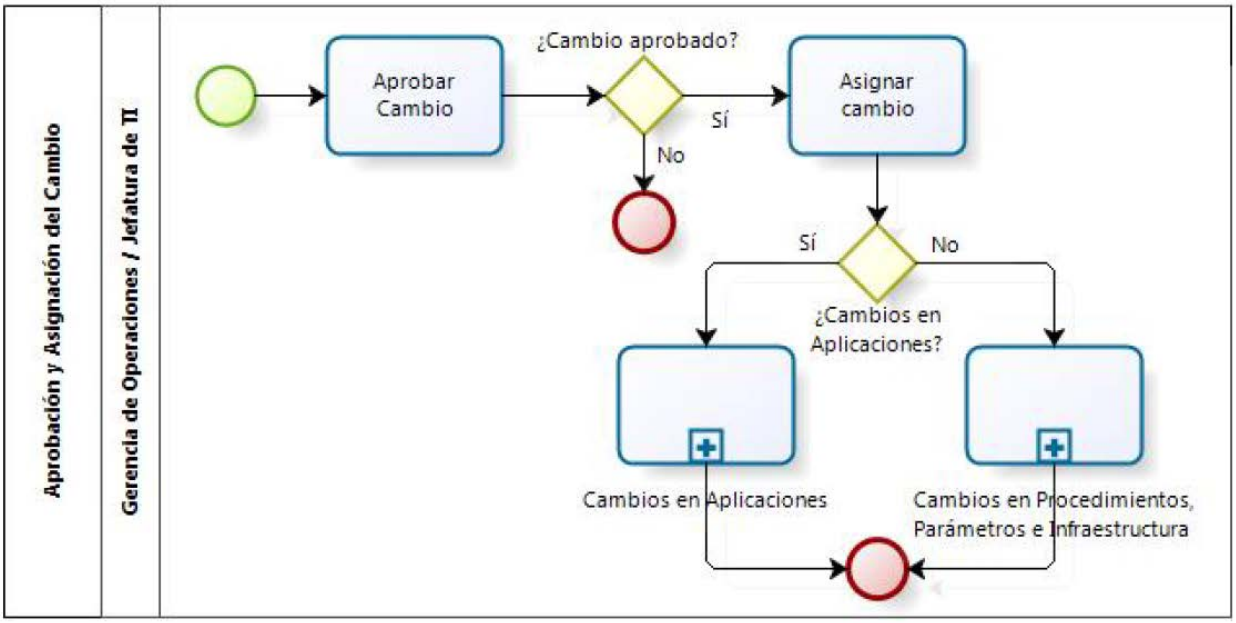
▪ Jefatura de Área ▪ Gerencias ▪ Usuario Final	27	Realiza la evaluación del cambio ejecutado para determinar si se apega a lo solicitado. En caso de no estar de acuerdo con el cambio continuar en paso 1; caso contrario, paso 28.
▪ Proveedor ▪ Jefatura de Informática ▪ Especialista SAP	28	Efectúa el cierre de la solicitud de cambio, y analiza si el cambio realizado amerita actualizar la configuración relacionada, en caso de necesitar cambiar la configuración continuar en Procedimiento de administración de la configuración; caso

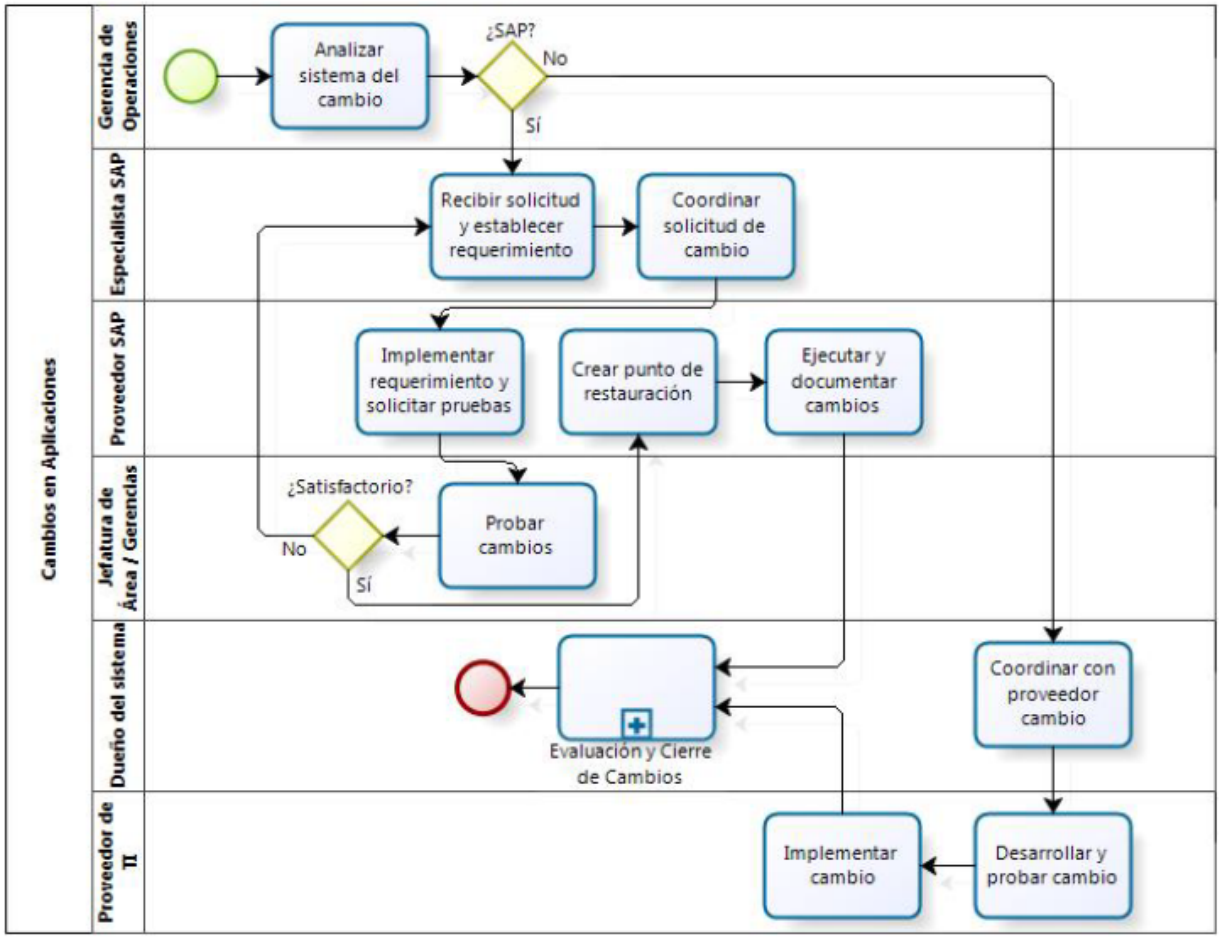
		contrario, Fin del Procedimiento.

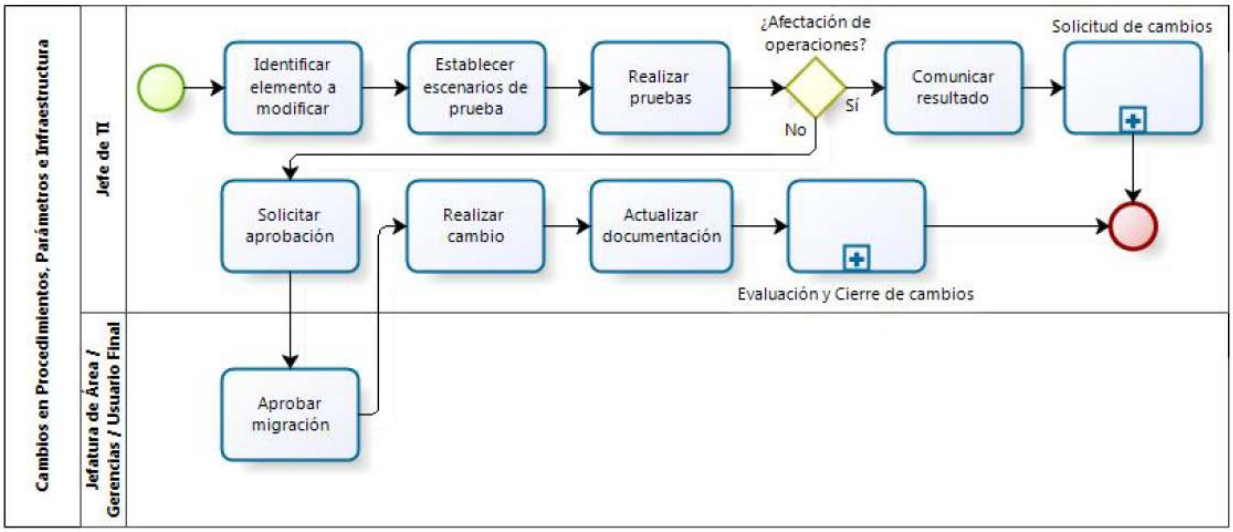
- **Cambios de emergencia**

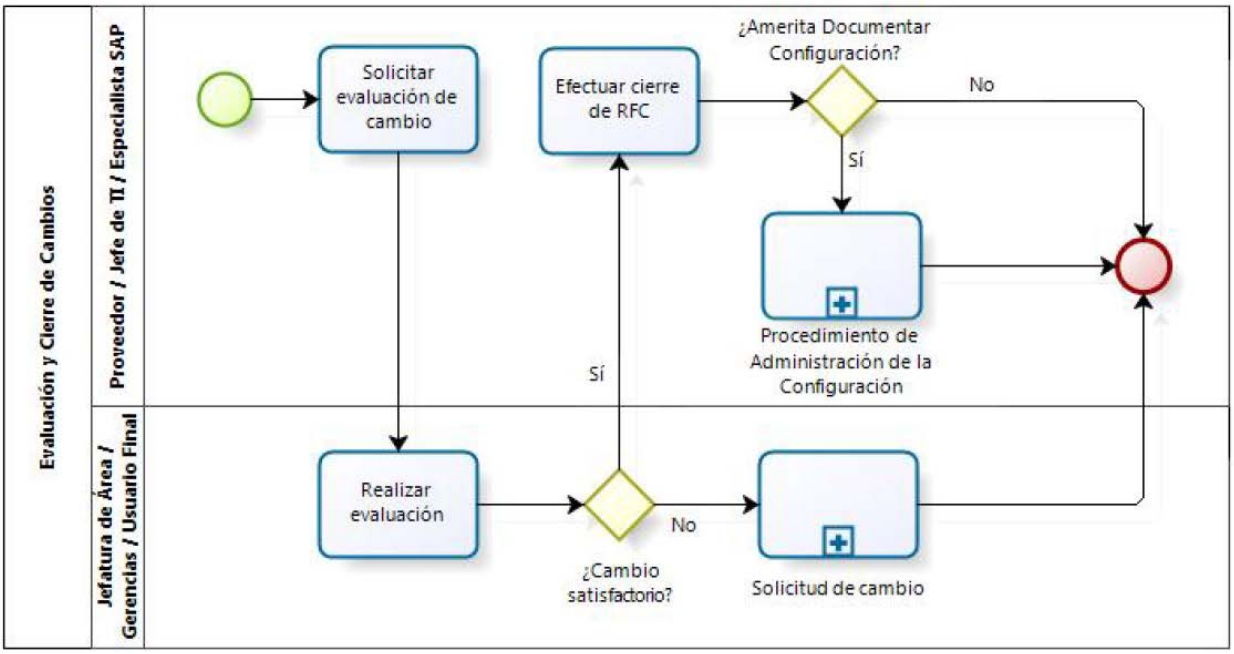
▪ Jefatura de Informática ▪ Proveedor	29	Identifica el cambio que se debe realizar, según lo especificado en la solicitud.
	30	Realiza el cambio y lo ejecuta en el ambiente de producción
	31	Documenta el cambio efectuado y solicita la aprobación formal. Continúa en paso 3.

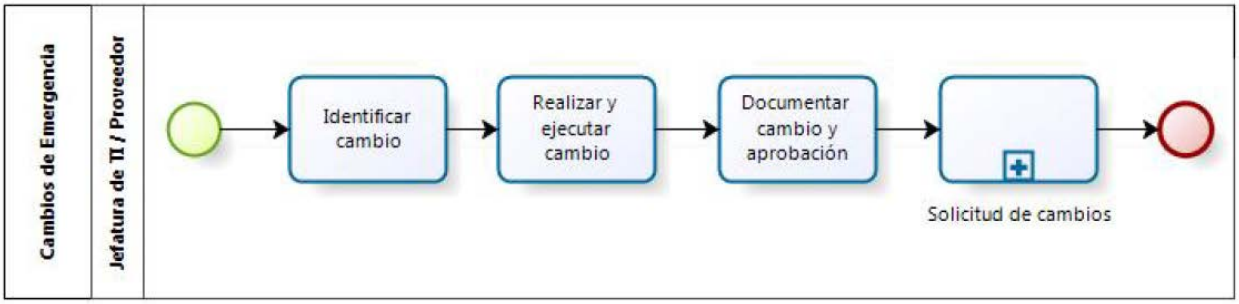



Aprobación y Asignación del Cambio
Gerencia de Operaciones / Jefatura de TI
Aprobar Cambio
¿Cambio aprobado?
Sí
No
Asignar cambio
Sí
No
¿Cambios en Aplicaciones?
Cambios en Aplicaciones
Cambios en Procedimientos, Parámetros e Infraestructura


Cambios en Aplicaciones
Gerencia de Operaciones
Especialista SAP
Proveedor SAP
Jefatura de Área / Gerencias
Dueño del sistema
Proveedor de TI
Analizar sistema del cambio
¿SAP?
No
Sí
Recibir solicitud y establecer requerimiento
Coordinar solicitud de cambio
Implementar requerimiento y solicitar pruebas
Crear punto de restauración
Ejecutar y documentar cambios
¿Satisfactorio?
No
Sí
Probar cambios
Evaluación y Cierre de Cambios
Coordinar con proveedor cambio
Implementar cambio
Desarrollar y probar cambio


Cambios en Procedimientos, Parámetros e Infraestructura
Jefe de TI
Identificar elemento a modificar
Establecer escenarios de prueba
Realizar pruebas
¿Afectación de operaciones?
Sí
No
Comunicar resultado
Solicitud de cambios
Solicitar aprobación
Realizar cambio
Actualizar documentación
Evaluación y Cierre de cambios
Jefatura de Área / Gerencias / Usuario Final
Aprobar migración


Evaluación y Cierre de Cambios
Proveedor / Jefe de TI / Especialista SAP
Solicitar evaluación de cambio
Efectuar cierre de RFC
¿Amerita Documentar Configuración?
No
Sí
Procedimiento de Administración de la Configuración
Sí
Jefatura de Área / Gerencias / Usuario Final
Realizar evaluación
¿Cambio satisfactorio?
No
Solicitud de cambio


Cambios de Emergencia
Jefatura de TI / Proveedor
Identificar cambio
Realizar y ejecutar cambio
Documentar cambio y aprobación
Solicitud de cambios

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
	1.0		Elaboración del primer documento

1. OBJETIVO

Establecer un procedimiento formal para administración de respaldos de Financiera Desyfin.

2. ALCANCE

Se consideran en este procedimiento los respaldos que se ejecutan para las siguientes plataformas tecnológicas:

- Servidor de dominio.
- Servidor de bases de datos.
- Servidor de archivos y otros componentes.
- Servidor de aplicaciones.
- Servidor de desarrollo.

3. GENERALIDADES

- Los respaldos deben ser resguardados por mínimo cinco años.
- La información respaldada debe estar encriptada, en la medida que la tecnología lo permita.
- El custodio es responsable de verificar periódicamente que los respaldos están almacenados en la empresa de custodia acorde a lo establecido en el contrato.

4. REFERENCIAS

- Política de administración de datos

5. Procedimiento de administración de datos

- **Gestión de respaldos**

Puesto	Número Actividad	Procedimiento
• Asistente de Informática	1	Realiza la configuración de los sistemas y los equipos para la ejecución periódica de respaldos para sistemas, datos y configuraciones. Según la estrategia de respaldos definida con la Jefatura de Informática.
	2	Verifica que la ejecución de los respaldos se haya dado correctamente, en caso de realizarse incorrectamente continuar en paso 3; si no, en paso 4.
	3	Realiza el respaldo manualmente. Identifica si es necesario registrar un incidente por la no ejecución automática del respaldo. Continuar en paso 2.
	4	Almacena el respaldo en el repositorio dedicado para dicho fin.
	5	Documenta el resultado del respaldo en la bitácora de control de respaldos. Fin del Procedimiento

- **Solicitud de restauración de datos**

▪ Usuario final	6	Identifica la necesidad de realizar la restauración de datos para el área de negocio específica.
	7	Registra en SysAid una solicitud de restauración de respaldo, indicando las razones por las cuales es necesario.
▪ Jefatura de Informática	8	Valida las solicitudes de restauración que tengan impacto en la operativa de sistemas de información.
▪ Asistente de Informática	9	Realiza la restauración de los datos solicitados.
▪ Asistente de Informática	10	Verifica que la restauración de datos se haya ejecutado correctamente. Si se ejecutó correctamente continuar en paso 11; si no, en paso 9.
	11	Comunica al usuario la ejecución exitosa de la restauración de los datos. Fin del Procedimiento

- **Restauración de datos periódica**

• Asistente de Informática	12	Realiza periódicamente restauraciones de datos de los respaldos generados para verificar que estén disponibles, funcionales, íntegros y seguros, soportando una eventual contingencia de negocio. En caso de que los respaldos no se puedan restaurar adecuadamente continuar en paso 13; si

		no, en paso 15.
	13	Registra en SysAid el problema con la restauración del respaldo
• Jefatura de Informática	14	Tomar las medidas necesarias como acciones correctivas o preventivas para evitar la ausencia de datos para el periodo del respaldo que se generó de manera incorrecta.
• Asistente de Informática	15	Documentar la ejecución de la restauración de datos, indicando el estatus de la misma, si fue correcta o incorrecta. Fin del Procedimiento

- **Eliminación de datos**

• Asistente de Informática	16	Identifica la necesidad de cambio de un equipo por obsolescencia o devolución en vencimiento de contrato de *Leasing*
	17	Retira el equipo que va a ser cambiado o devuelto.
	18	Respalda los datos de importancia presentes en el equipo del usuario final.
	19	Ejecuta eliminación segura de datos en todos los discos duros del equipo utilizando la herramienta *Kill Disk* o similar
	20	Entrega el equipo para ser devuelto en *leasing*, eliminado o donado. Fin del Procedimiento

- **Almacenamiento de respaldos en sitio sucursal o sitio externo.**

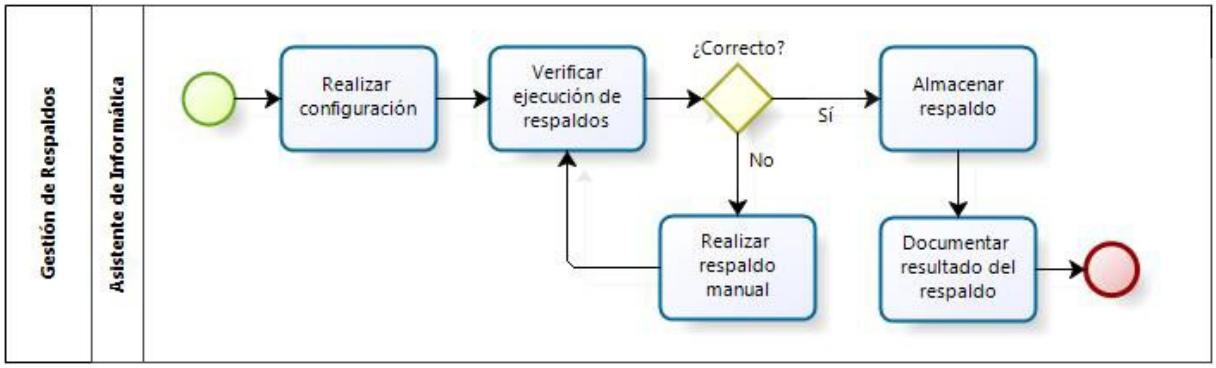
▪ Asistente de Informática	21	Identifica junto con la Jefatura de Informática los contenedores de respaldos que por seguridad y continuidad del negocio deben ser almacenados fuera de las oficinas centrales.
	22	Coordina con la Gerencia de sucursal destino, o sitio externo, el envío de los respaldos
	23	Adjunta los respaldos sellados en un sobre de seguridad o tula, y lo entrega al mensajero para ser enviado, junto con un formulario con la firma del emisor, la fecha, hora de envío, el mensajero a cargo del envío y características del respaldo (fecha, código, etiquetas, etc.)
▪ Mensajero	24	Traslada el respaldo hacia la sucursal o sitio externo destino, y firma el formulario de envío una vez entregado.
▪ Gerencia de sucursal o sitio externo	25	Recibe el sobre de seguridad o tula con el respaldo, y verifica que no haya sido forzado, así como que coincida con las características indicadas en el formulario. En caso de parecer forzado, o que las características no coincidan continuar en paso 26; si no, en paso 27.
	26	No recibe el respaldo y comunica la situación al emisor, para que se tomen las medidas respectivas. Fin

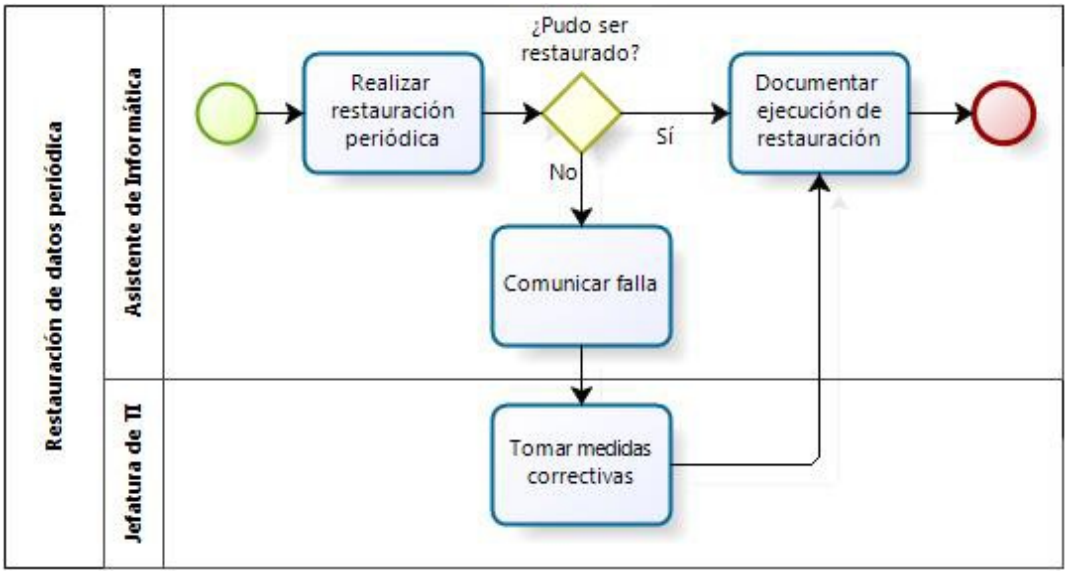
		del Procedimiento
	27	Firma el formulario, e indica la fecha y hora de recepción del mismo
	28	Almacena el respaldo en la bóveda de la sucursal o en el sitio externo designado para tal fin. Fin del Procedimiento
	29	Devuelve el formulario de envío de respaldos al emisor, para ser almacenado en un repositorio central.

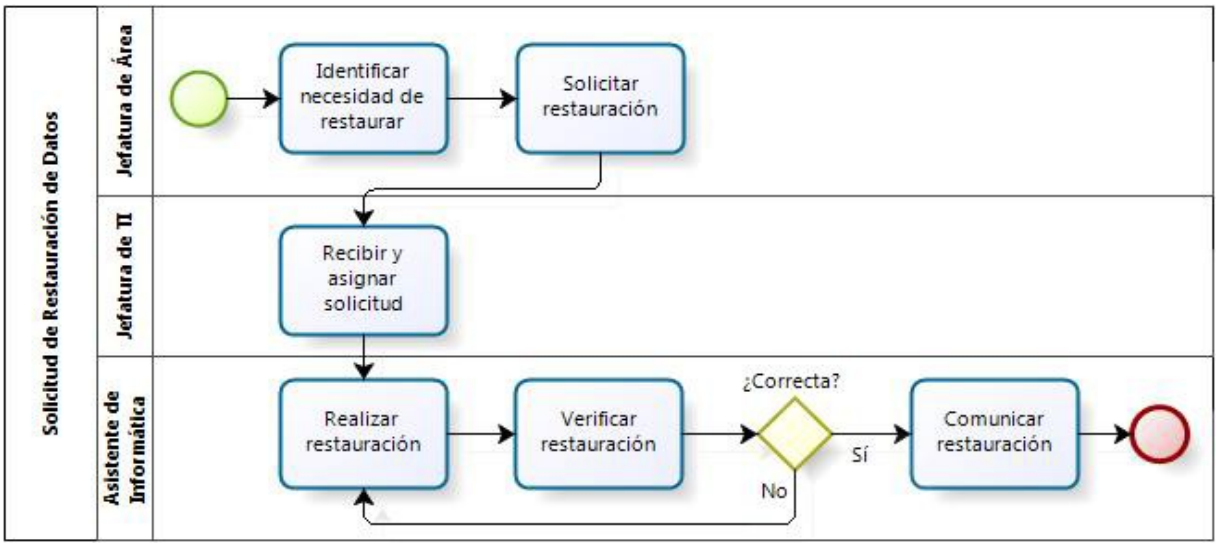
- **Solicitud de respaldos en sitio sucursal o sitio externo.**

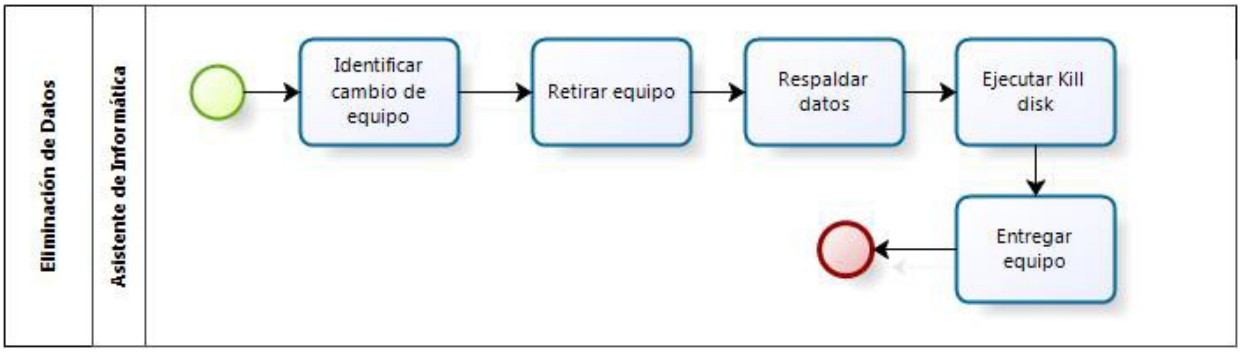
▪ Jefatura de Informática	30	Solicita mediante correo electrónico a la Gerencia de la sucursal o sitio externo, el envío del respaldo, indicando la fecha y características del mismo.
▪ Gerencia de sucursal o sitio externo	31	Recibe la solicitud de envío de respaldo.
	32	Procede a sacar el respaldo de la bóveda o sitio externo designado y lo adjunta en un sobre de seguridad o tula, con el formulario de envío de respaldos firmado, la fecha, hora del envío, el mensajero a cargo del envío y características del respaldo (fecha, código, etiquetas, etc.).
▪ Mensajero	33	Traslada el respaldo de la sucursal o sitio externo, a las oficinas centrales, y firma el formulario de envío de respaldos.
▪ Jefatura de Informática	34	Recibe el sobre de seguridad o tula con el respaldo, y verifica que no haya sido forzado, así como que coincida con las características indicadas en el formulario.

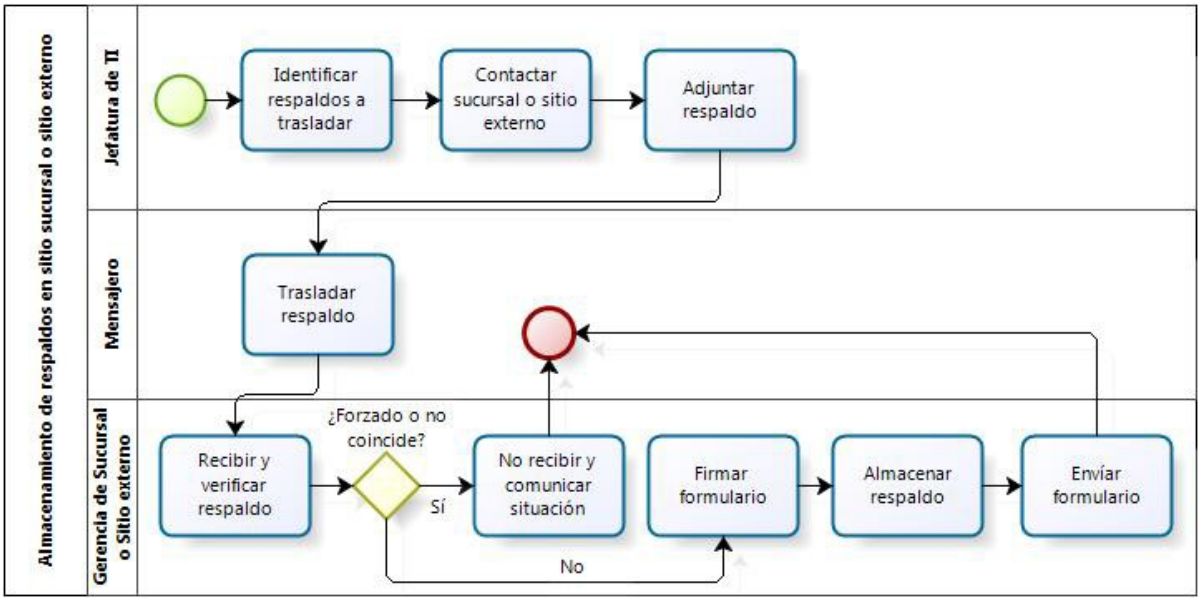
		En caso de parecer forzado, o que las características no coincidan continuar en paso 35; si no, en paso 36.
	35	Tomas las medidas respectivas, para asegurar la protección del respaldo, y de ser necesario comunica a la administración para que se tomen las medidas disciplinarias necesarias
	36	Firma el formulario, e indica la fecha y hora de recepción del mismo.
	37	Resguarda el formulario en un repositorio central, y almacena el respaldo. Fin del Procedimiento

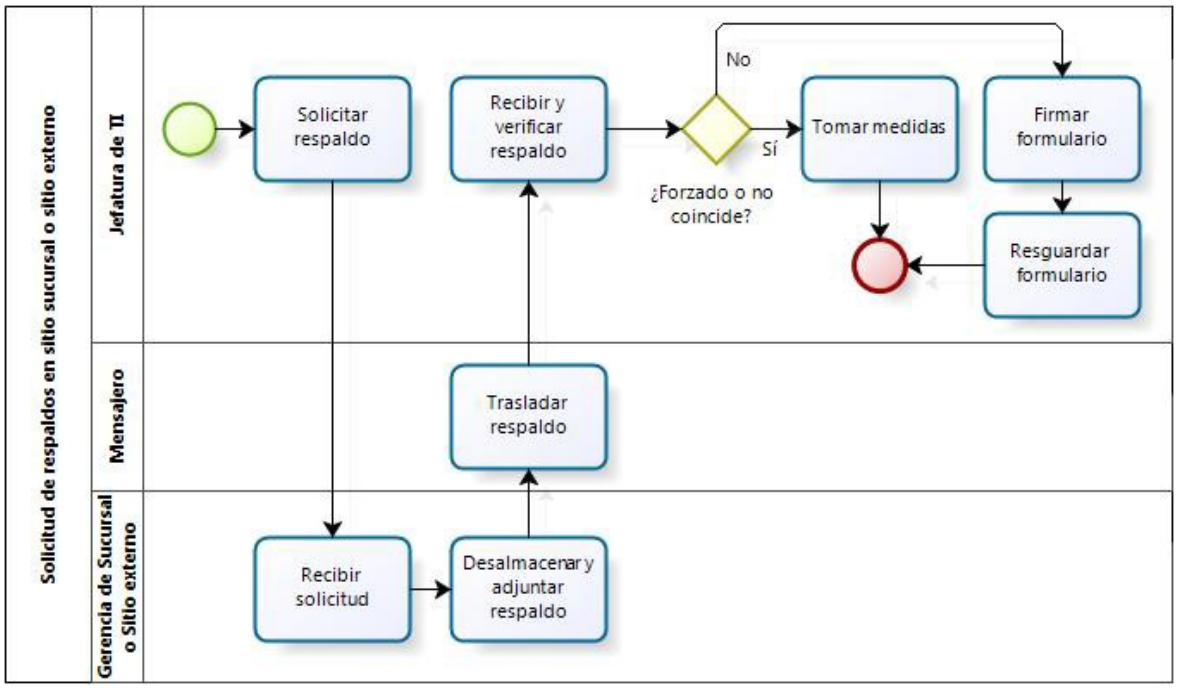


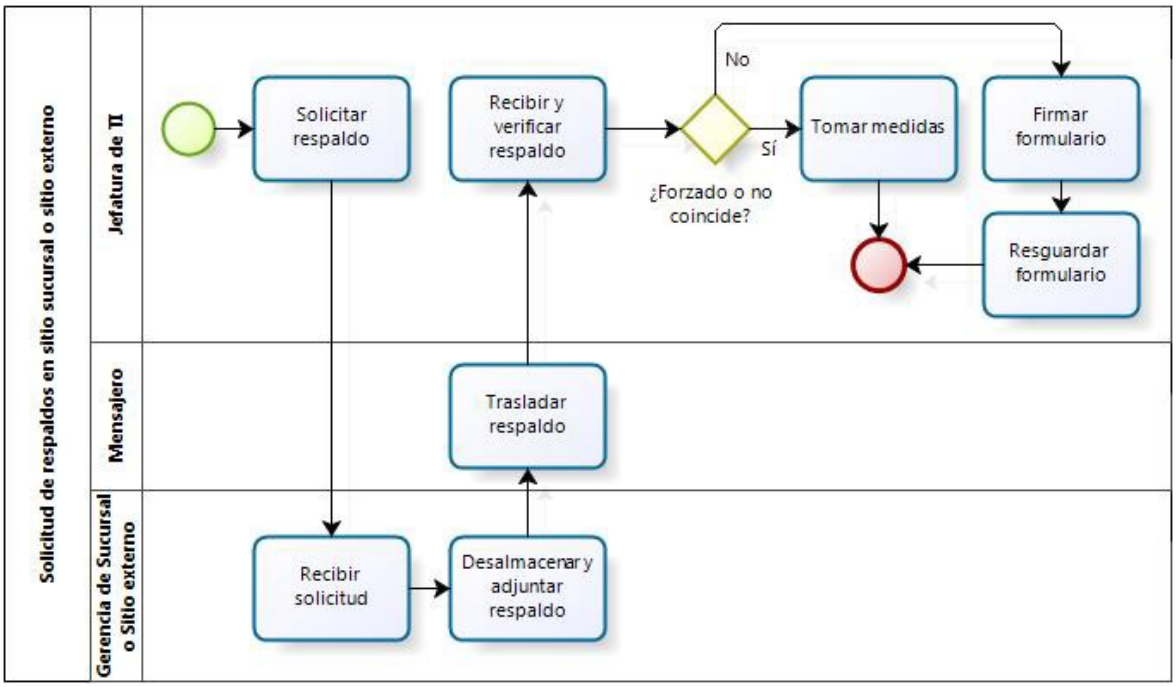

Restauración de datos periódica
Asistente de Informática
Jefatura de TI
Realizar restauración periódica
¿Pudo ser restaurado?
Sí
No
Documentar ejecución de restauración
Comunicar falla
Tomar medidas correctivas


Solicitud de Restauración de Datos
Jefatura de Área
Jefatura de TI
Asistente de Informática
Identificar necesidad de restaurar
Solicitar restauración
Recibir y asignar solicitud
Realizar restauración
Verificar restauración
¿Correcta?
Sí
No
Comunicar restauración


Eliminación de Datos
Asistente de Informática
Identificar cambio de equipo
Retirar equipo
Respaldar datos
Ejecutar Kill disk
Entregar equipo


Almacenamiento de respaldos en sitio sucursal o sitio externo
Jefatura de TI
Identificar respaldos a trasladar
Contactar sucursal o sitio externo
Adjuntar respaldo
Mensajero
Trasladar respaldo
Gerencia de Sucursal o Sitio externo
Recibir y verificar respaldo
¿Forzado o no coincide?
Sí
No recibir y comunicar situación
Firmar formulario
Almacenar respaldo
Envíar formulario
No


Solicitud de respaldos en sitio sucursal o sitio externo
Jefatura de TI
Solicitar respaldo
Recibir y verificar respaldo
No
Sí
¿Forzado o no coincide?
Tomar medidas
Firmar formulario
Resguardar formulario
Mensajero
Trasladar respaldo
Gerencia de Sucursal o Sitio externo
Recibir solicitud
Desalmacenar y adjuntar respaldo


Solicitud de respaldos en sitio sucursal o sitio externo
Jefatura de TI
Mensajero
Gerencia de Sucursal o Sitio externo
Solicitar respaldo
Recibir y verificar respaldo
No
Sí
¿Forzado o no coincide?
Tomar medidas
Firmar formulario
Resguardar formulario
Trasladar respaldo
Recibir solicitud
Desalmacenar y adjuntar respaldo

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
Mes, xxx	1.0		Elaboración del primer documento

1. OBJETIVO

Establecer un marco de trabajo con el cual se cumplan las directrices generales establecidas en el documento **Política Gestión de Activos de TI.**

2. DESCRIPCIÓN

2.1. Estructura del documento:

- Identificar y registrar los activos de TI (2.2)
- Revisiones de activos de TI (Equipos e Infraestructura) (2.3)
- Gestionar activos críticos (2.4)
- Mantenimiento preventivo de activos (2.5)
- Gestionar el ciclo de vida de los activos (2.6)
- Administrar licencias (2.7)

2.2. Identificar y registrar los activos de TI

2.2.1. El Departamento de Informática deberá establecer el responsable de mantener un registro actualizado de los activos, con el objetivo de garantizar un adecuado control. Ese control se deberá realizar para los equipos tecnológicos (físicos y virtuales) mediante el formato **F09 inventario de equipos**; adicionalmente, para las licencias de *software* el registro se deberá llevar en el formato **F10 Inventario de Software**.

2.2.2. Para cada activo identificado en el punto anterior se deberá identificar requisitos legales, reglamentarios o contractuales los cuales deben documentarse en el formato **F08 Requerimientos Asociados a los Activos.**

2.2.3. Adicionalmente, por medio de los formatos **F09 Inventario de Equipo**, se deberá dejar evidencia suficiente para determinar que el activo sigue siendo adecuado para su objetivo, es decir, si están en condiciones útiles, el periodo de vida del activo, si no se encuentran en obsolescencia o cualquier otro factor que permita demostrar que el activo sigue dando valor a la Financiera.

2.2.4. El responsable del registro deberá considerar los aspectos siguientes:

a. Los activos cuyo costo sea inferior a los $200 dólares americanos o su equivalente en otra moneda, no deberán ser registrados, por ejemplo: componentes de computadoras como dispositivos periféricos, tarjetas de video, teclados, entre otros; no obstante, activos tecnológicos que sean utilizados para el resguardo de datos, deberán ser rastreados sin importar su costo.

b. Para los activos físicos con costo mayor a los 200 dólares y que no sean componentes internos de servidores o computadoras, deberán tener una placa o etiqueta que permita identificar que el activo pertenece a la Financiera.

2.2.5. El Departamento de Informática será el responsable de actualizar periódicamente el registro de activos cada vez que se realice una compra, se retire de funcionamiento un activo o cuando sucedan cambios en el contrato de mantenimiento o alquiler de equipo en los casos que correspondan.

2.3. Revisiones de activos de TI (Equipos e Infraestructura)

2.3.1. Al menos una vez al año el Departamento de Contabilidad deberá realizar una verificación de los activos. La revisión deberá quedar documentada en el formato **F07 Bitácora de Revisión**.

2.3.2. En esa revisión se deberá verificar al menos los aspectos siguientes:

a. Verificar que los activos registrados en el **F09 inventario de equipos** se encuentren activos y en funcionamiento dentro de la Financiera.

b. Validar la no existencia de activos en uso que aún no han sido registrados en el formulario **F09 inventario de equipos**.

c. Verificar que los activos están siendo contabilizados.

Esta verificación podrá ser realizada mediante muestra y no considerar el total de activos; no obstante, en cada revisión se deberán considerar activos diferentes.

2.3.3. Cualquier situación identificada deberá ser comunicada a la Jefatura del Departamento de Informática y al Comité de TI con el fin de que se consideren las acciones necesarias que permitan solventar la situación.

2.4. Gestionar activos críticos

2.4.1. Será responsabilidad del encargado establecido en el apartado 2.2 de este documento la identificación de los activos, para ello deberá dejar evidencia en el formulario **F09 inventario de equipos** y **F10 Inventario de *Software***.

2.4.2. En caso de que los activos críticos tengan asociados contratos, se deberá seguir los lineamientos establecidos en el documento **P03 Procedimiento Gestión de Operaciones**, específicamente en el apartado “Servicios externalizados”.

2.4.3. Para los activos críticos el Departamento de Informática realizará un monitoreo de su rendimiento en tiempo real.

2.4.4. Al menos de manera semestral el Departamento de Informática deberá realizar las verificaciones siguientes:

a. Un análisis de tendencias de incidentes asociados a los activos críticos.

b. Considerar el riesgo de fallo total del activo y la necesidad de reemplazarlo.

c. Identificar si el activo tiene controles de redundancia implementados que permitan reducir el riesgo de fallo.

d. Determinar la periodicidad con la cual se le da mantenimiento preventivo al equipo.

e. Análisis del rendimiento del equipo y un estimado de la vida útil restante del equipo.

f. Análisis de costo del equipo el cual podrá considerar si el activo ha estado fallando, si está sobre utilizado o infrautilizado, el costo de darle mantenimiento, entre otros factores que considere necesarios.

g. Análisis de garantías documentadas en el documento **F08 Requerimientos Asociados a los Activos**.

Esta verificación podrá ser realizada mediante muestra y no considerar el total de activos; no obstante, en cada revisión se deberán considerar activos diferentes.

2.4.5. Esa revisión deberá quedar documentada en el formato **F07 Bitácora de Revisión**.

2.4.6. En caso de que se identifiquen situaciones a ser reportadas, se deberá de comunicar a la Jefatura del Departamento de Informática y al Comité de TI en conjunto con una recomendación de reparar o reemplazar el activo.

2.5. Mantenimiento preventivo de activos

2.5.1. Con el fin de mitigar los riesgos asociados a fallos en los activos y mantener la resiliencia de los mismos, el Departamento de Informática deberá establecer, de manera semestral y por medio del formulario **F11 Cronograma de Mantenimiento** un cronograma de mantenimiento preventivo, al menos para los activos críticos de infraestructura.

2.5.2. Ese cronograma deberá considerar la ejecución del mismo en periodos en los cuales el impacto a los servicios sea el menor, por ejemplo, evitar realizar mantenimientos cerca o durante un cierre de mes o evitar realizar cambios a sistemas durante fechas de envíos.

2.5.3. En caso de que no se cuente con el personal capacitado para realizar este tipo de mantenimientos, el Departamento de Informática deberá establecer contratos de mantenimientos con terceros, los cuales deberán ejecutarse según los lineamientos establecidos en el documento **P01 Procedimiento de Gestión de Proveedores.**

2.5.4. En caso de que se requiera la contratación de servicios de mantenimiento por medio de un tercero, será responsabilidad del Departamento de Informática en conjunto con el Comité de TI establecer los controles de seguridad y privacidad que consideren necesarios, así como también establecer un responsable de validar que los mismos se están cumpliendo a cabalidad.

2.5.5. Para determinar a cuáles equipos se les deberá dar mantenimiento se deberá considerar al menos, alguno de los aspectos siguientes:

a. Un análisis costo beneficio
b. Recomendaciones del proveedor o fabricante del activo
c. El riesgo asociado al fallo del activo
d. Cualquier otro factor que el Comité de TI o el Departamento de Informática considere necesario

2.5.6. Para los mantenimientos en los cuales no hay afectación a clientes externos, el Departamento de Informática con ayuda del Departamento de Recursos

humanos, deberán notificar por medio de un correo electrónico a los colaboradores el periodo y los sistemas que se verán afectados durante el mantenimiento.

2.5.7. Para los mantenimientos en los cuales hay afectación directa a los clientes de la Financiera, el Departamento de Informática con ayuda del Departamento de Negocio, deberán notificar por medio de un correo electrónico a los clientes el periodo y los servicios que se verán afectados durante el mantenimiento.

2.6. Gestionar el ciclo de vida de los activos

2.6.1. ***Adquisición de activos***

2.6.1.1. Cualquier activo de TI, deberá cumplir lo establecido en el apartado 2.2 de este documento; adicionalmente, y en caso donde los activos cuesten más de $200 dólares americanos o su equivalente en otra moneda, donde el Departamento de Informática o Comité de TI lo considere necesario deberá ser probado antes de ser aceptado.

2.6.1.2. Toda compra de activo deberá ser registrada y tramitada por medio de la herramienta de soporte técnico; adicionalmente, las compras de activos superiores de $1.000,00 dólares americanos o su equivalente en otra moneda, deberá ser aprobada por el gerente de operaciones.

2.6.2. ***Otorgar Activos de TI***

2.6.2.1. Cuando un activo de TI deba ser asignado a un colaborador, se deberá completar el formulario **F12 Boleta de Activo**, exceptuando, el préstamo temporal de equipo (laptops, proyector, entre otros) el cual se deberá registrar en una bitácora diferente.

2.6.2.2. Será responsabilidad del Departamento de Informática llenar el formulario mencionado anteriormente y enviarlo por correo electrónico al colaborador que se le asignará el activo, el cual será el responsable de los activos indicados en la boleta.

2.6.2.3. En caso de que el activo no vaya a ser asignado a un colaborador en específico, la boleta deberá ser enviada a la jefatura de los colaboradores que utilizarán el activo. En este caso la jefatura será responsable del activo.

2.6.2.4. Cuando un colaborador se traslada de ubicación y se le asigna otros activos, el colaborador deberá llenar el formulario y entregarlo al Departamento de Informática.

2.6.2.5. En caso de despido o renuncia del personal, será responsabilidad de la jefatura llenar la boleta y enviarla al Departamento de Informática.

2.6.3. ***Retiro de activos de TI***

2.6.3.1. Cuando un activo o grupo de activos deban ser retirados del uso de la Financiera, deberá llenarse el formulario **F13 Retiro de Activos**, por medio del cual se dejará evidencia de los activos que han sido desechados por la Financiera y que los mismos fueron retirados de manera segura, considerando al menos, que toda información ha sido borrada permanentemente y que han sido desechados donde no ocasionen un daño ambiental.

2.7. Administrar licencias

2.7.1. Al menos una vez al año el Departamento de Informática deberá realizar una verificación de los activos, con el fin de obtener un mejor valor en los productos y licencias, el responsable de esta revisión no podrá ser el mismo que lleve el control del registro. La revisión deberá quedar documentada en el formato **F07 Bitácora de Revisión**.

2.7.2. En esa revisión se deberá verificar al menos los aspectos siguientes:

a. Verificar la cantidad de licencias de *software* que se encuentran registradas en el documento **F10 inventario de *software*** contra el total de licencias instaladas

b. Comparar el número de licencias instaladas contra la cantidad de licencias en propiedad

Esta verificación podrá ser realizada mediante una muestra y no considerar el total de activos; no obstante, en cada revisión se deberán considerar activos diferentes.

2.7.3. Cualquier situación identificada deberá ser comunicada a la jefatura del Departamento de Informática y al Comité de TI, con el fin de que se consideren las acciones necesarias que permitan solventar la situación entre las cuales pueden estar las siguientes:

a. Cuando las copias instaladas son inferiores al número en propiedad, se debe determinar si existe una necesidad de mantener o cancelar licencias

b. Cuando las copias instaladas son superiores al número en propiedad, se deberá considerar primero la posibilidad de desinstalar copias que ya no sean necesarias o justificadas o analizar la necesidad de adquirir licencias adicionales.

3. Definiciones

Activos críticos: Se considerará como activos críticos aquellos recursos, infraestructura y sistemas que son esenciales e imprescindibles para mantener y desarrollar las funciones de la Financiera.

4. Matriz RACI

Proceso	Matriz RACI									Periodicidad
	Personas									
	Asistente Informática	Jefe Informática	Gerente de Operaciones	Depart. Contabilidad	Comité de TI	Depart. Negocios	Depart. RRHH	Clientes	Otros Depart.	
Mantener un registro actual de activos	R	A			I					Compra, Retiro, Cambios contractuales
Revisión de activos		I		A / R	I					Anualmente
Verificar y monitorear los activos críticos	R	A			I					Semestralmente
Dar mantenimiento preventivo a activos	R	A			R	R	R	I	I	Semestralmente
Otorgar activos de TI	R	A							I	Entrega de equipos a
Adquisición de activos	R	A	C		C					Antes de compra de activos
Retiro de activos	R	A								Al retirarse un activo
Administrar licencias	R	A			I					Anualmente

F08 Requerimientos Asociados a los Activos

FINANCIERA DESYFIN S.A
Código: GOP-INF-FOR-XXX
Requerimientos Asociados a los Activos

Versión: 1.0
Fecha de Emisión: Mes 2020
Fecha Revisión: Mes 2020
Código Iterno: F08

Id Activo	Tipo	Observaciones / Comentarios

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
Mes 2020	1.0		Elaboración del primer documento

Aprobado por:

F09 Inventario de equipos

FINANCIERA DESYFIN S.A
Código: GOP INF FOR XXX
Inventario de Equipos

Versión: 1.0
Fecha de Emisión: Mes 2020
Fecha Revisión: Mes 2020
Código Iterno: F09

Id Equipo	Descripción	Modalidad de Configuración	Marca	Modelo	Fecha Adquirido	Tipo de Equipo	Sistemas Operativos	Ambiente	Id Proveedor

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
Mes xxx	1.0		Elaboración del primer documento

Aprobado por: Jefe de Informática

F10 Inventario de Software

FINANCIERA DESYFIN S.A
Código: GOP-INF-FOR-XXXX
Inventario de Software

Versión: 1.0
Fecha de Emisión: Mes xxx
Fecha Revisión: Mes xxx
Código Interno: F10

Id Software	Nombre	Descripción	Versión	Fecha Implementación	Id Proveedor	Tipo Código Fuente	¿Se encuentra integrado?	¿Es Crítico?	Cantidad Licencias	Tipo Licencias	Observaciones

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
Mes xxx	1.0		Elaboración del primer documento

Aprobado por:

F11 Cronograma de mantenimiento

FINANCIERA DESYFIN S.A
Código: GOP-INF-FOR-XXXX
Cronograma Mantenimiento

Versión: 1.0
Fecha de Emisión: Mes 2020
Fecha Revisión: Mes 2020
Código Interno: F11

Fecha de Inicio:	
Fecha Fin:	

Periodo Fechas	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5
	Nombre de Equipo	Nombre de Equipo	Nombre de Equipo	Nombre de Equipo	Nombre de Equipo
Lunes					
Martes					
Miercoles					
Jueves					
Viernes					

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
Mes xxx	1.0		Elaboración del primer documento

Aprobado por:

Boleta de Activo F12

Descripción Activo	Fecha efectiva de traslado	Marca	Serie #	Placa #	Observaciones	Funcionario de entrega	Departamento	Funcionario que recibe	Departamento

FIRMA DE ENTREGA _____

FIRMA DE RECIBO _____

FECHA _____

F13 Retiro de Activos

Fecha de Inicio:
Fecha Fin:

FINANCIERA DESYFIN S.A
Código: GOP-INF-FOR-XXXX
Retiro de Activo

Versión: 1.0
Fecha de Emisión: Mes 2020
Fecha Revisión: Mes 2020
Código Interno: F11

ID Equipo	Descripción	¿Se eliminó información? SÍ/NO/NA	¿Se trasladó información? SÍ/NO/NA	Acción realizada	Responsable de desecho	Firma del responsable	Observaciones

Control de Versiones

Fecha	Versión	Actualizado por	Información de los Cambios Realizados
Mes xxx	1.0		Elaboración del primer documento

Aprobado por:

REFERENCIAS

Miranda, L. (2016). Análisis de productos y servicios de financiación: ADGN0108.Andalucía, España: IC Editorial.

PARA, C., & EMPRESARIOS, E. Y. (2017). Gestión financiera.

Definición de Información. *Revista Sistemas*. Recuperado de: https://sistemas.com/informacion.php

Urbina, G. B. (2016). *Introducción a la seguridad informática*. Grupo editorial PATRIA.

Chilán-Santana, E. I., & Pionce-Pico, W. F. (2017). Apuntes teóricos introductorios sobre la seguridad de la información. *Dominio de las Ciencias*, *3*(4), 284-295.

Izaguirre, R. D. L. F., & Barajas&, J. M. C. Device lock, una alternativa a la seguridad informática en el órgano de fiscalización. Superior periodo 2013-2015. 10 Temas de Ciberseguridad, 15.

Sain, G. (2018). ¿Qué es la seguridad informática?. *Pensamiento Penal*, 5.

Tapia, C., Guevara, E., Castillo, S., Rojas, M., & Salomon, L. (2016). *Fundamentos de Auditoria. Aplicación práctica de las Normas Internacionales de Auditoría*. México: Instituto Mexicano de Contadores Públicos

Urbina, G. B. (2016). *Introducción a la seguridad informática.* Grupo editorial PATRIA.

ISO Tools Norma ISO 27001 Como garantizar la seguridad de la información. Recuperado de: https://www.isotools.org/2017/07/27/norma-iso-27001-garantizar-la-seguridad-la-informacion/

Binwal, P. (2015, 29 de junio). Creating a Cybersecurity Governance Framework: The Necessity of Time. *Security Intelligence*

Macen R. (2014) Políticas de Seguridad de la Información.

Maldonado, G. B., & Cano, J. A. O. (2014). Metodología de la seguridad de la información como medida de protección en pequeñas empresas. *Cuaderno Activa*, 6, 71-77.

Arévalo, F. M., Cedillo, I. P., & Moscoso, S. A. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos Agile Methodology for Computer Risk Management. Revista Killkana Técnica. Vol, 1(2).

http://www.criptored.upm.es/descarga/gob_segu_y_gob_corp.pdf

Campos Ocampo, M. (2017). Métodos y técnicas de investigación académica.

Rodríguez Peñuelas, M. A. (2010). *Métodos de investigación*. México: Editorial Universidad Autónoma de Sinaloa.

García, M. A. C. (2019). Fuentes de información. *Boletín Científico de las Ciencias Económico Administrativas del ICEA*, *8*(15), 57-58.

Evertson, C., & Merlin, G. (2008). La observación como indagación y método. *Métodos cuantitativos aplicados*, 2, 174-188.

Herrera, C. D. (2018). Investigación cualitativa y análisis de contenido temático. Orientación intelectual de Revista Universum. Revista general de información y documentación, 28(1), 119.

Prieto, A., Lloris, A., & Torres, J. C. (1989). Introducción a la Informática (Vol. 20). McGraw-Hill.

Torres, M., Salazar, F. G., & Paz, K. (2019). Métodos de recolección de datos para una investigación.

Ruis, M. S., & Jorge, J. V. (2008). Fuentes de Información Primarias, Secundarias y Tercerias.

Cauas, D. (2015). Definición de las variables, enfoque y tipo de investigación. Bogotá: Biblioteca electrónica de la Universidad Nacional de Colombia, 2.

Barragán, R., Salman, T., Ayllón, V., Sanjinés, J., Langer, E. D., Córdova, J., & Rojas, R. (2003). *Guía para la formulación y ejecucción de Proyectos de Investigación.* Bolivia: Offset Boliviana Ltda.

Puente, W. (2000). Técnicas de investigación. Recuperado el, 9.

Wolinsky, J. (2003). *Manual de auditoría para la gestión de negocios*. Buenos Aires: Buyatti.

Lara, Arturo (2012). *Toma el control de tu negocio*. México: Lid Editorial. Biblioteca Avante.

APÉNDICES

Por medio de esta encuesta se maneja los principales aspectos para evaluar la seguridad de la información de la Financiera Desyfin y los procesos utilizados para el control de dicha seguridad. La encuesta tiene como finalidad evidenciar el Trabajo Final de Graduación como parte de los requisitos para optar por el Grado de Licenciatura en Informática en la Universidad Internacional de las Américas. Agradezco su colaboración, debido a que su opinión es importante para determinar los elementos que se consideran significativos en la evaluación e implementación de la seguridad de la información, como las debilidades en seguridad que tiene la Financiera. Sus respuestas serán tratadas con entera confidencialidad.

A5. Política de Seguridad:

1. ¿La organización cuenta con un documento que recopile lineamientos para la seguridad de la información (política)?

Sí existe y la conozco
Sí existe, pero la desconozco
No existe

2. ¿Las políticas emitidas han sido comunicadas, comprendidas y aceptadas por mi persona?

No se ha realizado el proceso
Sí me las han comunicado y las mismas fueron aceptadas por mi persona
Si me las han comunicado, pero no las he aceptado

3. ¿Todas las políticas tienen un formato y estilo consistentes?

Sí
No

A6. Organización de la seguridad de la información:

1. ¿La organización cuenta con una política que cubra la segregación de funciones?

Sí existe y la conozco
Sí existe, pero la desconozco
No existe

2. ¿Conoce si en laorganización hay un responsable o área encargada de la seguridad de la información?

Sí
No

3. ¿Los roles y las responsabilidades están claramente definidos y asignados a personas acorde al puesto de trabajo?

Sí
No

4. ¿Sabes si se mantiene contacto con temas de seguridad grupos de interés especial? Ejemplo: policía, entes reguladores, entre otros

Sí
No

A8. Gestión de Activos:

1. ¿La organización cuenta con una política sobre el uso aceptable de los recursos tecnológicos, tales como correo electrónico, mensajería instantánea, carpetas compartidas, responsabilidades de los usuarios, entre otros?

Sí existe y la conozco
Sí existe, pero la desconozco
No existe

2. ¿La organización cuenta políticas o documentos formales relacionados con la clasificación de la información?

Sí existe y la conozco
Sí existe, pero la desconozco
No existe

3. ¿La organización gestiona los activos? (hardware, software, documentación, entre otros)

Sí
No

4. ¿La organización cuenta con una política o documentación formal que regulen la eliminación de los activos?

Sí existe y la conozco
Sí existe, pero la desconozco
No existe

5. ¿Se cuenta con una política o documentación formal relacionado al servicio de información enviada fuera de la organización?

Sí
No

6. ¿Se implementan controles de seguridad relacionado al envido y entrega de documentos fuera de la organización?

Sí
No

A9- Control de Acceso:

1. ¿La organización cuenta con una política o documentación formal de control de acceso?

Sí existe y la conozco
Sí existe, pero la desconozco
No existe

2. ¿Se utiliza un identificador de usuario único para cada colaborador al momento de ingreso al sistema?

Sí
No

3. ¿Se cuenta con procedimiento formal para gestionar los roles, perfiles o permisos de acceso a los sistemas de información?

Sí existe y la conozco
Sí existe, pero la desconozco
No existe

4. ¿Cuáles mecanismos de inicio de sesión se han implementado para iniciar sesion en sus computadoras y aplicaciones de trabajo?

Contraseña
Token
PIN
Biométrico

5. ¿Se deshabilitan los accesos de usuario de forma inmediata tras un despido?

Sí
No

6. Ante un incidente de seguridad informática ¿Existe un proceso formal de cambio de contraseñas?

Sí existe y la conozco
Sí existe, pero la desconozco
No existe

7. ¿Se hacen revisiones formales y periódica de los roles, perfiles o permisos de accesos de los usuarios en sistemas y aplicaciones?

Sí
No

8. ¿Se revisan los derechos de acceso para usuarios con privilegios elevados de forma más exhaustiva y frecuente?

Sí

No

9. ¿La organización cuenta con políticas y procedimientos para gestionar los privilegios de acceso del usuario a la red?

Sí existe y la conozco

Sí existe, pero la desconozco

No existe

10. ¿Se aplican medidas técnicas para garantizar la seguridad en las redes (segregación de redes, cortafuegos, entre otros)?

Sí

No

11. ¿El código fuente se almacena en una o más bibliotecas de programas fuente o repositorios?

Sí

No

12. ¿El ambiente de pruebas, desarrollo y producción de los aplicativos se encuentran separados, independientes y correctamente identificados?

Sí

No

A11- Seguridad Física y del Entorno:

1. ¿El cuarto de servidores y redes se encuentran restringido al personal respectivo acorde a su rol dentro de la organización?

Sí

No

2. ¿Cuáles mecanismos de seguridad utilizan dentro del cuarto de servidores y redes?

Tarjeta de proximidad

Biométrico
UPS
Cerraduras de seguridad
CCTV
Alarmas

3. ¿Dentro de la organización, se cuenta con mecanismos de seguridad interna?

Detector de humo
UPS
Seguridad privada
Extintores
Supresores de incendio
Alarmas
Otros:

4. ¿La organización cuenta con un procedimiento de recuperación ante desastres (Plan de Continuidad del Negocio)?

Sí existe y la conozco
Sí existe, pero la desconozco
No existe

5. ¿Los aplicativos cuentan con el cierre de sesión automático al momento de un periodo de inactividad?
Sí
No

6. ¿La organización cuenta con políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas?

Sí existe y la conozco

Sí existe, pero la desconozco

No existe

A12 - Seguridad de las Operaciones

1. ¿La organización cuenta con una política de gestión de cambios?

Sí existe y la conozco

Sí existe, pero la desconozco

No existe

2. ¿Los cambios están debidamente documentados, justificados y autorizados por la administración?

Sí se encuentran documentados, justificados y autorizados

Sí, pero no se cumple con todas las especificaciones mencionadas anteriormente.

No se encuentran documentados, justificados ni autorizados

No estoy seguro(a)

3. ¿La organización cuenta con una política sobre la instalación de software?

Sí existe y la conozco

Sí existe, pero la desconozco

No existe

4. ¿La instalación software en los sistemas está limitada personal autorizado con privilegios de sistema adecuados?

Si, corresponde al Departamento de Informática

No, yo puedo instalar libremente software en mi PC de trabajo

No estoy seguro(a)

5. ¿La organización cuenta con políticas y procedimientos asociados a controles del Antivirus?

Sí existe y la conozco

Sí existe, pero la desconozco

No existe

6. ¿La organización cuenta con políticas y procedimientos asociados a las copias de seguridad (respaldos)?

Sí existe y la conozco

Sí existe, pero la desconozco

No existe

A13- Seguridad de las Comunicaciones:

1. ¿La Organización cuenta con políticas de redes físicas e inalámbricas?

Sí se cuenta con políticas y las conozco

Sí se cuenta con políticas, pero las desconozco

No se cuenta con políticas

2. ¿La organización cuenta con políticas y procedimientos relacionados con la transmisión segura de información, tales como correo electrónico, uso de USB, carpetas compartidas, entre otras?

Sí se cuenta con políticas y procedimientos y los conozco

Sí se cuenta con políticas y procedimientos, pero los desconozco

No se cuenta con políticas y procedimientos

3. ¿Cuáles mecanismos de autenticación se utiliza para los accesos a la red de la organización?

Contraseña

Token

PIN

Firma Digital

4. ¿La organización cuenta con un monitoreo de servicios de red?

Sí

No

5. ¿La organización cuenta con una segmentación de red?

Si existe

No existe

6. ¿La organización cuenta con acuerdos de confidencialidad?

Sí existe y la conozco

Sí existe, pero la desconozco

No existe

A16 - Gestión de Incidentes de Seguridad:

1. ¿La organización cuenta con políticas y procedimientos para la gestión de incidentes?

Sí se cuenta con políticas y procedimientos y los conozco

Sí se cuenta con políticas y procedimientos, pero los desconozco

No se cuenta con políticas y procedimientos

2. Cuando ocurren incidentes de la seguridad de la información (alerta de virus, interrupciones en el sistema, entre otros) ¿cómo son informados?

Mediante llamada al Departamento de Informática

Informo al Jefe de mi Departamento

Formulo un caso por medio de la Mesa de Ayuda

Lo notifico vía correo electrónico al Departamento de Informática

Voy directamente a la oficina de los compañeros del Departamento de Informática y presento el aviso

No lo informo

3. ¿La organización cuenta con un proceso de clasificación y/o escalamiento para priorizar los incidentes?

Sí hay un procedimiento y lo conozco

Sí hay un procedimiento, pero lo desconozco

No hay un procedimiento

4. ¿La organización cuenta con personal capacitado, competente y confiable con herramientas adecuadas y procesos definidos para el manejo de los incidentes?

Sí y se cuenta con la capacitación adecuada

Sí, pero se requiere de mayor capacitación

No, acudimos a un tercero