UNIVERSIDAD DON BOSCO
VICERRECTORÍA ACADÉMICA
FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE

Maestro(a) en Seguridad y Gestión de Riesgos Informáticos

PROYECTO

Modelo de políticas de seguridad y gestión de la información, basados en la ISO 27001, aplicables a las cooperativas de Ahorro y Crédito del municipio de San Vicente, departamento de San Vicente, El Salvador.

PRESENTADO POR

Claudia Valentina Salazar Ruano

Eliseo Eulises Romero Ayala

ASESOR

Julio Alberto Guzmán Martínez

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América

Mayo 2024

AGRADECIMIENTOS

A DIOS

Gracias por permitirme alcanzar esta meta que ahora estoy por culminar.

A LAS MUJERES DE MI FAMILIA

Todas ellas ejemplos de perseverancia y superación personal y profesional:

Mi madre Anabel Salazar, por su apoyo, cariño y comprensión durante este periodo, y por haberme inculcado el hábito de la lectura y el aprendizaje.

Mi hermana Susana Salazar y abuela Elisa Salazar gracias por su cariño, apoyo y guía.

Mi abuela Otilia Salazar, que siempre llevo en mi corazón.

A MI ASESOR Y PROFESORES

Que con vocación trataron de transmitirnos sus conocimientos de la mejor manera.

Claudia Valentina Salazar Ruano

AGRADECIMIENTOS

A DIOS TODO PODEROSO

Quien ha sido mi fuerza y guía en todo momento de mi vida, brindándome sabiduría, fortaleza y una luz durante este proceso el cual florece con este nuevo logro académico.

1º Tesalonicenses 5.18 "… *y den gracias a Dios en toda ocasión; esta es, por voluntad de Dios, su vocación de cristianos*…"

A MIS PADRES

Delmy Amabel Ayala de Romero y Manuel Antonio Romero Chávez, por sus consejos y apoyo incondicional que me han mostrado durante toda mi vida. Los amo.

A MIS HERMANOS/AS

Por su cariño y apoyo desinteresado en los momentos más importantes durante el proceso académico.

A MI ESPOSA E HIJOS

Infinitas gracias por su amor, apoyo, paciencia y comprensión durante estos años para culminar un nuevo logro académico.

A MI ASESOR

Julio Guzmán, por asesorarme en este proceso que sin duda ha marcado mi vida profesional y de igual manera a los maestros/as que durante el desarrollo de la carrera compartieron sus conocimientos con mi persona.

Eliseo Eulises Romero Ayala

Contenido

Introducción 7

1 Capítulo I: Generalidades 8

1.1 Planteamiento del problema 8

1.2 Justificación 9

1.3 Delimitación 10

1.4 Objetivos 10

2 Capítulo II: Marco Teórico 11

2.1 Antecedentes de las Cooperativas de Ahorro y Crédito 11

2.2 Asociaciones Cooperativas de Ahorro y Crédito 12

2.3 Seguridad informática 13

2.4 Información 13

2.5 Política de Seguridad 13

2.6 Objetivos de seguridad 14

2.7 Actividades de seguridad de auditoría 16

2.8 Que es un ciberataque 16

2.9 Organización Internacional de Normalización (ISO) 18

2.10 ISO 27001:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos. 18

2.11 ISO/IEC 27002:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información 21

2.12 PCI DSS 22

2.13 COBIT: Marco de Control para Empresas de Tecnología de la Información 24

2.14 ITIL. Las mejores prácticas en Gestión de Servicios de TI. 25

2.15 Gestión de la Seguridad de la Información 26

2.16 Ley de Protección de Datos Personales en El Salvador 26

2.17 Ley de Bancos Cooperativas y Sociedades de Ahorro y Crédito.....28

2.18 Ley Especial Contra Delitos Informáticos y Conexos 28

2.19 Ley de Firmas Electrónicas.....29

2.20 Marco Técnico Aplicable.....30

3 Capítulo III: Metodología.....36

3.1 Tipo de investigación 36

3.2 Población y muestra 37

3.3 Técnica e instrumento.....38

3.4 Procedimiento.....38

3.5 Análisis estadístico o de información 40

4 Capítulo IV: Resultados 41

4.1 Análisis de la información 41

5 Capítulo V. Propuesta.....61

5.1 Política de Gestión de Seguridad de la Información (PGSI) para Cooperativas de Ahorro y Crédito en el departamento de San Vicente, El Salvador. 61

5.2 Política de Control de Acceso e Información de Datos para las Cooperativas de Ahorro y Crédito de San Vicente, El Salvador. 81

5.3 Política de Auditoría y Revisión de Seguridad de la Información para las Cooperativas de Ahorro y Crédito en San Vicente, El Salvador. 89

5.4 Desarrollo de Aplicación Móvil para la verificación de cumplimiento de los controles de la ISO 27001:2022.....96

6 Conclusiones 104

7 Recomendaciones 105

8 Bibliografía.....106

9 Anexos.....109

Introducción

Las Cooperativas de San Vicente en El Salvador, tienen varios desafíos para consolidarse como instituciones financieras estables y hacer crecer sus organizaciones, uno de estos desafíos es actualizarse en el uso de tecnologías, pero no deben dejar a un lado la protección de los activos de información, lo cual es un proceso continuo, debido a los avances tecnológicos y el surgimiento de nuevas amenazas cibernéticas.

En el desarrollo de este documento se plantea una propuesta que ayudaría a sentar bases sólidas en las cooperativas para el fortalecimiento de la seguridad de la información.

En el primer capítulo se presenta de forma resumida la problemática actual relacionada con las cooperativas en el área de seguridad de la información, las razones por las que es importante abordar esta problemática y los objetivos específicos que se buscan cumplir con esta investigación.

En el segundo capítulo se brindan los conceptos involucrados en la investigación comenzando con los antecedentes y descripción de las Asociaciones Cooperativas de Ahorro y crédito, luego se presenta el contexto actual de la seguridad de la información y las normativas y marcos teóricos más reconocidos y ampliamente utilizados, como ISO 27001, COBIT, ITIL, entre otros. También describimos los marcos regulatorios que son de cumplimiento legal en El Salvador, para las cooperativas de ahorro y crédito.

En el tercer capítulo veremos la metodología, de cómo se realizó la investigación, sus resultados y análisis de estos, para finalmente, en un último apartado se brinda una propuesta que busca contribuir en el fortalecimiento de la seguridad de la información en las cooperativas, siendo ésta una guía para asegurar la confidencialidad, integridad y disponibilidad de los datos. También como parte de la propuesta se desarrolló una herramienta tecnológica en modo aplicación Android, que será de utilidad para verificar el cumplimento de las políticas.

1 Capítulo I: Generalidades

1.1 Planteamiento del problema

Actualmente las cooperativas de ahorro y crédito, se enfrentan a desafíos significativos en términos de seguridad de la información. A pesar de que hacen los esfuerzos posibles en proteger esta información sensible, muchas de estas entidades carecen de un modelo de políticas de seguridad y gestión de la información robusto y fiable, basado en estándares reconocidos internacionalmente como la ISO 27001:2022.

La falta de un enfoque sistemático y estructurado para la seguridad de la información puede exponer a estas entidades financieras a una serie de riesgos y amenazas.

En algunas cooperativas, especialmente las más pequeñas o menos desarrolladas, puede que los miembros no estén plenamente conscientes de los riesgos asociados con la falta de políticas de seguridad.

Los líderes y miembros de la cooperativa pueden carecer de experiencia o conocimientos en materia de gestión de seguridad, lo que dificulta el desarrollo e implementación de políticas efectivas.

Abordar esta problemática requiere un enfoque holístico que incluya la sensibilización, la asignación de recursos adecuados, la formación y capacitación, la colaboración con expertos en seguridad, y el monitoreo continuo del entorno de riesgo y de las necesidades de la cooperativa.

Por lo tanto, ante este escenario se evidencia que no se tiene un modelo de políticas de seguridad y gestión de la información basado en la ISO 27001:2022, específicamente adaptado a las necesidades y características de las cooperativas de ahorro y crédito.

1.2 Justificación

La seguridad de la información es de vital importancia en la actualidad debido a diversos factores que afectan a individuos, empresas y gobiernos.

Dada la creciente amenaza de ciberataques al sector financiero, se debe poner mayor énfasis en garantizar y proporcionar controles de ciberseguridad, detección de amenazas y respuestas a incidentes para garantizar la Confidencialidad, Integridad, Disponibilidad de los datos tanto de los usuarios como de las entidades mismas.

Las organizaciones manejan una gran cantidad de datos e información confidencial que deben protegerse contra amenazas internas y externas, por tanto, al definir medidas y controles ayuda en gran medida a proteger estos activos de información contra accesos no autorizados, pérdidas o filtraciones.

La seguridad de la información implica identificar, evaluar y mitigar riesgos relacionados con la confidencialidad, integridad y disponibilidad de los datos, esto para garantizar que los datos de los usuarios estén bajo la debida protección de la entidad receptora.

En el informe ESET Security Report 2023: el panorama de la seguridad en las empresas de América Latina, menciona que los países con el mayor porcentaje de detecciones de códigos maliciosos en campañas de phishing son Ecuador 8%, seguido por Costa Rica 7,2%, Colombia 5,7%, Guatemala 5,2% y El Salvador 5,1%. En este contexto, el 66% de las empresas señalaron que el robo o fuga de información es su mayor preocupación en materia de ciberseguridad [1].

¿Cuáles son las principales formas de ataque que registran las organizaciones? Según la encuesta, el 70% considera que el phishing es la forma de ataque más común, seguida por los ataques con malware (63%) y en tercer lugar los que buscan robar credenciales de acceso (56%).

Nótese aquí la importancia en materia de ciberseguridad y la protección de datos de los usuarios, se vuelve primordial para las empresas, por esta razón, el presente trabajo de investigación se enfoca en proporcionar un Modelo de políticas de seguridad y gestión de la información, basados en la ISO 27001, aplicables a las cooperativas de Ahorro y Crédito del municipio de San Vicente, departamento de San Vicente, adaptado con sus actividades y necesidades, que les permita establecer las bases de un plan de seguridad apropiado.

En el área de San Vicente se han identificado seis cooperativas que proporcionan servicios financieros a sus socios o miembros. Con la adaptación de estos modelos de políticas de seguridad y gestión de la información, se pretende que en el futuro sean adoptadas por las otras sucursales que se tienen a lo largo y ancho del país.

1.3 Delimitación

La investigación se efectuará con los encargados de las áreas de Tecnologías de la Información (TI) o área de ciberseguridad de las cooperativas del municipio de San Vicente, departamento de San Vicente, con el fin de poder diagnosticar cuales son las medidas de protección que tienen como institución hacia la protección de la información de los datos de los socios y de la misma empresa.

1.4 Objetivos

General

Proponer modelo de políticas de seguridad y gestión de la información, a las cooperativas de Ahorro y Crédito del municipio de San Vicente, departamento de San Vicente, de acuerdo a la norma ISO 27001.

Específicos

- Definir el marco teórico relacionado a los modelos de políticas de seguridad actuales aplicables al sector financiero.

- Diseñar una política de gestión de la seguridad de la información de acuerdo con la ISO 27001 aplicables a las actividades de las cooperativas de Ahorro y Crédito del municipio de San Vicente, departamento de San Vicente.
- Elaborar una Política de control de acceso, que garantice que el acceso a la información sea autorizado y gestionado adecuadamente.
- Definir políticas de auditoría y revisión que garanticen la eficacia continua de las medidas de seguridad.
- Establecer modelos y controles para el manejo de información sensible dentro de la cooperativa en función de la norma ISO 27001 y estándares que sean aplicables a la seguridad de la información y protección a ciberataques.

2 Capítulo II: Marco Teórico

2.1 Antecedentes de las Cooperativas de Ahorro y Crédito

El Cooperativismo es asociativo, nace para defender a las personas, surgen las asociaciones en forma de empresa propia destinada a satisfacer las necesidades comunes de las mismas. El Cooperativismo en materia socioeconómica defiende a las personas, en su doble carácter “como consumidores y productores”. Los considerados padres del cooperativismo moderno son Roben Owen y Willian King, pero también contribuyeron grandemente otros pensadores franceses y alemanes. En El Salvador se escucha, por primera vez, del cooperativismo en forma teórica, en una cátedra de enseñanza, en la facultad de jurisprudencia y ciencias sociales de la Universidad de El Salvador. Fue en 1914, que se organiza la primera cooperativa, por un grupo de zapateros, en San Salvador en la cuesta del Palo Verde y en 1938, se funda la Cooperativa Algodonera.

Luego el Cooperativismo llegó al gremio de los empleados públicos, como un medio de defensa contra el agiotismo. Las cooperativas contaban con el apoyo del gobierno en turno, que aportaba capital inicial, pero los empleados identifican el capital cedido por el gobierno,

como propiedad de ellos y no creyeron que estaban obligados, por esa razón, a resarcir las cantidades que se les concedían en calidad de préstamo. Así mismo el surgimiento de secciones y departamentos en instituciones gubernamentales el sector inició su crecimiento hasta que el Estado decide centralizar este rol en una sola Institución que dirija y coordine la actividad cooperativa en el país. Fue el 25 de noviembre de 1969 que la Asamblea Legislativa, promulgó el Decreto No. 560 que dio pie a la creación del INSAFOCOOP como una corporación de derecho público con autonomía en los aspectos económico y administrativo, ese mismo día se promulga la primera Ley General de Asociaciones Cooperativas. A falta de presupuesto que permitiera su funcionamiento el INSAFOCOOP comenzó a operar hasta el 1 de julio de 1971. Hoy con más de 40 años al servicio del sector cooperativo, la institución ha crecido descentralizando su trabajo en oficinas ubicadas en las distintas zonas del país dando un servicio a través de sus regionales en todo lo ancho y largo de El Salvador.

En 1966 se fundó la Federación de Cooperativas de Ahorro y Crédito de El Salvador (FEDECACES), como organismo cooperativo de segundo nivel, producto del apoyo de la "Alianza por el Progreso" CUNA-AID [2].

2.2 Asociaciones Cooperativas de Ahorro y Crédito

Dentro de las Asociaciones Cooperativas de servicios, se encuentran las Asociaciones Cooperativas de Ahorro y Crédito; las cuales se constituyen por personas que se organizan para facilitar servicios de ahorro y préstamo, principalmente a sus asociados; ofreciéndoles intereses razonables, rapidez en el trámite de préstamos, fomento del hábito de ahorro sistemático y el establecimiento de lazos de unión y confianza con sus asociados.

- Podrán recibir depósitos de terceras personas que tengan la calidad de aspirantes a asociados
- Facilita servicios de intermediación financiera en beneficios de sus asociados
- La junta monetaria autorizó las condiciones, en cuanto al tipo de interés y límites, de

estas operaciones

Cuál sería la diferencia esencial entre la banca y las cooperativas de ahorro y crédito.

La principal diferencia radica en que la banca ha sido creada para lucrarse de los servicios que ofrecen maximizando la ganancia de los accionistas, mientras que las cooperativas su finalidad no es el lucro, ya que el objetivo primordial es que los miembros unan sus recursos para brindar servicios a otros miembros y así ofrecer productos más competitivos en relación a la banca [3].

2.3 Seguridad informática

La seguridad informática se enfoca en minimizar los riesgos y vulnerabilidades en los recursos de hardware y software relacionados con el acceso y la utilización malintencionada de la información de los sistemas de software, para garantizar la integridad, confidencialidad y disponibilidad de esta [4].

2.4 Información

Datos procesados, incluyendo datos que pueden ser utilizados en la producción, transmisión o interpretación de datos, en un contexto específico [5].

2.5 Política de Seguridad

La política de seguridad es un conjunto de reglas que se aplican a las actividades del sistema y a los recursos de comunicaciones que pertenecen a una organización. Estas reglas incluyen áreas como la seguridad física, personal, administrativa y de la red [6].

La política de seguridad define qué es lo que desea proteger y qué espera de los usuarios del sistema. Proporciona una base para la planificación de la seguridad al diseñar nuevas aplicaciones o ampliar la red actual. Describe responsabilidades del usuario como las de proteger información confidencial y crear contraseñas no triviales. La política de seguridad también debe describir cómo se va a supervisar la efectividad de las medidas de seguridad.

Esta supervisión le ayudará a determinar si alguna persona podría intentar burlar las defensa en sus múltiples niveles de seguridad [6].

2.6 Objetivos de seguridad

Los objetivos de seguridad entran dentro de una o más de estas categorías:

2.6.1 Protección de recursos

El esquema de protección de recursos garantiza que solo los usuarios autorizados podrán acceder a los objetos del sistema. La capacidad de asegurar todo tipo de recursos del sistema es una de las ventajas del Sistema. Primero deberá definir con precisión las distintas categorías de usuarios que pueden acceder al sistema. Asimismo, cuando cree la política de seguridad, deberá definir qué tipo de autorización de acceso desea otorgar a estos grupos de usuarios [6].

2.6.2 Autenticación

Es la seguridad o la verificación de que el recurso (persona o máquina) situado en el otro extremo de la sesión es realmente el que dice ser. Una autenticación convincente defiende el sistema contra riesgos de seguridad como la suplantación, en las que el remitente o el destinatario utiliza una identidad falsa para acceder al sistema. Tradicionalmente, los sistemas han utilizado contraseñas y nombres de usuario para la autenticación; los certificados digitales pueden ofrecer un método más seguro de autenticación, a la vez que proporcionan otras ventajas de seguridad. Los usuarios autenticados podrían tener distintos tipos de permisos, según su nivel de autorización [6].

2.6.3 Autorización

La autorización es el proceso de determinar quién o qué puede acceder a los recursos del sistema o ejecutar determinadas actividades en un sistema. Normalmente, la autorización se realiza en el contexto de la autenticación [6].

2.6.4 Integridad

Es la seguridad de que la información entrante es la misma que la que se ha enviado. Para entender la integridad, primero deberá comprender los conceptos de integridad de los datos e integridad del sistema [6].

- Integridad de los datos: los datos están protegidos contra cambios o manipulaciones no autorizadas. La integridad de los datos los defiende contra riesgos de seguridad como la manipulación, donde alguien intercepta y modifica la información sin estar autorizado para ello. Además de proteger los datos que están almacenados en la red, podría necesitar medidas de seguridad adicionales para garantizar la integridad de los datos cuando estos entran en su sistema procedentes de fuentes que no sean de confianza. Cuando los datos que entran en su sistema proceden de una red pública, necesitará métodos de seguridad para realizar estas tareas:
  - Proteger los datos para que no se puedan husmear ni interpretar, lo que se suele hacer cifrándolos.
  - Asegurar que las transmisiones no han sido alteradas (integridad de los datos).
  - Demostrar que se ha producido la transmisión (no repudio). En el futuro, es posible que necesite el equivalente electrónico del correo certificado.
- Integridad del sistema: el sistema proporciona resultados coherentes con el rendimiento esperado.

2.6.5 No repudio

Prueba de que se ha producido una transacción o de que se ha enviado o recibido un mensaje. El uso de certificados digitales y de la criptografía de claves públicas para firmar transacciones, mensajes y documentos es la base del no repudio. El remitente y el destinatario están ambos de acuerdo en que el intercambio tiene lugar. La firma digital de los datos es una prueba suficiente [6].

2.6.6 Confidencialidad

Es la seguridad de que la información confidencial permanece privada y no es visible para los escuchas intrusos. La confidencialidad es fundamental para la seguridad total de los datos. El cifrado de los datos con certificados digitales y la capa de sockets segura (SSL) o con una conexión de redes privadas virtuales (VPN) permite asegurar la confidencialidad al transmitir datos entre varias redes que no sean de confianza. La política de seguridad debe indicar qué métodos se emplearán para proporcionar la confidencialidad de la información dentro de la red y de la información que sale de ella [6].

2.7 Actividades de seguridad de auditoría

Consisten en supervisar los eventos relacionados con la seguridad para proporcionar un archivo de anotaciones de los accesos satisfactorios y de los no satisfactorios (denegados). Los registros de accesos satisfactorios indican quién está haciendo cada tarea en los sistemas. Los registros de accesos no satisfactorios (denegados) indican que alguien está intentando abrirse paso a través de las barreras de seguridad del sistema o que alguien tiene dificultades para acceder al sistema [6].

2.8 Que es un ciberataque

Un ciberataque es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital [7].

Los actores de amenazas suelen irrumpir en las redes informáticas porque buscan algo específico. Los objetivos comunes incluyen:

- Dinero
- Datos financieros de las empresas
- Listas de clientes

- Datos de clientes, incluida información de identificación personal (PII, en sus siglas en inglés) u otros datos personales confidenciales
- Direcciones de email y credenciales de inicio de sesión
- Propiedad intelectual, como secretos comerciales o diseños de productos

Si tienen éxito, los ataques cibernéticos pueden dañar a las empresas. Pueden causar tiempo de inactividad, pérdida de datos y pérdida de dinero.

- Ciberataques más comunes
    - Programa malicioso (malware). El malware es un software malicioso que puede hacer que los sistemas infectados no funcionen. Los programas maliciosos pueden destruir datos, robar información o incluso borrar archivos críticos para la capacidad de ejecución del sistema operativo.
    - Ingeniería Social. Los ataques de ingeniería social manipulan a las personas para que hagan cosas que no deberían hacer, como compartir información que no deberían compartir, descargar software que no deberían descargar o enviar dinero a los delincuentes.
    - Ataque de denegación de servicios. Los ataques de denegación de servicio (Denegación de Servicio - DoS) y Denegación de Servicio Distribuido (DDoS) inundan los recursos de un sistema con tráfico fraudulento. Este tráfico abruma al sistema, evitando las respuestas a solicitudes legítimas y reduciendo la capacidad del sistema de realizarla dichas operaciones. Un ataque de denegación de servicio puede ser un fin en sí mismo o una configuración para otro ataque.
    - Compromiso de cuenta. Compromiso de cuenta es cualquier ataque en el que los piratas informáticos secuestran la cuenta de un usuario legítimo para realizar actividades maliciosas. Los ciberdelincuentes pueden entrar en la cuenta de un

usuario de muchas maneras. Pueden robar credenciales a través de ataques de phishing o comprar bases de datos de contraseñas robadas de la web oscura.

2.9 Organización Internacional de Normalización (ISO)

La Organización Internacional de Normalización (ISO por sus siglas en inglés) desarrolla estándares requeridos por el mercado que representan un consenso de sus miembros acerca de productos, tecnologías, sistemas y métodos de gestión, entre otros. Estos estándares, por naturaleza, son de aplicación voluntaria, ya que el carácter no gubernamental de ISO no le da autoridad legal para forzar su implantación. Sólo en aquellos casos en los que un país ha decidido adoptar un determinado estándar como parte de su legislación, puede convertirse en obligatorio [8].

2.10 ISO 27001:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos.

La ISO 27001:2022 es la norma internacional que proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como cumplimiento legal. La aplicación y disposición de implementación de esta normativa es esencial para proteger sus activos más importantes, la información de sus clientes y empleados, la imagen corporativa y otra información privada. La norma ISO incluye un enfoque basado en procesos para lanzar, implantar, operar y mantener un SGSI [9].

Beneficios de la ISO 27001 en su versión 2022

- Información segura en todas sus formas, incluidas copias impresas y digitales.
- Datos digitales mejor protegidos.
- Protocolos de seguridad de la información basados en la nube.
- Aumentar la resiliencia cibernética.

- Marco administrado central que consolida toda la información con procesos únicos y eficaces para evitar la interferencia de procesos entre sí.
- Garantía de protección general sobre medios, recursos y sistemas de información, incluso contra los riesgos digitales y otras amenazas.
- Implementación de un proceso de evaluación y respuesta a las amenazas de seguridad en evolución permanente.
- Políticas, procesos y procedimientos para la integridad, confidencialidad y disponibilidad de los datos [10].

Requerimientos de la norma

- Contexto de la organización.
  - Entender la organización y su contexto
  - Comprender las necesidades y expectativas de las partes interesadas
  - Determinación del alcance del sistema de gestión de seguridad de la información
  - Sistema de gestión de seguridad de la información
- Liderazgo.
  - Liderazgo y compromiso
  - Política
  - Funciones, responsabilidades y autoridades de la organización
- Planificación.
  - Acciones para abordar riesgos y oportunidades
  - Objetivos de seguridad de la información y planificación para alcanzarlos
- Soporte.
  - Recursos
  - Competencia

- Conciencia
- Comunicación
- Información documentada

- Operación.
  - Planificación y control operativo
  - Evaluación de riesgos de seguridad de la información
  - Tratamiento de riesgos de seguridad de la información
- Evaluación del desempeño.
  - Seguimiento, medición, análisis y evaluación
  - Auditoría interna
  - Revisión por la dirección
- Mejora.
  - Mejora continua
  - No conformidad y acción correctiva

La información se ha convertido en un activo crítico para las organizaciones en la era digital, y su protección se ha vuelto esencial para garantizar la continuidad del negocio y la confianza de todos los involucrados en la empresa. En este contexto, la norma ISO 27001 emerge como un estándar internacional clave para la gestión de la seguridad de la información, proporcionando un marco robusto y sistemático para abordar los desafíos contemporáneos en materia de ciberseguridad, para la protección de la información de las cooperativas de ahorro y crédito.

Esta norma establece directrices claras y principios fundamentales para la creación, implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI). Esta norma internacional, reconocida mundialmente, no solo aborda la protección de datos sensibles, sino que también fomenta un enfoque integral que considera la confidencialidad, integridad y disponibilidad de la información.

En el contexto específico de las cooperativas de ahorro y crédito, donde la información financiera y personal de los miembros es de vital importancia, adoptar un enfoque basado en la ISO 27001 no solo es una medida proactiva, sino también una demostración tangible de compromiso con la protección de los activos de la organización y la confianza de los miembros.

2.11 ISO/IEC 27002:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información

Proporciona un conjunto de referencia de controles genéricos de seguridad de la información, incluida una guía de implementación. Seguridad de la información, ciberseguridad y protección de datos [11].

La perspectiva integral de ISO/IEC 27002:

- Prioriza el enfoque y protección de los activos de información
- Enfatiza el monitoreo al separar los objetivos de algunos controles.
- Favorece la priorización al integrar varios controles que se convierten en uno.
- Se basa en resiliencia, protección, defensa y gestión.

Nuevos controles ISO/IEC 27002:2022:

- Inteligencia de amenazas.
- Seguridad de la información para el uso de servicios en la nube.
- Preparación de las TIC para la continuidad del negocio.
- Supervisión de la seguridad física.
- Gestión de la configuración.
- Eliminación de información.
- Enmascaramiento de datos.
- Prevención de fuga de datos.
- Actividades de seguimiento.
- Filtrado web.

- Codificación segura.

En el panorama actual de amenazas cibernéticas y riesgos de seguridad, la gestión efectiva de la seguridad de la información se ha vuelto imperativa para organizaciones de todos los sectores. En este contexto, la norma ISO/IEC 27002 emerge como un estándar internacional crucial para establecer controles y prácticas de seguridad que salvaguarden la confidencialidad, integridad y disponibilidad de la información.

Es un estándar complementario a la ISO 27001, que proporciona directrices detalladas para la implementación de controles de seguridad de la información. Mientras que la ISO 27001 establece el marco general de un Sistema de Gestión de Seguridad de la Información (SGSI), la ISO 27002 se centra en los controles específicos que las organizaciones deben considerar para gestionar los riesgos de seguridad.

En el contexto específico de las cooperativas de ahorro y crédito, donde la información financiera y personal es de suma importancia, adoptar este tipo de normativas dado que proporcionan un marco específico y detallado para establecer controles de seguridad adecuados. Esto no solo fortalece la protección de los activos de la cooperativa, sino que también contribuye a mantener la confianza de los miembros y cumplir con regulaciones y normativas específicas del sector financiero.

2.12 PCI DSS

PCI DSS – "Payment Card Industry Data Security Standard" (Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago), es un conjunto de normas de seguridad de la información diseñado para garantizar la protección de los datos de tarjetas de pago y transacciones relacionadas.

Es un estándar de seguridad establecido por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC) para proteger la información confidencial de los

titulares de tarjetas. Este estándar se aplica a todas las entidades que almacenan, procesan o transmiten datos de tarjetas de pago, incluidas las cooperativas de ahorro y crédito.

Beneficios de la Implementación de PCI DSS:

- Protección de Datos Sensibles
- Confianza del Cliente
- Reducción de Riesgo
- Cumplimiento Legal

Relevancia del PCI DSS con respecto a las cooperativas de ahorro y crédito.

- Manejo de Transacciones Financieras
- Confianza del Socio y Cliente
- Prevención de Fraudes
- Evitar Sanciones y Multas [12].

Los requisitos que deben cumplir los PCI DSS

1. Instalar y mantener una configuración de firewall para proteger los datos de los titulares de tarjetas.
2. No utilizar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
3. Proteger los datos almacenados de los titulares de tarjetas.
4. Cifrar la transmisión de los datos de los titulares de tarjetas a través de redes públicas abiertas.
5. Usar y actualizar con regularidad el software antivirus.
6. Desarrollar y mantener sistemas y aplicaciones seguras.
7. Limitar el acceso a los datos de los titulares, únicamente a lo que los negocios necesitan saber.

8. Asignar una identificación única a cada persona con acceso a una computadora.
9. Restringir el acceso físico a los datos de los titulares de tarjetas.
10. Rastrear y monitorear todo acceso a los recursos de la red y a los datos de titulares de tarjetas.
11. Probar con regularidad los sistemas y procesos de seguridad.
12. Mantener una política que aborde la seguridad de la información [13].

2.13 COBIT: Marco de Control para Empresas de Tecnología de la Información

COBIT 5, o Control Objectives for Information and Related Technologies versión 5, es un marco de gobierno y gestión de TI (Tecnologías de la Información) desarrollado por ISACA (Information Systems Audit and Control Association).

Tiene como objetivo proporcionar un enfoque integral y estructurado para el gobierno y la gestión de las tecnologías de la información en las organizaciones.

Principales características

- Marco de Gobierno de TI. Proporciona un marco de trabajo que ayuda a las organizaciones a desarrollar, implementar, supervisar y mejorar sus sistemas de gobierno de TI.
- Enfoque Holístico. Abarca toda la organización, integrando los objetivos de negocio con los de TI para garantizar un alineamiento efectivo.
- Proceso de Mejora Continua. Se basa en el ciclo de mejora continua, proporcionando un conjunto de procesos y controles que permiten a las organizaciones adaptarse y evolucionar de manera constante.
- Relación con Otros Estándares: Se integra con otros estándares y marcos de trabajo, como ITIL (Information Technology Infrastructure Library) y ISO 27001, facilitando la implementación conjunta.

- Enfoque de Valor. Se centra en la creación de valor a través del uso efectivo de la tecnología, asegurando que las inversiones en TI estén alineadas con los objetivos empresariales [14].

La implementación de COBIT puede contribuir a la mejora de la seguridad, eficiencia y rendimiento en la gestión de servicios financieros

2.14 ITIL. Las mejores prácticas en Gestión de Servicios de TI.

ITIL "Information Technology Infrastructure Library" (Biblioteca de Infraestructura de Tecnologías de la Información), es un marco de gestión de servicios de TI que proporciona un conjunto de prácticas y procesos estandarizados para mejorar la eficiencia y la calidad de los servicios de tecnología de la información.

Principales características

- Proceso de Servicio: organiza los servicios de TI en ciclos de vida, desde la estrategia hasta la operación y mejora continua.
- Mejores Prácticas: Proporciona mejores prácticas para la planificación, diseño, implementación, operación y mejora continua de los servicios de TI.
- Enfoque en el Cliente: Pone énfasis en la entrega de servicios centrados en el cliente y la satisfacción de las necesidades del negocio.
- Gestión de Incidentes y Problemas: Incluye procesos definidos para manejar incidentes, problemas y cambios en la infraestructura de TI.
- Gobierno y Cumplimiento: Ayuda a establecer un marco de gobierno para garantizar que los servicios de TI cumplan con los requisitos regulatorios y de la organización.

La implementación de ITIL en cooperativas de ahorro y crédito puede proporcionar un marco sólido para mejorar la eficiencia operativa, la experiencia del cliente, la adaptabilidad a

las necesidades del negocio, la gestión de riesgos y el cumplimiento normativo, contribuyendo así al éxito y la estabilidad de la institución financiera [15].

2.15 Gestión de la Seguridad de la Información

La seguridad requerida se establece mediante políticas, procesos, comportamientos, gestión de riesgos y controles, los cuales deben mantener un equilibrio entre:

- **Prevención** Asegurarse de que no ocurran incidentes de seguridad
- **Detección** rápida y confiable de incidentes que no se pueden prevenir
- **Corrección** Recuperarse de incidentes una vez detectados.

También es importante lograr un equilibrio entre proteger a la organización de daños y permitirle innovar. Los controles de seguridad de la información que son demasiado restrictivos pueden hacer más daño que bien, o pueden ser eludidos por personas que intentan trabajar más fácilmente. Los controles de seguridad de la información deben considerar todos los aspectos de la organización y alinearse con su apetito por el riesgo.

La gestión de la seguridad de la información interactúa con todas las demás prácticas. Crea controles que cada práctica debe considerar al planificar cómo se realizará el trabajo. También depende de otras prácticas para ayudar a proteger la información.

La gestión de la seguridad de la información debe ser impulsada desde el nivel más alto de la organización, sobre la base de requisitos de gobernanza claramente entendidos[9].

2.16 Ley de Protección de Datos Personales en El Salvador

Establece las reglas para el tratamiento de datos personales y la protección de la privacidad de los individuos. En el año 2019 la Asamblea Legislativa de El Salvador aprueba esta ley con el objetivo de brindar una protección integral de los datos personales de las personas naturales en cuanto resulte pertinente, indistintamente en la forma que se almacenen y resguarden.

Según el Art. 2.- Esta ley será de aplicación a los datos personales que figuren en bases de datos total o parcialmente automatizadas o manuales, pertenecientes a organismos públicos o privados, que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos por los sectores públicos o privados, en la República de El Salvador.

Se regirá por esta ley todo tratamiento de datos de personas naturales que sea efectuado en el territorio salvadoreño en el marco de las actividades del establecimiento del responsable del tratamiento, con excepción de:

I. El tratamiento de datos de historial crediticios que realicen los sujetos obligados en los supuestos de la Ley de Regulación de los Servicios de Información sobre el Historial de Créditos de las Personas.

II. El tratamiento que las personas naturales lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente interno, personales o domésticos, y sin fines de divulgación o utilización comercial.

III. El tratamiento de la información obtenida mediante un proceso previo de disociación o anonimización, de manera que el resultado no pueda asociarse al Titular

IV. Los tratamientos que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.

Principios

- Principio de legalidad
- Principio de calidad
- Principio de finalidad
- Principio de Licitud o del previo consentimiento informado
- Principio de seguridad de los datos
- Principio o deber de confidencialidad
- Principio de transparencia
- Principio de prohibición

- Principio de responsabilidad proactiva
- Principio de privacidad
- Principio de aviso de privacidad [16].

2.17 Ley de Bancos Cooperativas y Sociedades de Ahorro y Crédito

La presente ley tiene por objeto regular la organización, el funcionamiento y las actividades de intermediación financiera que realizan los bancos cooperativos y las sociedades de ahorro y crédito que se indican en la presente ley, con el propósito de que cumplan con sus objetivos económicos y sociales, y garanticen a sus depositantes y socios la más eficiente y confiable administración de sus recursos [17]

2.18 Ley Especial Contra Delitos Informáticos y Conexos

La presente Ley tiene por objeto proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas en los términos aplicables y previstos en la presente Ley [18].

Artículo 4. Define el Acceso Indebido a Sistemas Informáticos - El que intencionalmente y sin autorización o excediendo la que se le hubiere concedido, acceda, intercepte o utilice parcial o totalmente un sistema informático que utilice las Tecnologías de la Información o la Comunicación, será sancionado con prisión de uno a cuatro años.

Artículo 5: Define en qué consiste el Acceso Indebido a los Programas o Datos Informáticos - El que a sabiendas y con la intención de usar cualquier dispositivo de la Tecnología de la Información o la Comunicación, accediera parcial o totalmente a cualquier

programa o a los datos almacenados en él, con el propósito de apropiarse de ellos o cometer otro delito con éstos, será sancionado con prisión de dos a cuatro años.

Artículo 7: Establece las penas para quienes cometan delitos informáticos, incluidos aquellos relacionados con la seguridad de la información … *Si el delito previsto en el presente artículo se cometiere de forma culposa, por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, será sancionado con prisión de uno a tres años*….

Artículo 9: Trata sobre la protección de datos informáticos y establece medidas para garantizar la confidencialidad e integridad de la información… *En igual sanción incurrirá quien induzca a un tercero para que de forma involuntaria, ejecute un programa, mensaje, instrucciones o secuencias para violar medidas de seguridad*...

Artículo 10: Establece disposiciones relacionadas con la seguridad de los sistemas informáticos y las medidas que deben tomarse para proteger la información contra accesos no autorizados y Estafa Informática. … *El que manipule o influya en el ingreso, el procesamiento o resultado de los datos de un sistema que utilice las Tecnologías de la Información y la Comunicación, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos o programación, valiéndose de alguna operación informática o artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial indebido para sí o para otro, será sancionado con prisión de dos a cinco años*…

2.19 Ley de Firmas Electrónicas

Tiene como objetivo principal regular el uso de firmas electrónicas y garantizar la seguridad y validez de los documentos electrónicos [19].

Art. 5.- El tratamiento de los datos personales que precisen los prestadores de servicios de certificación y los prestadores de servicio de almacenamiento de documentos electrónicos para el desarrollo de dichas actividades.

2.20 Marco Técnico Aplicable

La Organización Internacional de Normalización (ISO por sus siglas en inglés) como forma de estandarizar soluciones y procedimientos aplicables a las organizaciones, ha creado las normas técnicas internacionales que ayuden a la disminución o control de riesgos informáticos, para lo cual ha establecido lineamientos y guías que permitan el correcto tratamiento, así como incluir todas las áreas críticas de una organización [8].

Tabla 1

Lista de Controles Sugeridos por la ISO 27001:2022

Controles organizacionales	
Políticas de seguridad de la información	**Control** La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos.
Roles y responsabilidades de seguridad de la información	**Control** Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.
Responsabilidades de gestión	**Control** La gerencia debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos del tema de la organización.
Inteligencia de amenazas	**Control** La información relacionada con las amenazas a la seguridad de la información se recopilará y analizará para generar información sobre amenazas.
Inventario de información y otros activos asociados	**Control** Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.

Clasificación de la información	**Control** La información se clasificará de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.
Transferencia de información	**Control** Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.
Control de acceso	**Control** Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados se establecerán e implementarán en función de los requisitos de seguridad de la información y del negocio.
Derechos de acceso	**Control** Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización.
Seguridad de la información para el uso de servicios en la nube	**Control** Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer de acuerdo con los requisitos de seguridad de la información de la organización.
Protección de registros	**Control** Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.
Privacidad y protección de la información de identificación personal (PII)	**Control** La organización deberá identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.
Revisión independiente de la seguridad de la información.	**Control** El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.
Procedimientos operativos documentados	**Control** Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.
Controles de personas	
Acuerdos de confidencialidad o no divulgación	**Control** Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas relevantes.

Trabajo remoto	**Control** Se implementarán medidas de seguridad cuando el personal trabaje de forma remotapara proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la organización.
Informes de eventos de seguridad de la información	**Control** La organización debe proporcionar un mecanismo para que el personal informe eventos deseguridad de la información observados o sospechados a través de los canales apropiados de manera oportuna.
Controles físicos	
Perímetros físicos de seguridad	**Control** Los perímetros de seguridad se definirán y utilizarán para proteger las áreas quecontienen información y otros activos asociados.
Entrada física	**Control** Las áreas seguras deben estar protegidas por controles de entrada y puntos deacceso apropiados.
Asegurar oficinas, salas e instalaciones	**Control** Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones.
Monitoreo de seguridad física	**Control** Los locales deberán ser monitoreados continuamente para el acceso físico noautorizado.
Protección contra amenazasfísicas y ambientales.	**Control** Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, tales como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.
Trabajar en áreas seguras	**Control** Se diseñarán e implementarán medidas de seguridad para trabajar en áreas seguras.
Escritorio despejado y pantalla despejada	**Control** Se deben definir y hacer cumplir adecuadamente las reglas de escritorio limpio para documentos ymedios de almacenamiento extraíbles y las reglas de pantalla limpia para las instalaciones de procesamiento de información.
Medios de almacenamiento	**Control** Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificacióny los requisitos de manipulación de la organización.
Utilidades de apoyo	**Control** Las instalaciones de procesamiento de información deben estar protegidas contra cortes deenergía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.
Mantenimiento de equipo	**Control** El equipo se mantendrá correctamente para garantizar la disponibilidad, integridad yconfidencialidad de la información.

Eliminación segura o reutilización de equipos	**Control** Los elementos del equipo que contengan medios de almacenamiento se verificarán para garantizar que todos los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.
Controles tecnológicos	
Dispositivos de punto final de usuario	**Control** Se protegerá la información almacenada, procesada o accesible a través de los dispositivos finales del usuario.
Derechos de acceso privilegiado	**Control** La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará.
Restricción de acceso a la información	**Control** El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica del tema establecida sobre el control de acceso.
Acceso al código fuente	**Control** El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se gestionará adecuadamente.
Autenticación segura	**Control** Las tecnologías y procedimientos de autenticación segura se implementarán en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.
Gestión de capacidad	**Control** El uso de los recursos se controlará y ajustará de acuerdo con los requisitos de capacidad actuales y previstos.
Protección contra malware	**Control** La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.
Gestión de vulnerabilidades técnicas	**Control** Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.
Gestión de la configuración	**Control** Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.
Eliminación de información	**Control** La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento será eliminada cuando ya no sea necesaria.
Enmascaramiento de datos	**Control** El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas con el tema específico, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.

Prevención de fuga de datos	**Control** Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.
Copia de seguridad de la información	**Control** Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad específica del tema acordada.
Redundancia de las instalaciones de procesamiento de información	**Control** Las instalaciones de procesamiento de información se implementarán con suficiente redundancia para cumplir con los requisitos de disponibilidad.
Inicio sesión	**Control** Se producirán, almacenarán, protegerán y analizarán registros que registren actividades, excepciones, fallas y otros eventos relevantes.
Actividades de seguimiento	**Control** Las redes, los sistemas y las aplicaciones deberán ser monitoreados por comportamiento anómalo y se tomarán las acciones apropiadas para evaluar posibles incidentes de seguridad de la información.
Instalación de software en sistemas operativos	**Control** Se implementarán procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.
Seguridad en redes	**Control** Las redes y los dispositivos de red se asegurarán, administrarán y controlarán para proteger la información en los sistemas y aplicaciones.
Seguridad de los servicios de red.	**Control** Se identificarán, implementarán y controlarán los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.
Segregación de redes	**Control** Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización.
Filtrado web	**Control** El acceso a sitios web externos se gestionará para reducir la exposición a contenido malicioso.
Uso de criptografía	**Control** Se deben definir e implementar reglas para el uso efectivo de la criptografía, incluida la gestión de claves criptográficas.
Ciclo de vida de desarrollo seguro	**Control** Se establecerán y aplicarán reglas para el desarrollo seguro de software y sistemas.

Requisitos de seguridad de la aplicación	**Control** Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.
Principios de arquitectura e ingeniería de sistemas seguros	**Control** Se deben establecer, documentar, mantener y aplicar principios para la ingeniería de sistemas seguros en cualquier actividad de desarrollo de sistemas de información.
Codificación segura	**Control** Los principios de codificación segura se aplicarán al desarrollo de software.
Pruebas de seguridad en desarrollo y aceptación.	**Control** Los procesos de pruebas de seguridad se definirán e implementarán en el ciclo de vida del desarrollo.
Separación de los entornos de desarrollo, prueba y producción	**Control** Los entornos de desarrollo, prueba y producción deben estar separados y protegidos.
Gestión del cambio	**Control** Los cambios en las instalaciones de procesamiento de información y los sistemas de información estarán sujetos a procedimientos de gestión de cambios.
Información de prueba	**Control** La información de las pruebas se seleccionará, protegerá y gestionará adecuadamente.
Protección de los sistemas de información durante las pruebas de auditoría	**Control** Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos deben planificarse y acordarse entre el evaluador y la gerencia correspondiente.

Fuente: ISO 27001:2022

COBIT 5 Procesos catalizadores

Este modelo de gestión de seguridad[20] propone dos procesos catalizadores, que al aplicarlos de manera adecuada contribuyen con la seguridad informática de las empresas.

Tabla 2

Procesos Catalizadores COBIT5

PROCESO	DESCRIPCIÓN	PRACTICAS CLAVES DEL PROCESO
DSS05 Gestionar Servicios de Seguridad	Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.	**DSS05.01** Proteger contra software malicioso. **DSS05.02** Gestionar la seguridad de la red y las conexiones. **DSS05.03** Gestionar la seguridad de los puestos de usuario final. **DSS05.04** Gestionar la identidad del usuario y el acceso lógico. **DSS05.05** Gestionar el acceso físico a los activos de TI. **DSS05.06** Gestionar documentos sensibles y dispositivos de salida. **DSS05.07** Supervisar la infraestructura para detectar eventos relacionados con la seguridad
APO13 Gestionar la seguridad	Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.	**APO13.01** Establecer y mantener un SGSI. **APO13.02** Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información. **APO13.03** Supervisar y revisar el SGSI.

Fuente: Procesos Cobit5.

3 Capítulo III: Metodología

3.1 Tipo de investigación

La investigación es de tipo cualitativo, dado que se utiliza la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación y puede o no probar hipótesis en su proceso de interpretación [21].

El enfoque cualitativo se selecciona cuando se busca comprender la perspectiva de los participantes (individuos o grupos pequeños de personas a los que se investigará) acerca de los fenómenos que los rodean, profundizar en sus experiencias, perspectivas, opiniones y significados, es decir, la forma en que los participantes perciben subjetivamente su realidad. También es recomendable seleccionar el enfoque cualitativo cuando el tema del estudio ha sido poco explorado, o no se ha hecho investigación al respecto en algún grupo social específico. El proceso cualitativo inicia con la idea de investigación [21].

Para el desarrollo de la investigación se utiliza la investigación primaria o de campo el cual consiste en obtener de la población una muestra y así conocer toda aquella información que se requiere para determinar si la implementación de un modelo integral de políticas de seguridad y gestión de la información mejorará la efectividad de las organizaciones para proteger sus activos digitales y reducir el riesgo de brechas de seguridad, en las cooperativas de ahorro y crédito del municipio de San Vicente, departamento de San Vicente, El Salvador. (Ver Anexo 1).

En cuanto a la investigación secundaria o bibliográfica, se procede a la búsqueda de información en libros (físicos o virtuales), tesis, folletos, revistas científicas, diccionarios y otros relacionados con la investigación, a efecto de obtener un fundamento teórico para el desarrollo de esta investigación.

3.2 Población y muestra

Población: una población es el conjunto de todos los casos que concuerdan con una serie de especificaciones [21].

La población de la que se obtiene los datos para esta investigación es de las cooperativas de ahorro y crédito del municipio de san Vicente, específicamente con los encargados del área de TI(Tecnología e Información) o en su defecto el área de ciberseguridad con el propósito de determinar si la implementación de un modelo integral de políticas de seguridad y gestión de la información mejorará la efectividad de las organizaciones para proteger sus activos digitales y reducir el riesgo de brechas de seguridad.

Para esta investigación se ha tomado a consideración la totalidad de la población, en este caso son seis las cooperativas de ahorro y crédito, siendo estas ACCESO DE R.L., CAJA DE CRÉDITO SAN VICENTE, ACAASS SAN VICENTE, BANCOVI DE R.L., CREDICAMPO, ACODJAR de R.L.

Tabla 3

Población encuestada

N.	INSTITUCIÓN	# ENCUESTAS
1	ACCESO DE R.L	Por seguridad no dieron permiso
2	CAJA DE CRÉDITO SAN VICENTE	Por seguridad no dieron permiso
3	ACAASS SAN VICENTE	1
4	BANCOVI DE R.L.	Por seguridad no dieron permiso
5	CREDICAMPO	5
6	ACODJAR DE R.L.	5

La cantidad de personas encuestadas **N=11**.

3.3 Técnica e instrumento

La técnica que se utiliza es la encuesta y como instrumento de recolección de datos es el cuestionario que contiene preguntas cerradas para su análisis, este instrumento va dirigido al personal clave de las organizaciones, tales como gerentes de tecnologías, jefaturas de informática, jefes de ciberseguridad, para que con sus respuestas se puedan alcanzar los objetivos planteados en la investigación (Ver Anexo 1).

3.4 Procedimiento

El proceso de investigación consta de una serie de pasos que se detallan a continuación [21].

Paso 1: Planteamiento del problema, revisión de la literatura, inmersión en el campo

Una vez concebida la idea del estudio, el investigador debe familiarizarse con el tema en cuestión. Aunque el enfoque cualitativo es inductivo, necesitamos conocer con mayor profundidad el “terreno que estamos pisando”. Esto se refiere a dos aspectos:

- Revisión de la literatura

En los estudios cualitativos sí se revisa la literatura, aunque al inicio menos intensivamente que en la investigación cuantitativa. La literatura es útil para:

1. Detectar conceptos claves que no habíamos pensado.
2. Nutrirnos de ideas en cuanto a métodos de recolección de datos y análisis, respecto de cómo les han servido a otros.
3. Tener en mente los errores que otros han cometido anteriormente.
4. Conocer diferentes maneras de pensar y abordar el planteamiento.
5. Mejorar el entendimiento de los datos y profundizar las interpretaciones.

- Inmersión en el campo

Una vez que hemos elegido un ambiente, contexto o lugar apropiado, comenzamos la tarea de responder a las preguntas de investigación. El ambiente puede ser tan variado como el planteamiento del problema. Y el contexto implica una definición geográfica, pero es inicial, puesto que puede variar, ampliarse o reducirse.

Paso 2: Muestreo

Según Mertens[22], señala que en el muestreo cualitativo es usual comenzar con la identificación de ambientes propicios, luego de grupos y, finalmente, de individuos. Incluso, la muestra puede ser una sola unidad de análisis (estudio de caso). La investigación cualitativa, por sus características, requiere de muestras más flexibles.

Paso 3: Recolección y análisis de datos

Para el enfoque cualitativo, la recolección de datos resulta fundamental, lo que se busca en un estudio cualitativo es obtener datos (que se convertirán en información) de personas, seres vivos, comunidades, contextos o situaciones en profundidad; en las propias “formas de expresión” de cada uno de ellos.

La recolección de datos ocurre en los ambientes naturales y cotidianos de los participantes o unidades de análisis.

- Construcción de instrumentos

Se elaborarán los instrumentos destinados a recabar información de los directivos de las áreas de TI o ciberseguridad, tomando como base fundamental los objetivos planteados en la investigación y así poder dar operatividad a estos, de tal manera que se pueda conocer mediante la información brindada por los sujetos de estudio en cuanto a la efectividad de las organizaciones para proteger sus activos digitales y reducir el riesgo de brechas de seguridad.

- Análisis de los datos

El análisis de los datos es posterior a la recolección y tabulación de los mismos, para poder tomar decisiones con respectos a las respuestas brindadas por el espacio muestral.

Paso 4: Reporte de resultados

Estos reportes también deben ofrecer una respuesta al planteamiento del problema y fundamentar las estrategias que se usaron para abordarlo, así como los datos que fueron recolectados, analizados e interpretados por el investigador.

Paso 5: Divulgación de la investigación

Se elaborará el informe que contiene el proceso y los resultados obtenidos en la investigación, también, serán mostrados a través de una defensa final del Trabajo de Investigación, exponiendo los aspectos importantes encontrados.

3.5 Análisis estadístico o de información

El vaciado de la información será por medio del programa de Microsoft Excel 2019, esto con el fin de digitalizar las respuestas de los sujetos encuestados; al mismo tiempo para tener un respaldo para posibles consultas posteriores, y hacer uso de las características de este

programa en cuanto a la generación de gráficos que permitirán el análisis de la información recopilada.

4 Capítulo IV: Resultados

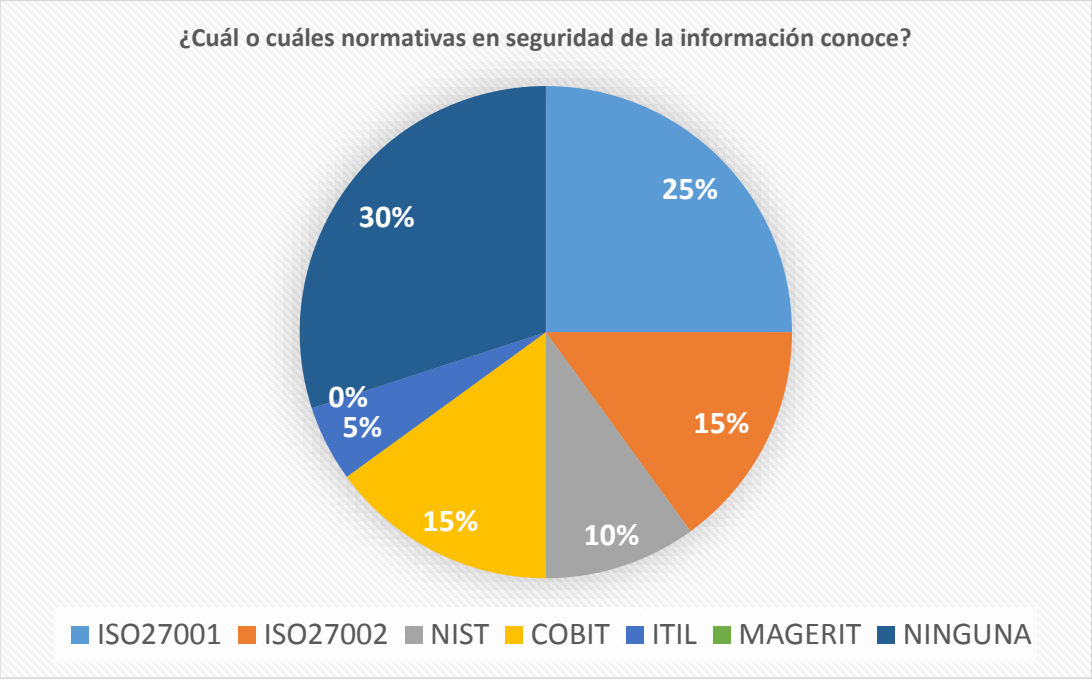
Para dar cumplimiento al objetivo de la investigación “Proponer modelo de políticas de seguridad y gestión de la información, a las cooperativas de Ahorro y Crédito del municipio de San Vicente, departamento de San Vicente, de acuerdo a la norma ISO 27001”, se plantearon objetivos específicos; con el fin de lograr cada uno de estos apartados se identificaron unidades de análisis o sujetos involucrado en el campo de estudio, de los cuales se obtuvieron información por medio del instrumento cuestionario.

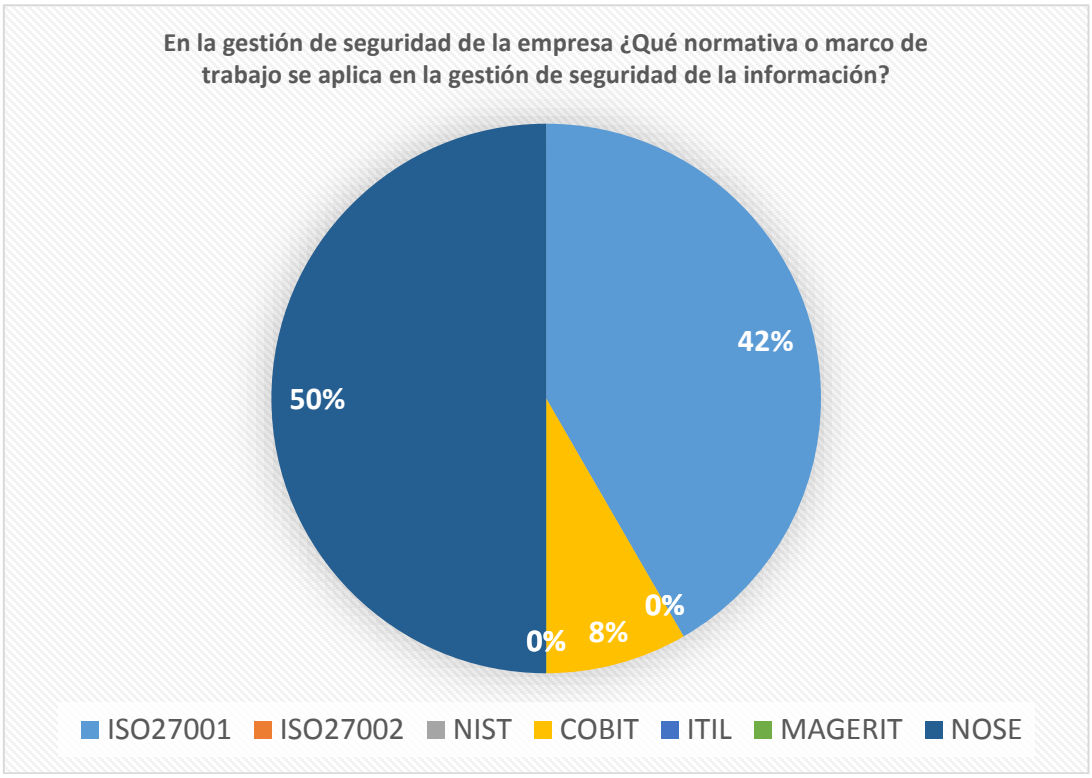
4.1 Análisis de la información

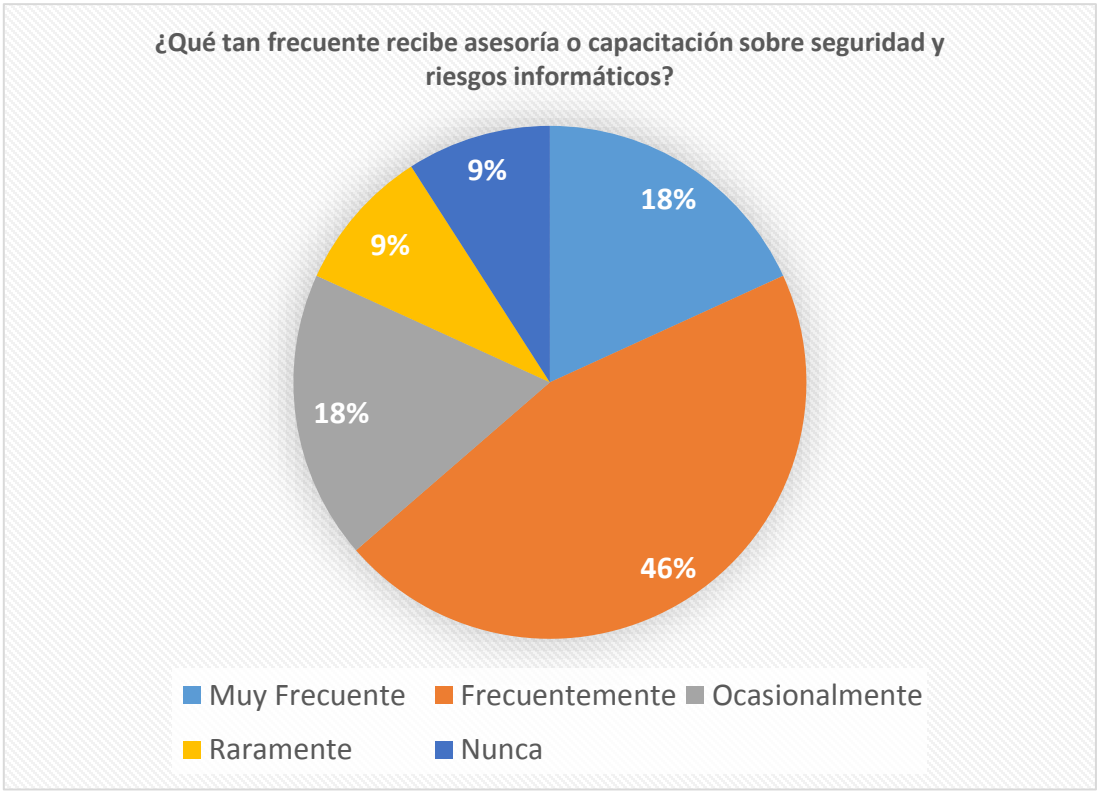
Objetivo Específico	# Preguntas del Cuestionario
Desarrollar el marco teórico relacionado a los modelos de políticas de seguridad actuales aplicables al sector financiero.	2
Proponer una política de gestión de la seguridad de la información de acuerdo con la ISO 27001 aplicables a las actividades de las cooperativas de Ahorro y Crédito del municipio de San Vicente, departamento de San Vicente.	13
Plantear una Política de control de acceso, que garantice que el acceso a la información sea autorizado y gestionado adecuadamente.	6
Definir políticas de auditoría y revisión que garanticen la eficacia continua de las medidas de seguridad.	4

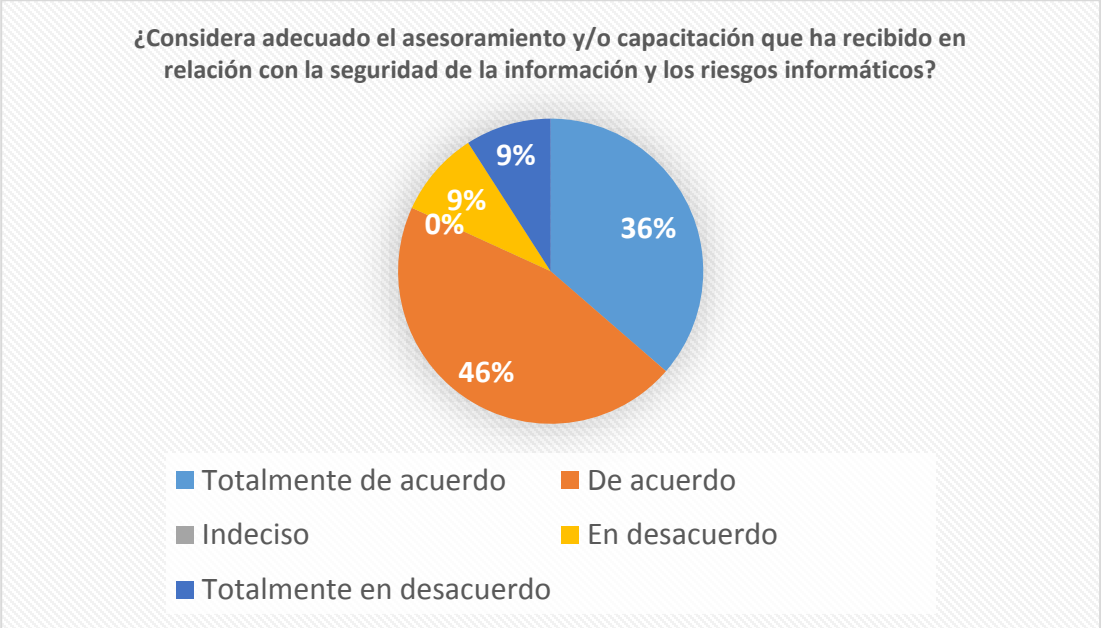
Establecer modelos y controles para el manejo de información sensible dentro de la cooperativa en función de la norma ISO 27001 y estándares que sean aplicables a la seguridad de la información y protección a ciberataques.	5

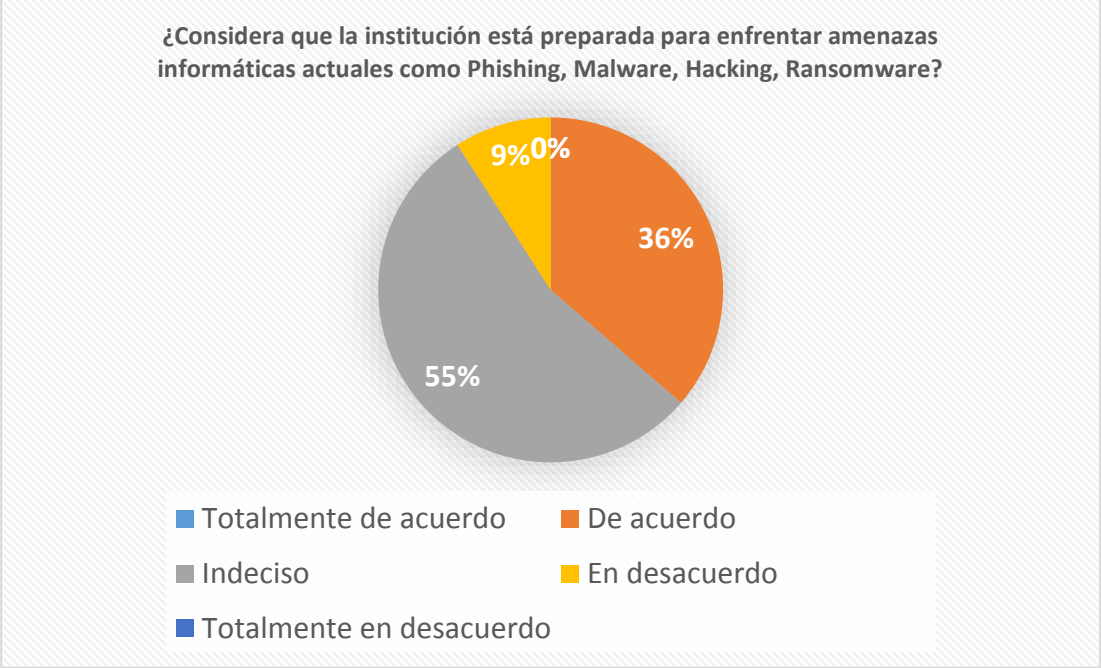
De la aplicación de las encuestas se determinaron los siguientes resultados, según los siguientes indicadores:

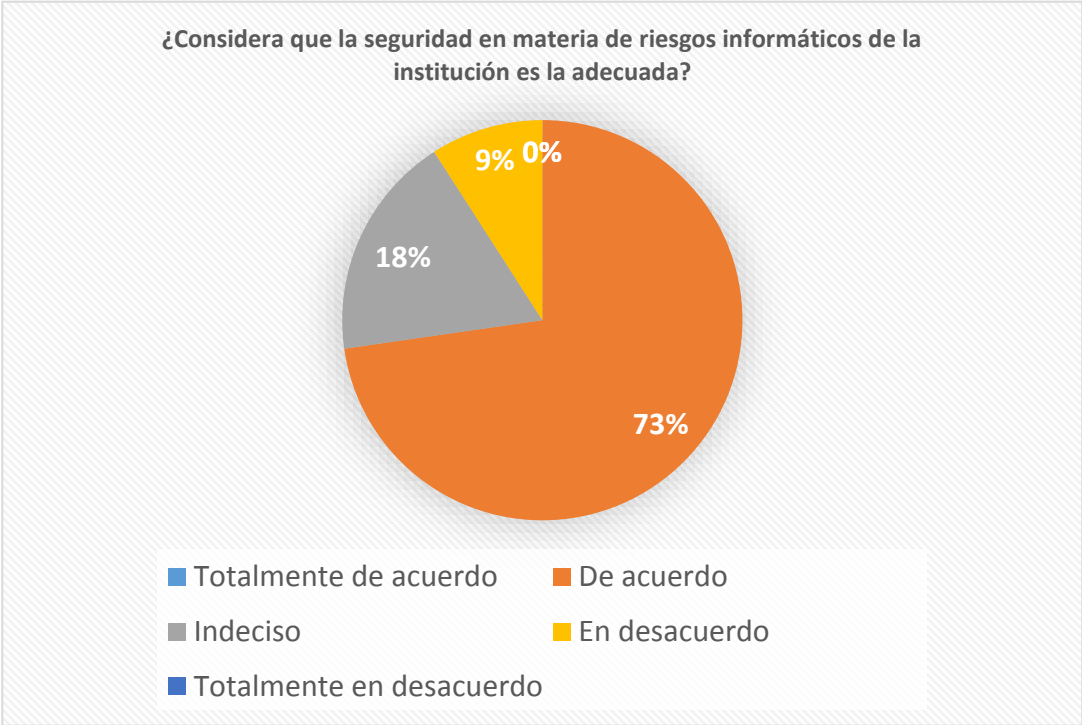


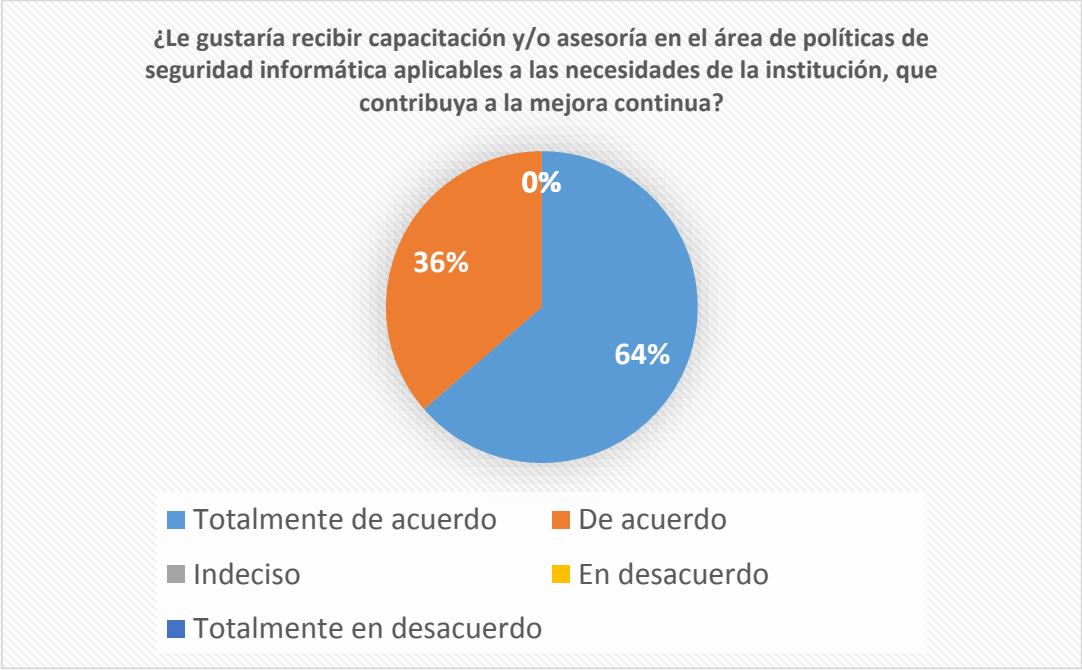

En la gestión de seguridad de la empresa ¿Qué normativa o marco de trabajo se aplica en la gestión de seguridad de la información?
42%
0%
8%
0%
50%
ISO27001
ISO27002
NIST
COBIT
ITIL
MAGERIT
NOSE

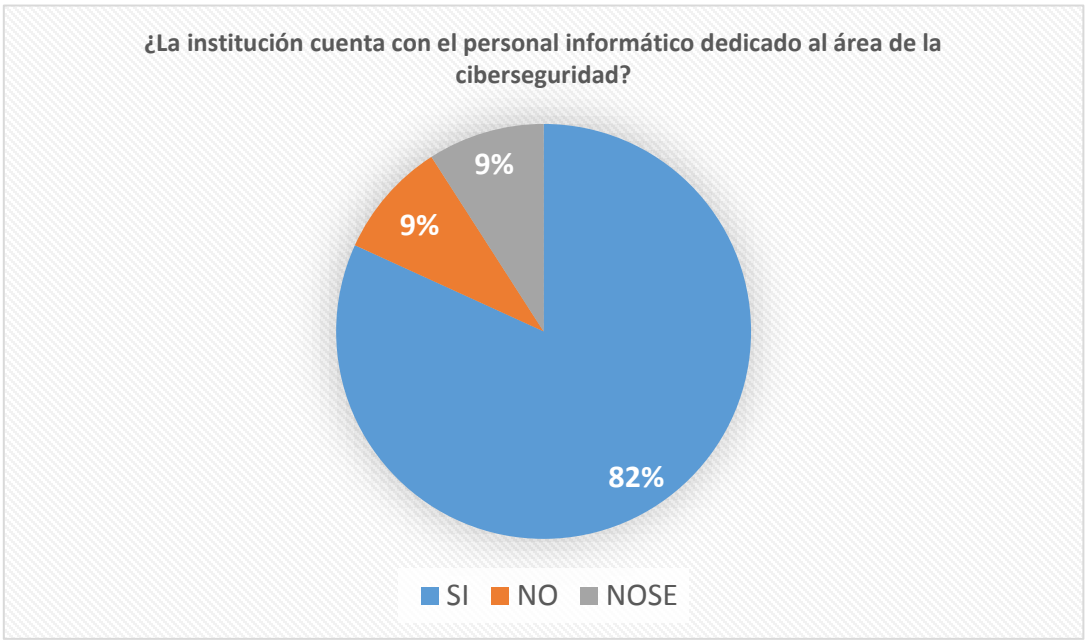

¿Qué tan frecuente recibe asesoría o capacitación sobre seguridad y riesgos informáticos?
18%
46%
18%
9%
9%
Muy Frecuente
Frecuentemente
Ocasionalmente
Raramente
Nunca

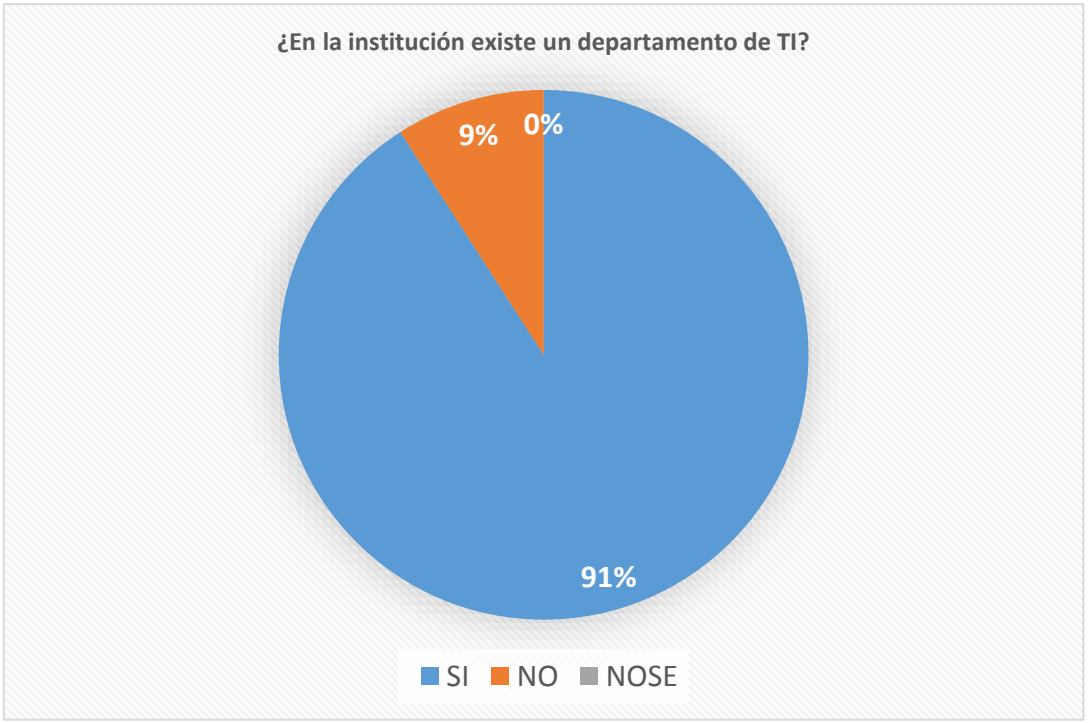

¿Considera adecuado el asesoramiento y/o capacitación que ha recibido en relación con la seguridad de la información y los riesgos informáticos?
9%
9%
0%
36%
46%
Totalmente de acuerdo
De acuerdo
Indeciso
En desacuerdo
Totalmente en desacuerdo

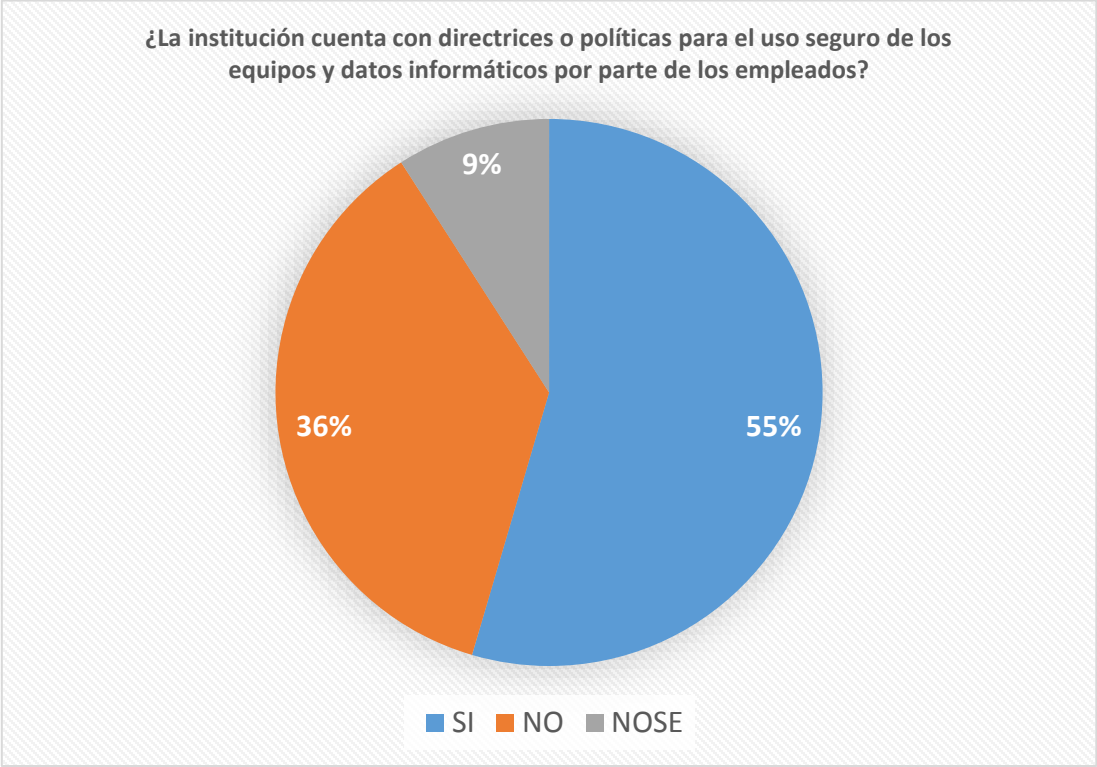

¿Considera que la institución está preparada para enfrentar amenazas informáticas actuales como Phishing, Malware, Hacking, Ransomware?
9%
0%
36%
55%
Totalmente de acuerdo
De acuerdo
Indeciso
En desacuerdo
Totalmente en desacuerdo

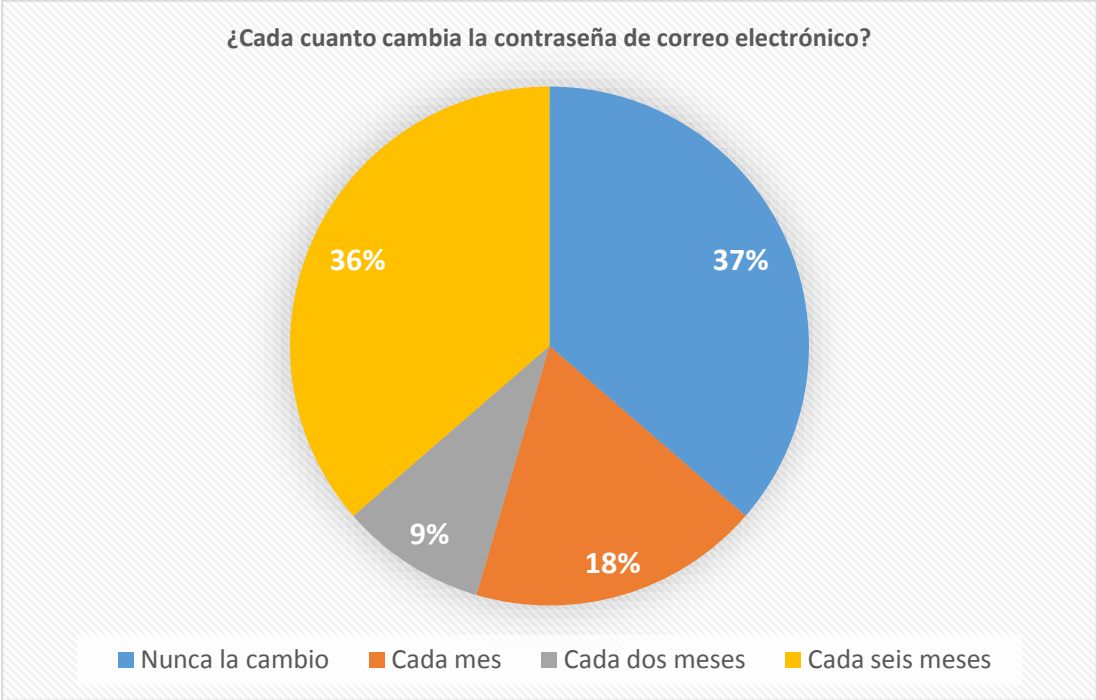

¿Considera que la seguridad en materia de riesgos informáticos de la institución es la adecuada?
9%
0%
18%
73%
Totalmente de acuerdo
De acuerdo
Indeciso
En desacuerdo
Totalmente en desacuerdo


¿Le gustaría recibir capacitación y/o asesoría en el área de políticas de seguridad informática aplicables a las necesidades de la institución, que contribuya a la mejora continua?
0%
36%
64%
Totalmente de acuerdo
De acuerdo
Indeciso
En desacuerdo
Totalmente en desacuerdo

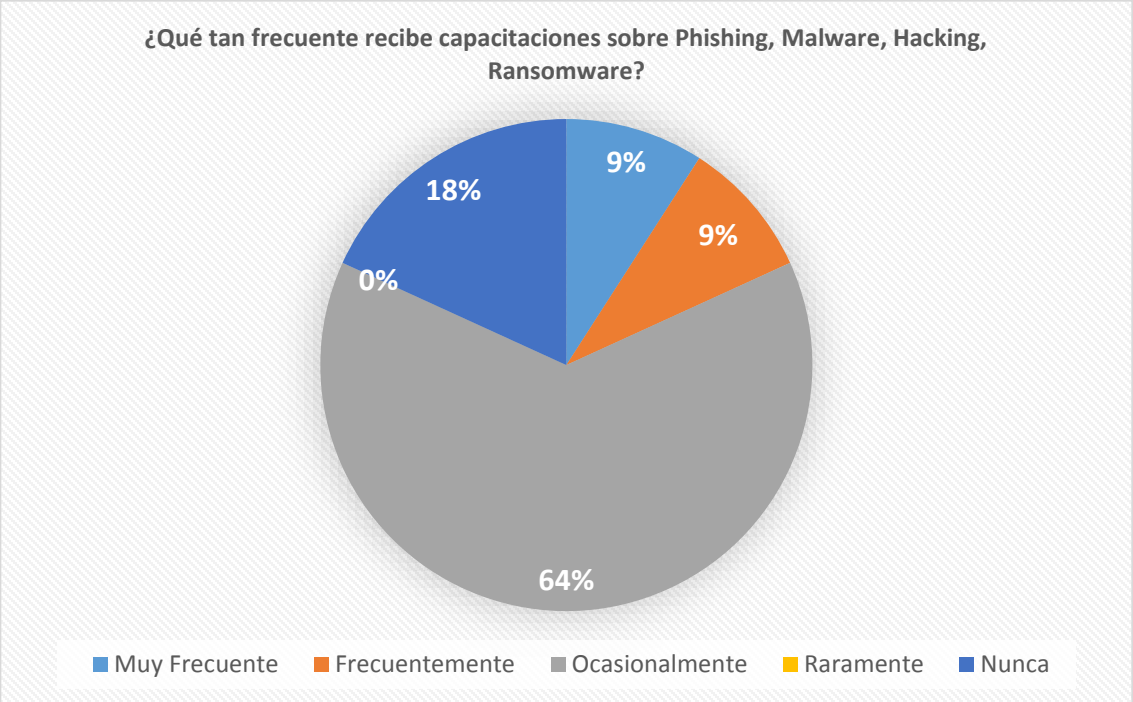

¿La institución cuenta con el personal informático dedicado al área de la ciberseguridad?
9%
9%
82%
SI
NO
NOSE

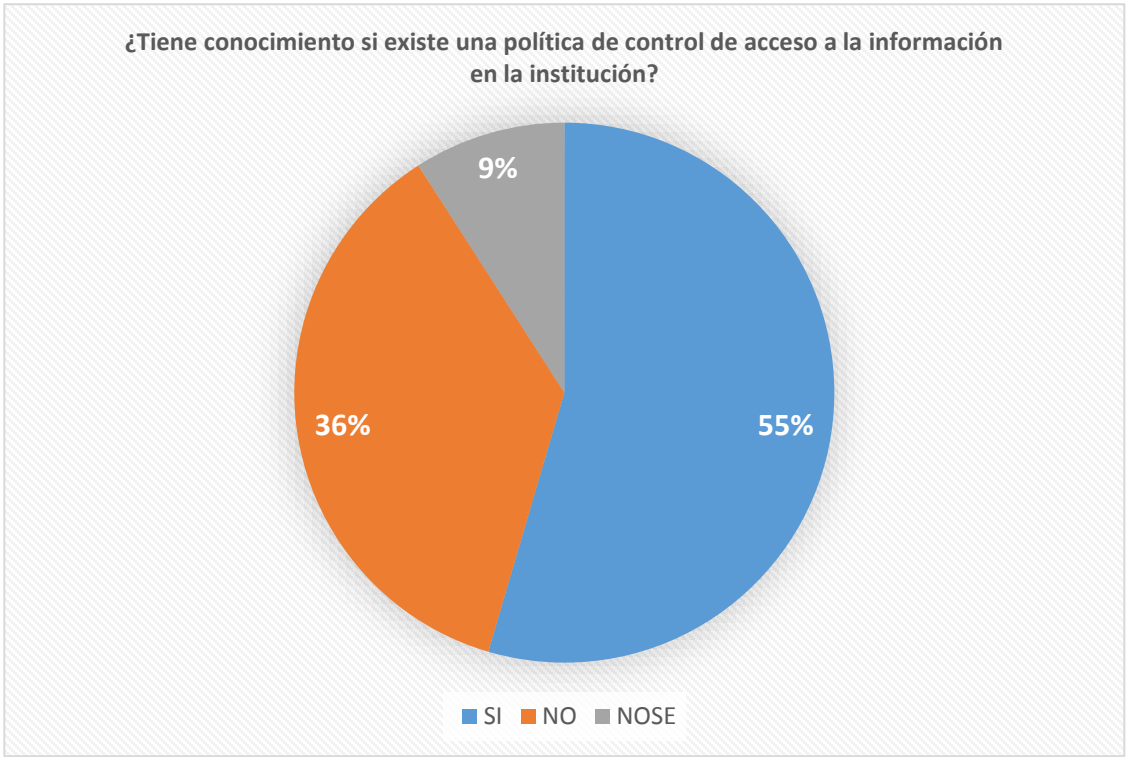

¿En la institución existe un departamento de TI?
9%
0%
91%
SI
NO
NOSE

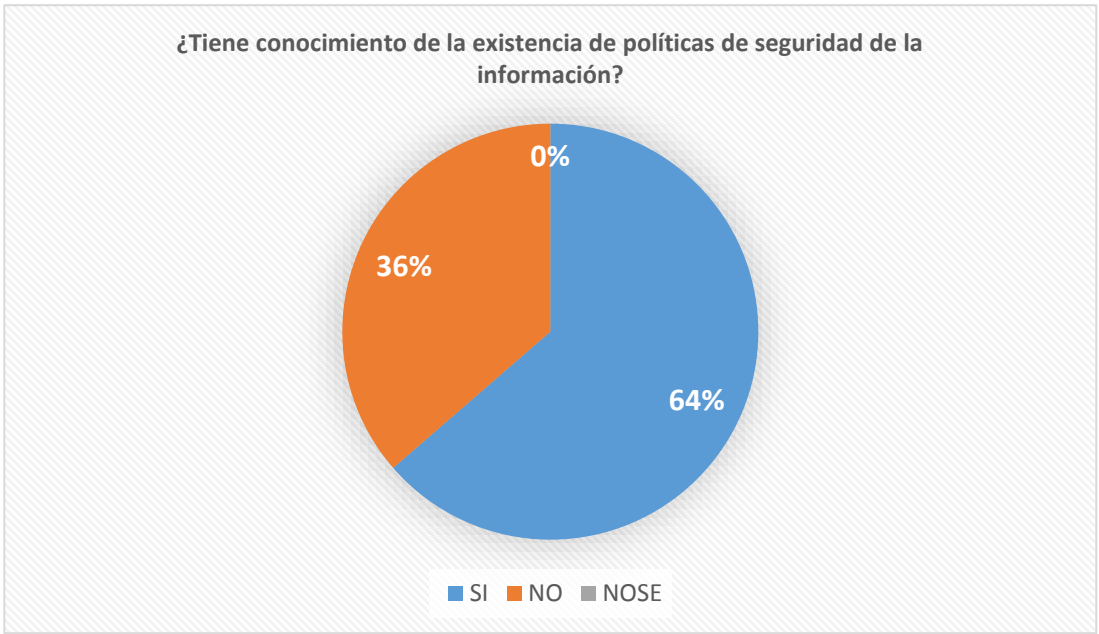

¿La institución cuenta con directrices o políticas para el uso seguro de los equipos y datos informáticos por parte de los empleados?
9%
36%
55%
SI
NO
NOSE

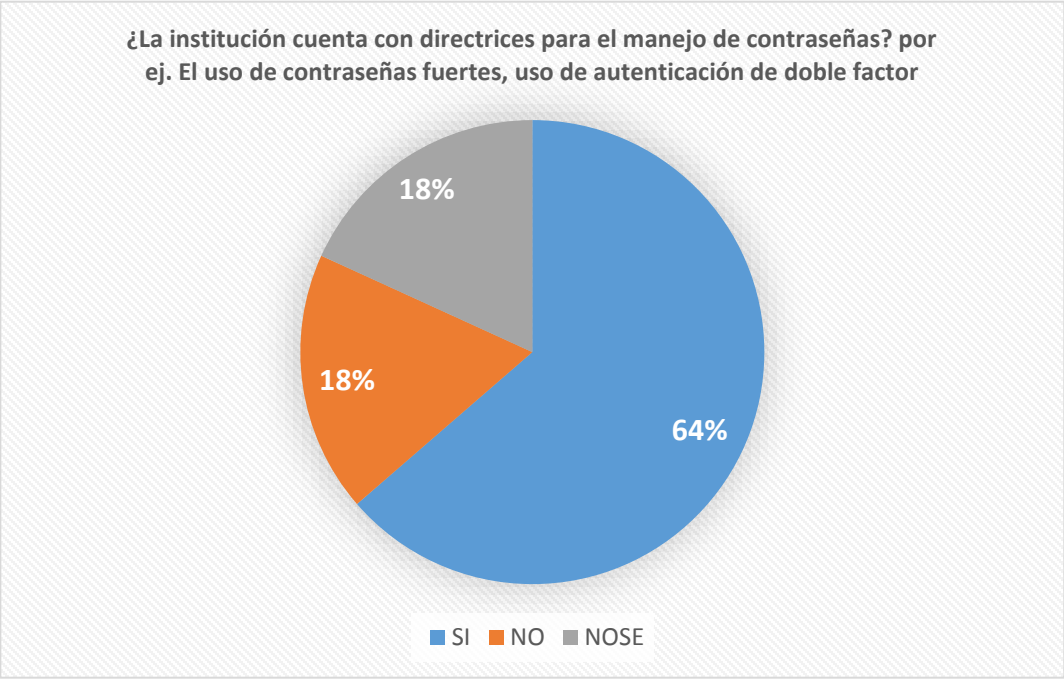

¿Cada cuanto cambia la contraseña de correo electrónico?
36%
37%
9%
18%
Nunca la cambio
Cada mes
Cada dos meses
Cada seis meses

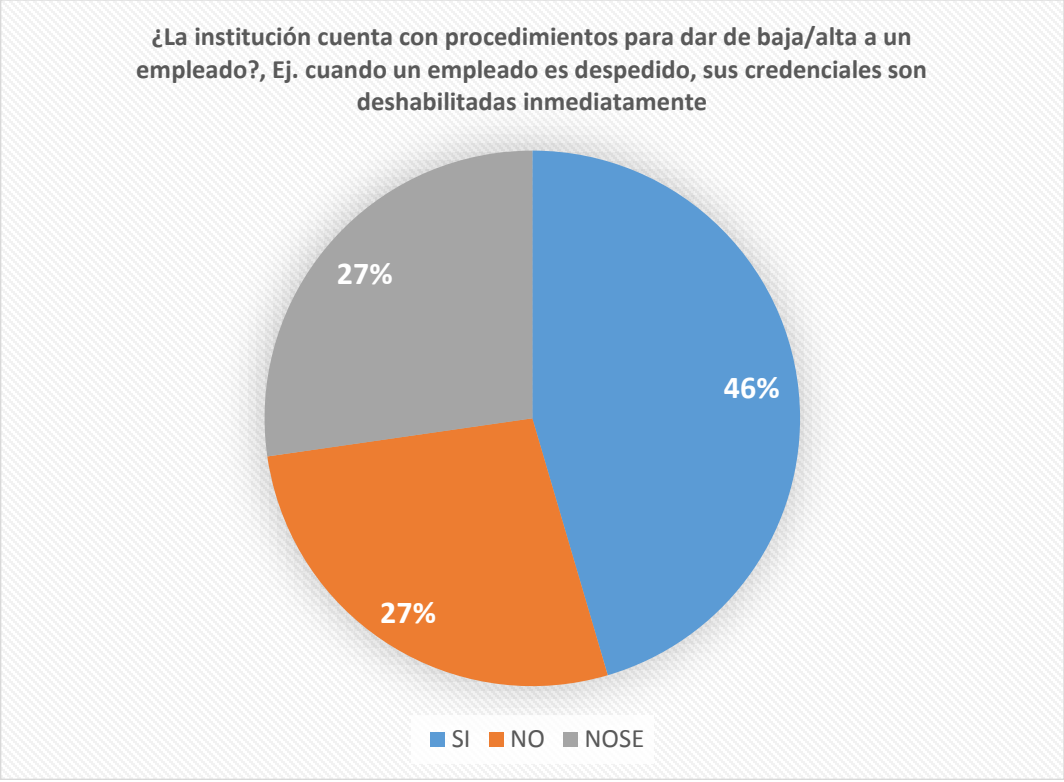

¿Qué método usa para NO olvidar las contraseñas?
0%
11%
0%
33%
56%
La anoto en un papelito
La escribo en el escritorio de la computadora
La tego escrita en la cartera
Uso un baúl de contraseñas
Uso una contraseña maestra

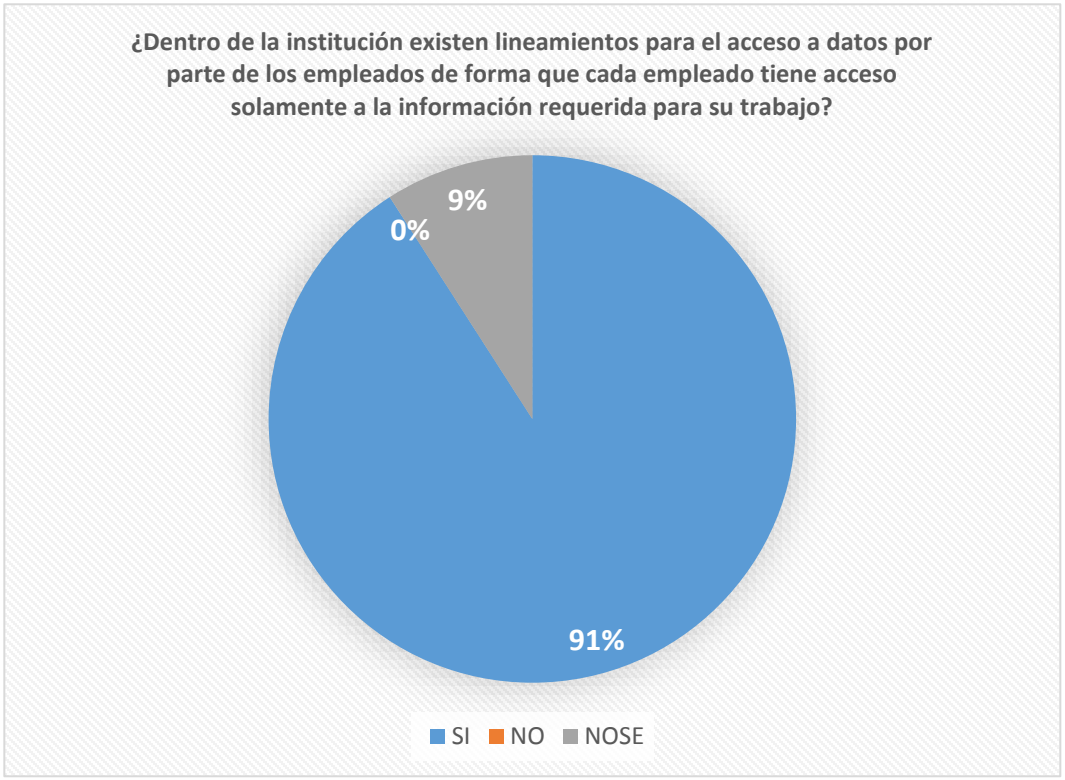

¿Qué tan frecuente recibe capacitaciones sobre Phishing, Malware, Hacking, Ransomware?
9%
9%
0%
18%
64%
Muy Frecuente
Frecuentemente
Ocasionalmente
Raramente
Nunca

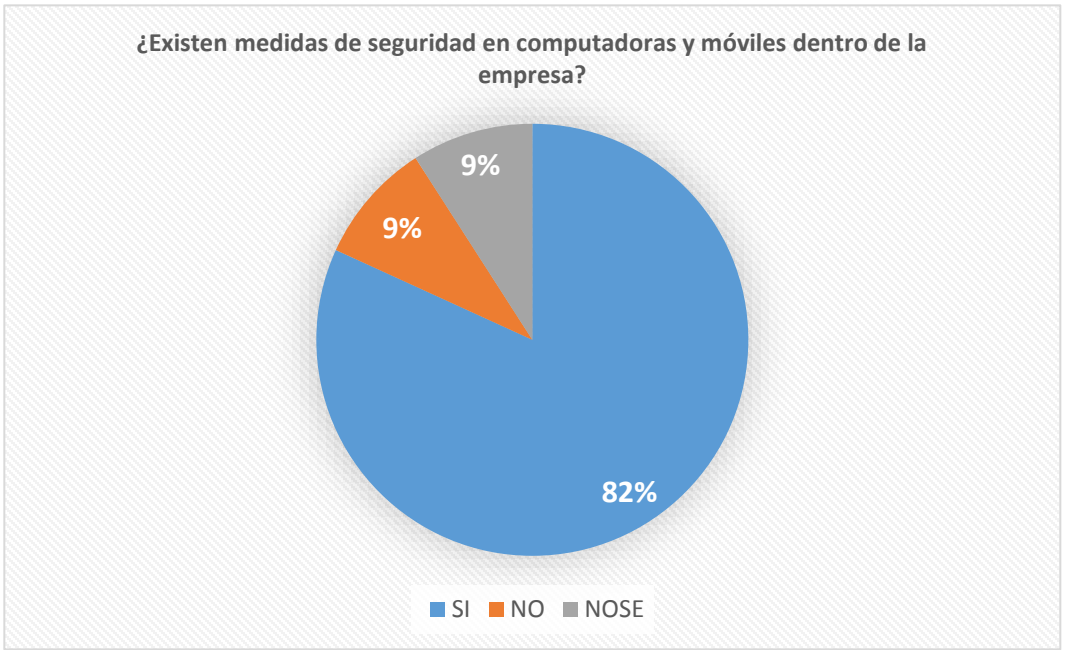

¿Tiene conocimiento si existe una política de control de acceso a la información en la institución?
9%
36%
55%
SI
NO
NOSE

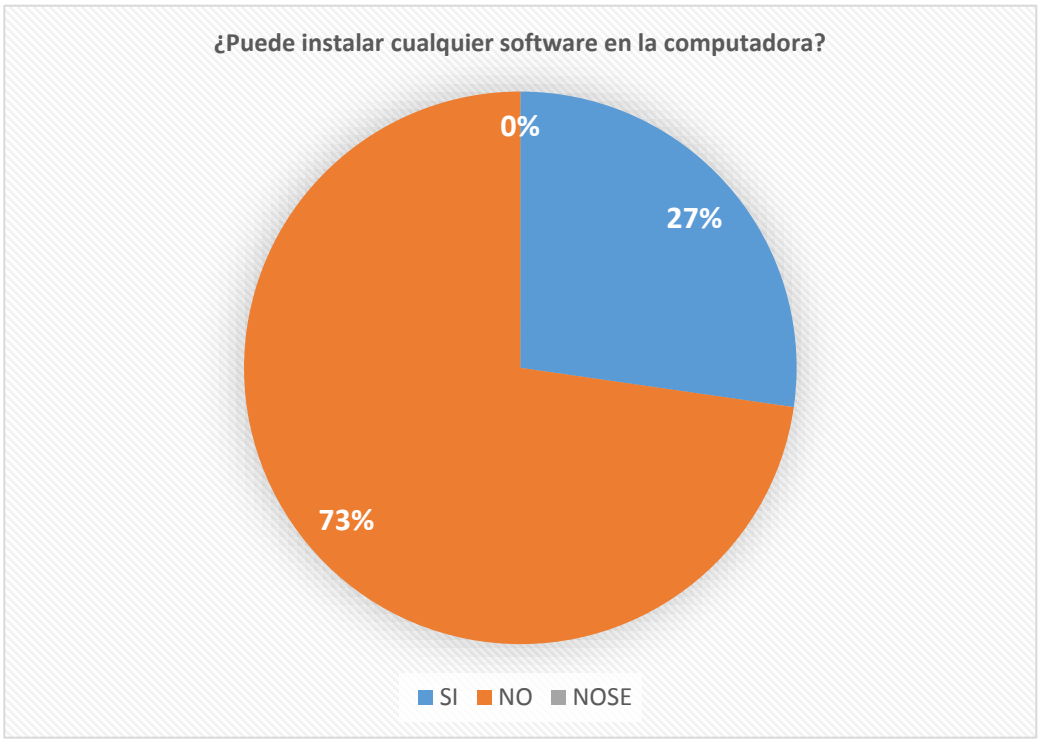

¿Tiene conocimiento de la existencia de políticas de seguridad de la información?
0%
36%
64%
SI
NO
NOSE

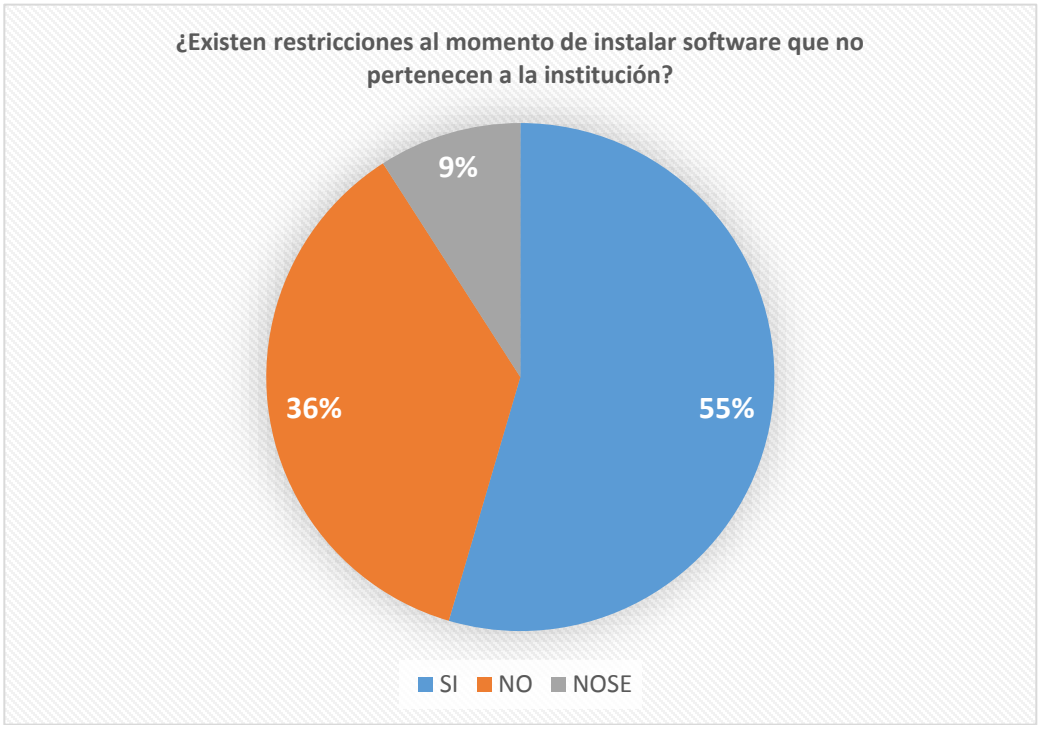

¿La institución cuenta con directrices para el manejo de contraseñas? por ej. El uso de contraseñas fuertes, uso de autenticación de doble factor
18%
18%
64%
SI
NO
NOSE

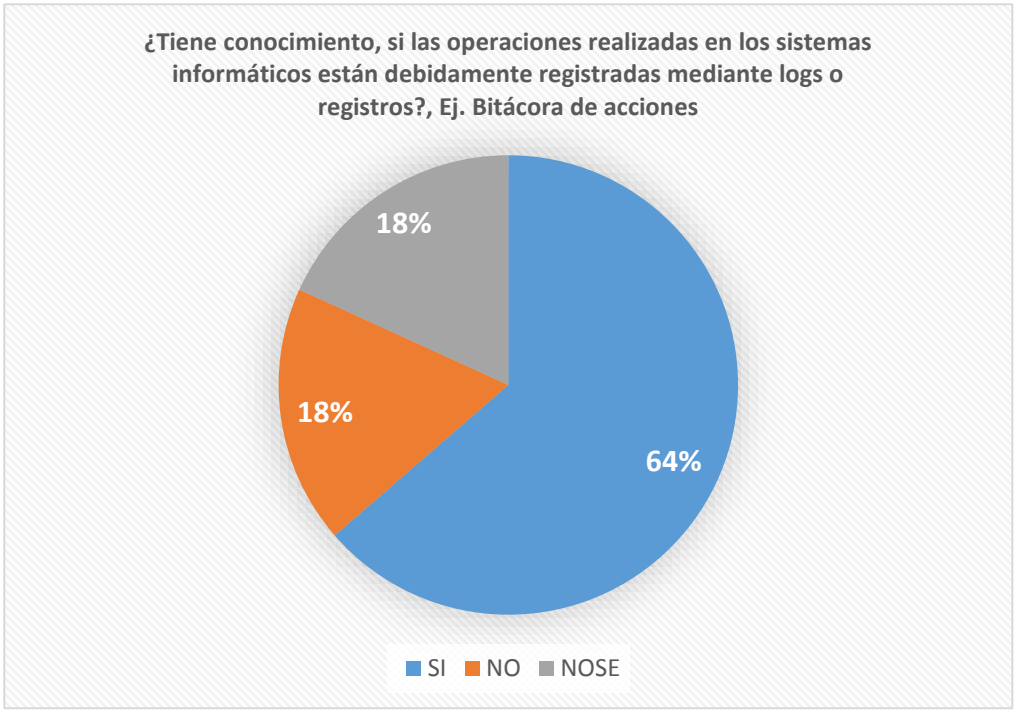

¿La institución cuenta con procedimientos para dar de baja/alta a un empleado?, Ej. cuando un empleado es despedido, sus credenciales son deshabilitadas inmediatamente
27%
46%
27%
SI
NO
NOSE

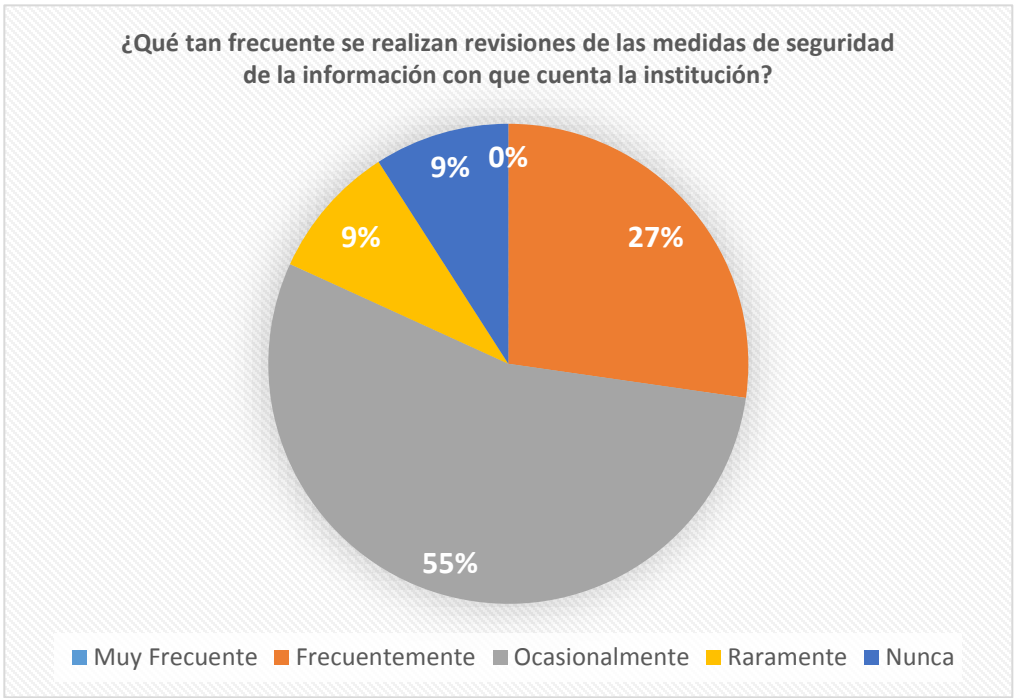

¿Dentro de la institución existen lineamientos para el acceso a datos por parte de los empleados de forma que cada empleado tiene acceso solamente a la información requerida para su trabajo?
9%
0%
91%
SI
NO
NOSE

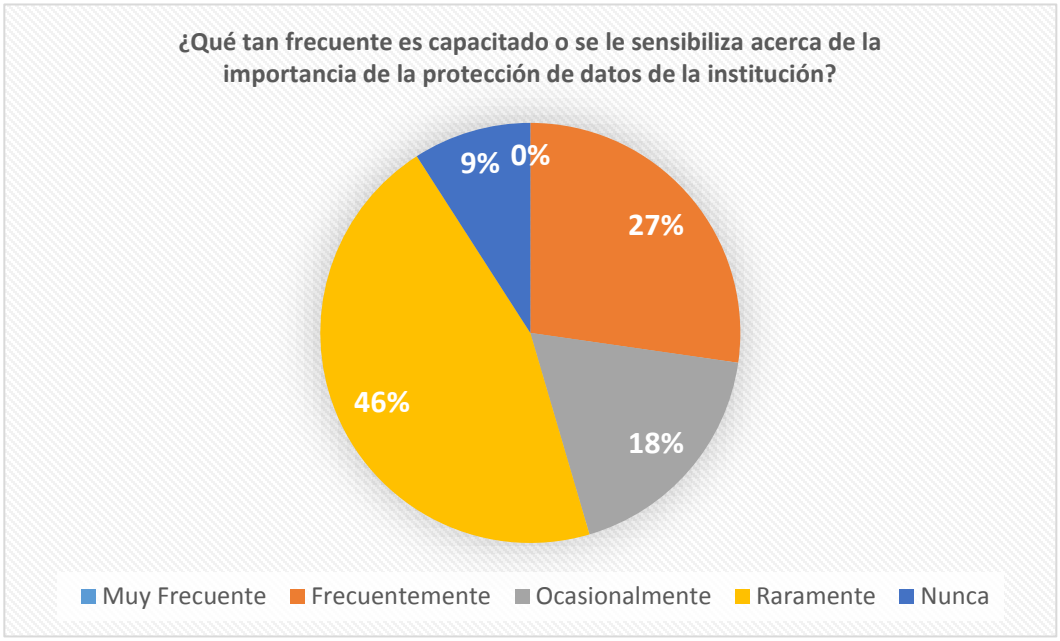

¿Existen medidas de seguridad en computadoras y móviles dentro de la empresa?
9%
9%
82%
SI
NO
NOSE

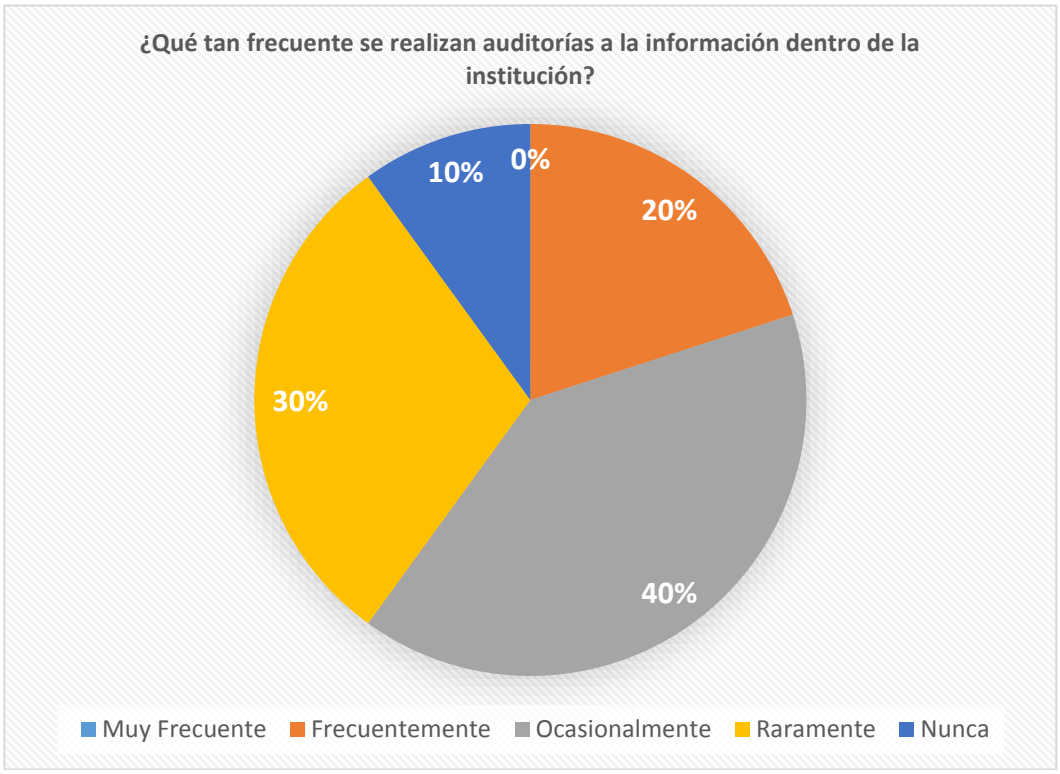

¿Puede instalar cualquier software en la computadora?
0%
27%
73%
SI
NO
NOSE

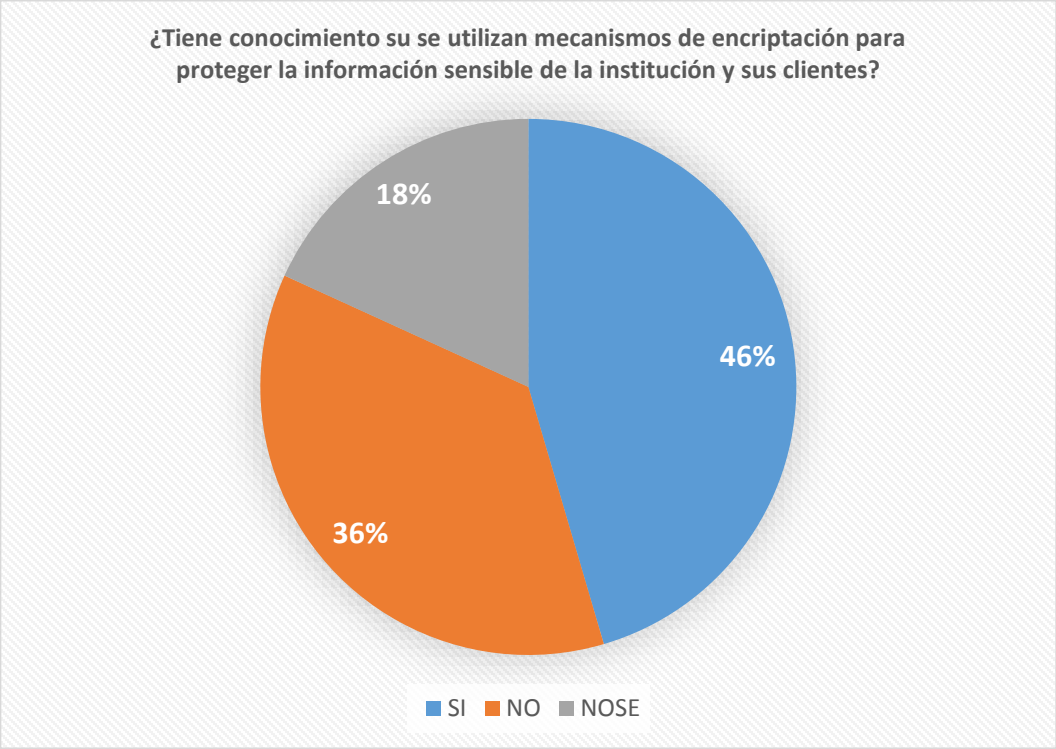

¿Existen restricciones al momento de instalar software que no pertenecen a la institución?
9%
36%
55%
SI
NO
NOSE

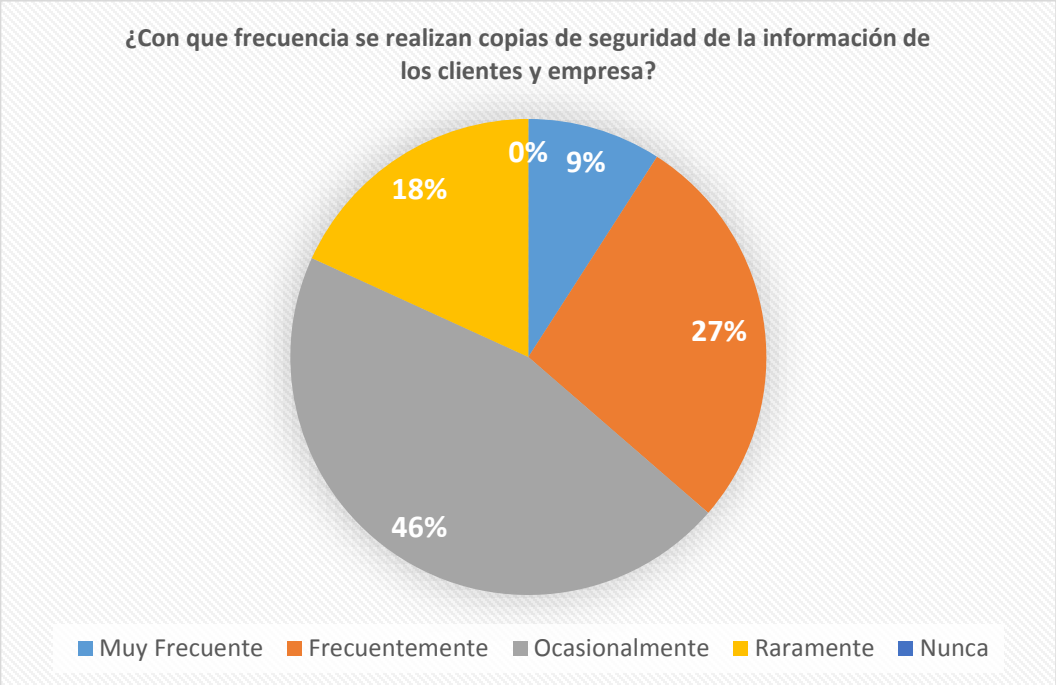

¿Tiene conocimiento, si las operaciones realizadas en los sistemas informáticos están debidamente registradas mediante logs o registros?, Ej. Bitácora de acciones
18%
18%
64%
SI
NO
NOSE

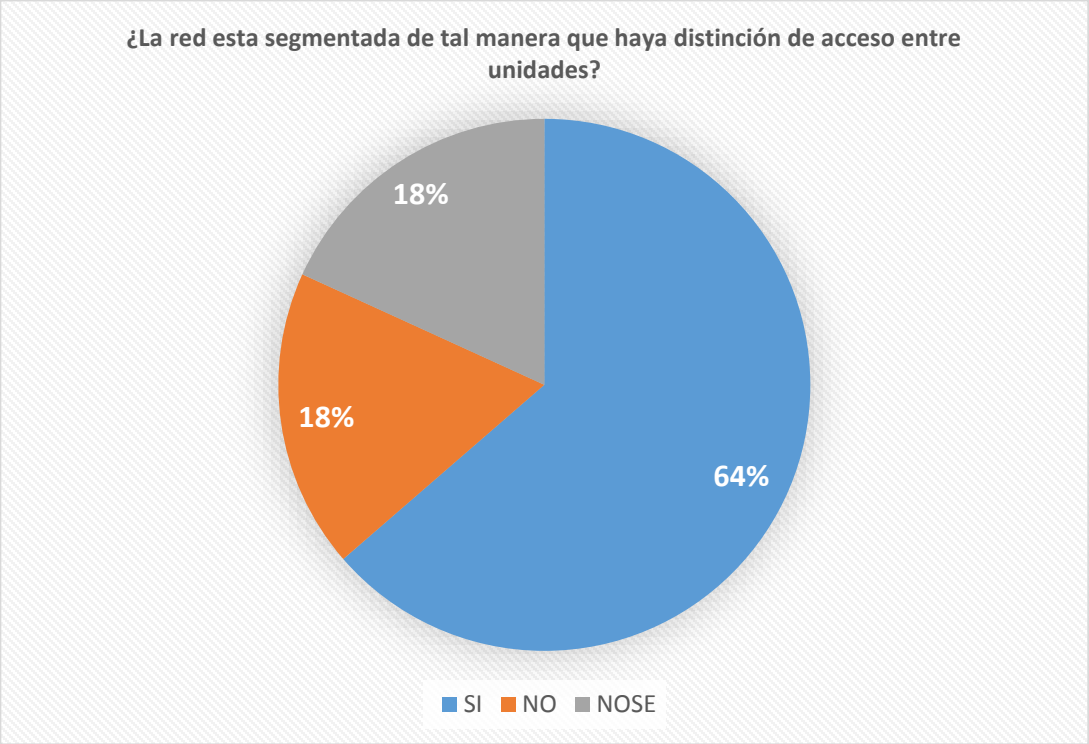

¿Qué tan frecuente se realizan revisiones de las medidas de seguridad de la información con que cuenta la institución?
9%
0%
27%
9%
55%
Muy Frecuente
Frecuentemente
Ocasionalmente
Raramente
Nunca

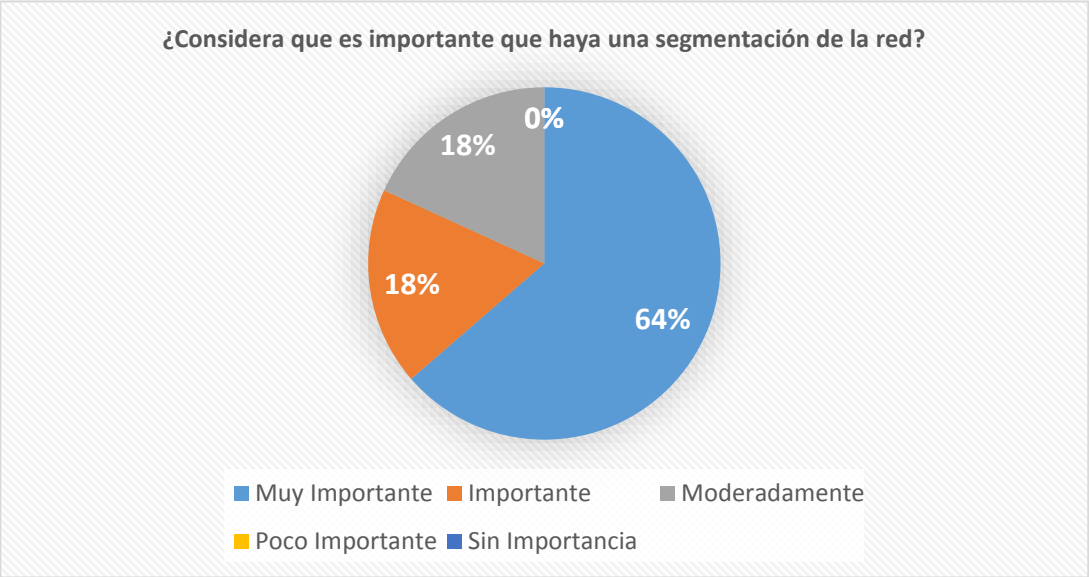

¿Qué tan frecuente es capacitado o se le sensibiliza acerca de la importancia de la protección de datos de la institución?
0%
27%
18%
46%
9%
Muy Frecuente
Frecuentemente
Ocasionalmente
Raramente
Nunca

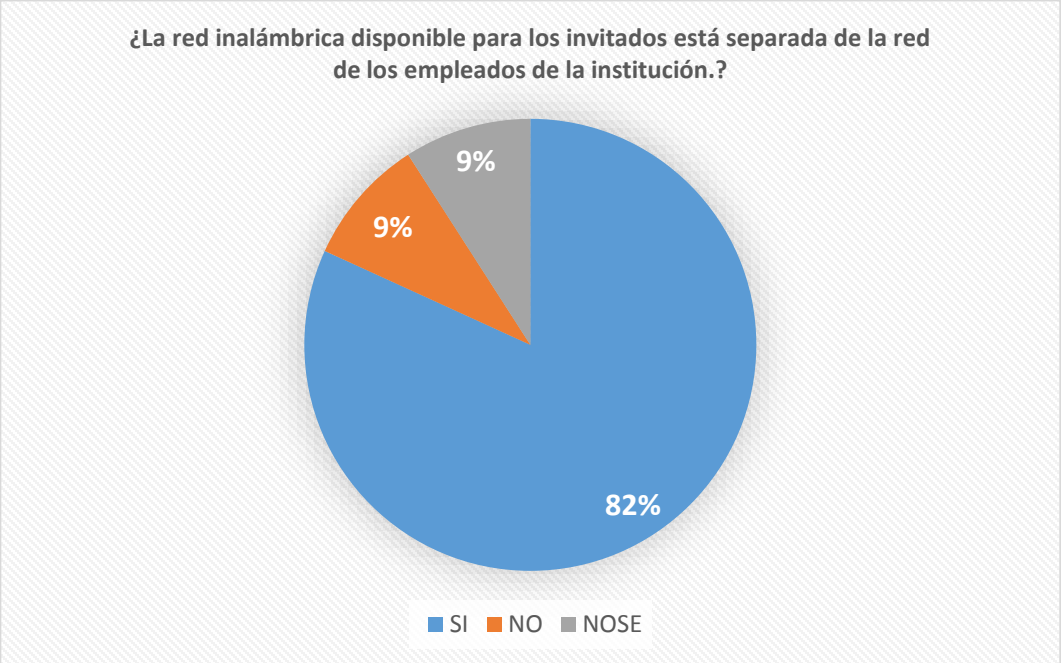

¿Qué tan frecuente se realizan auditorías a la información dentro de la institución?
0%
20%
40%
30%
10%
Muy Frecuente
Frecuentemente
Ocasionalmente
Raramente
Nunca


¿Tiene conocimiento su se utilizan mecanismos de encriptación para proteger la información sensible de la institución y sus clientes?
18%
46%
36%
SI
NO
NOSE


¿Con que frecuencia se realizan copias de seguridad de la información de los clientes y empresa?
0%
9%
18%
27%
46%
Muy Frecuente
Frecuentemente
Ocasionalmente
Raramente
Nunca


¿La red esta segmentada de tal manera que haya distinción de acceso entre unidades?
18%
18%
64%
SI
NO
NOSE


¿Considera que es importante que haya una segmentación de la red?
0%
18%
18%
64%
Muy Importante
Importante
Moderadamente
Poco Importante
Sin Importancia



Análisis según objetivos

Objetivo 1: Desarrollar el marco teórico relacionado a los modelos de políticas de seguridad actuales aplicables al sector financiero.

Es relevante observar que la normativa ISO 27001 es ampliamente conocida y aplicada en el ámbito de la seguridad de la información. Esto puede deberse a su amplio reconocimiento internacional y su enfoque integral para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información.

La baja aplicación de normativas como NIST y MAGERIT puede deberse a factores como en la región donde están funcionando estas entidades (por ejemplo, NIST es más comúnmente asociado con Estados Unidos) o a la falta de conocimiento específico sobre estas normativas.

El sector financiero parece estar apoyándose principalmente en normativas como ISO 27001 y marcos de trabajo como ITIL para abordar sus necesidades de seguridad de la

información y gestión de servicios de TI. Sin embargo, existen oportunidades para aumentar el conocimiento y la aplicación de otras normativas como NIST y MAGERIT, lo que podría proporcionar enfoques complementarios y fortalecer aún más la postura de seguridad de las organizaciones financieras.

Objetivo 2. Proponer una política de gestión de la seguridad de la información de acuerdo con la ISO 27001 aplicables a las actividades de las cooperativas de Ahorro y Crédito del municipio de San Vicente, departamento de San Vicente.

Según los resultados obtenidos se puede destacar que la mayoría de los encuestados reciben asesorías o capacitación ocasionalmente sobre seguridad y riesgos informáticos. Esto sugiere una necesidad de programas de capacitación más frecuentes y regulares para mejorar la conciencia y las habilidades en seguridad informática, en cuanto, a la percepción sobre la calidad del asesoramiento recibido se destaca que la información proporcionada es útil y adecuada.

Los encuestados tienen ciertas dudas sobre si la institución está preparada para enfrentar amenazas informáticas actuales, dado que el 55% responde con cierta incertidumbre, destacando la necesidad de evaluar y fortalecer las medidas de seguridad existentes, así poder mitigar ciertas vulnerabilidades que poseen las instituciones.

La mayoría de los encuestados en un 64% están totalmente de acuerdo en recibir capacitación y/o asesoría en políticas de seguridad informática, lo que subraya la importancia de programas de capacitación continuos y personalizados, más enfocados en la educación sobre mejores prácticas de gestión de contraseñas, dado que en gran porcentaje utiliza una contraseña maestra como método para que las contraseñas no se les olvide.

Por tanto, podemos ver una visión detallada de la situación actual de seguridad de la información en las cooperativas de ahorro y crédito del municipio de San Vicente. Dados estos resultados, se puede proponer una política de gestión de seguridad de la información que

aborde las áreas de mejora identificadas, como la necesidad de programas de capacitación más frecuentes y la clarificación de las políticas de seguridad existentes. La norma ISO 27001 puede servir como un marco útil para desarrollar estas políticas y mejorar la postura de seguridad de las instituciones.

Objetivo 3. Plantear una Política de control de acceso, que garantice que el acceso a la información sea autorizado y gestionado adecuadamente.

Según los datos proporcionados por los encuestados notamos que la mayoría cuentan con directrices para el manejo de contraseñas, lo que es positivo ya que el uso de contraseñas fuertes y la autenticación de doble factor son prácticas importantes para mejorar la seguridad de las cuentas.

En cuanto a los lineamientos para el acceso a datos por parte de los empleados muestran que las instituciones tienen lineamientos para el acceso a datos, lo que es crucial para garantizar que cada empleado tenga acceso solo a la información necesaria para su trabajo.

Los resultados de la encuesta muestran que muchas instituciones ya tienen algunos controles de acceso en su lugar, pero también hay áreas donde se puede mejorar. Por tanto, es fundamental desarrollar y aplicar una política de control de acceso integral que aborde todas las áreas identificadas sensibles en cuanto a la seguridad para garantizar que el acceso a la información sea autorizado y gestionado adecuadamente, minimizando así los riesgos de seguridad.

Objetivo 4. Definir políticas de auditoría y revisión que garanticen la eficacia continua de las medidas de seguridad.

Los resultados brindan una visión general en cuanto a las auditorías de la información, la mayoría de las instituciones realizan revisiones de las medidas de seguridad de la información de forma ocasional, lo que indica que existe un reconocimiento de la importancia

de la revisión periódica de las medidas de seguridad. Sin embargo, la frecuencia de estas revisiones podría ser más alta para garantizar una evaluación más rigurosa y continua de la eficacia de las medidas implementadas para garantizar la trazabilidad y la detección de posibles incidentes de seguridad.

En cuanto a la frecuencia de auditorías a la información, los resultados indican que se hace ocasionalmente en la mayoría de instituciones, pero hay una proporción considerable que las realiza raramente o nunca. Ante esto podemos destacar la importancia de establecer políticas que promuevan la realización regular de auditorías para identificar posibles vulnerabilidades o debilidades en el sistema de seguridad de la información.

Objetivo 5. Establecer modelos y controles para el manejo de información sensible dentro de la cooperativa en función de la norma ISO 27001 y estándares que sean aplicables a la seguridad de la información y protección a ciberataques.

Los resultados de la encuesta muestran que un buen porcentaje de las empresas financieras realizan copias seguridad de la información de forma ocasional o frecuente, esto es positivo ya que la realización regular de copias de seguridad es esencial para garantizar la disponibilidad y la integridad de los datos, en caso de incidentes o fallos.

En cuanto a la segmentación de las redes que poseen las empresas, se demuestra que hay una distinción de acceso entre unidades. Dicha segmentación es crucial para limitar el acceso no autorizado a partes sensibles de la red y proteger la información contra posibles amenazas internas y externas.

Por tanto, podemos destacar que gran parte de las prácticas relacionadas con el manejo de información sensible dentro de la cooperativa están alineadas con las mejores prácticas de seguridad de la información y los estándares como ISO 27001.

5 Capítulo V. Propuesta

Según los resultados proporcionados por los encuestados un 42% indica que las instituciones financieras conocen la Normativa ISO 27001, pero que no saben a ciencia cierta si esta es aplicada conforme a lo que indica la norma, por tanto, se propone una serie de políticas (Política de gestión de Seguridad de la Información, Política de Control de Acceso, Política de Auditoría y Revisión de Seguridad de la Información) las cuales permitirán:

Reducción de riesgos: Las políticas permiten identificar y controlar riesgos y amenazas, lo que disminuye la exposición a incidentes de seguridad.

Cumplimiento legal: Las instituciones financieras deben proteger los datos personales según la ley. La falta de políticas puede resultar en sanciones y daño a la reputación.

Protección de datos: La implementación de políticas permiten garantizar la integridad y confidencialidad de los datos y sistemas utilizados para procesarlos.

Mejora de procesos: Implementar esta serie de políticas ayuda a ajustar y mejorar los procesos de control en todas las áreas de la organización.

5.1 Política de Gestión de Seguridad de la Información (PGSI) para Cooperativas de Ahorro y Crédito en el departamento de San Vicente, El Salvador.

La presente Política de Gestión de Seguridad de la Información establece las directrices y procedimientos necesarios para proteger la información de la Cooperativa de Ahorro y Crédito, conforme a los requisitos de la norma ISO 27001:2022.

Política de Gestión de Seguridad de la Información (PGSI) para Cooperativas de Ahorro y Crédito en el departamento de San Vicente, El Salvador.

Mayo, 2024

1. Objetivos

Objetivo General

Establecer los lineamientos de seguridad necesarios para garantizar la integridad, confidencialidad y disponibilidad de la información de las cooperativas de ahorro y crédito de San Vicente, en El Salvador, de acuerdo con la norma ISO 27001:2022 y otras regulaciones legales que sean aplicables.

Objetivos Específicos

- Definir un marco gerencial para la implementación de la política de seguridad de información de la cooperativa.
- Determinar medidas que ayuden a reducir y mitigar los riesgos tecnológicos que afecten a los activos de información de la cooperativa.
- Diseñar lineamientos y medidas de gestión de activos de información acordes con el estándar ISO 27001:2022 y otras regulaciones de ley aplicables
- Proponer medidas de revisión que permitan la mejora continua de la seguridad de la información.
- Establecer las directrices de manejo de información que al ser aplicadas generen confianza y seguridad a los asociados, clientes, proveedores, entre otros.

2. Alcance

Esta política es aplicable a los activos de información, procesos y actividades financieras de la Cooperativa de Ahorro y Crédito. Además, aplica a todos los empleados, socios, proveedores y terceros que tengan acceso a sistemas o datos de la cooperativa.

3. Responsabilidad

- Consejo de Administración o Junta Directiva: Es responsable de aprobar la Política de Gestión de Seguridad de la Información y asegurar que se cumplan las normativas legales y regulatorias.

- Gerencia General: El gerente general o CEO tiene la responsabilidad de supervisar la implementación de las políticas aprobadas por el consejo. Asegurar que todos los departamentos cumplan con los procedimientos establecidos y que se destinen los recursos adecuados para la gestión de la seguridad de los datos.
- Departamento de Tecnología de la Información (TI): El equipo de TI implementa las medidas técnicas necesarias para controlar la gestión de la seguridad de la información. Esto incluye la configuración de sistemas de gestión de identidades y accesos (IAM), firewalls, sistemas de detección de intrusos y otras herramientas de seguridad cibernética.
- Todos los empleados y socios son responsables de conocer y cumplir con la política y procedimientos de seguridad de la información, proteger los activos de información y reportar cualquier incidente de seguridad de manera oportuna.

4. Vigencia

La política de seguridad de la información entrará en vigor, una vez sea aprobada por la Junta Directiva de la cooperativa. Esta normativa deberá ser revisada y actualizada como mínimo una vez al año. También se deberá revisar cuando se hagan cambios sustanciales en el área tecnológica de la cooperativa o si ocurrieran incidentes que afecten los activos de información.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.1, A5.35, A5.36)

5. Marco técnico

La elaboración de la presente política de seguridad de la información se basó en ISO 27001:2022, el cual establece los controles que garanticen la seguridad de la información en una organización.

6. **Términos y Definiciones**

- **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

- **Alta Gerencia (Alta Dirección)**: Persona o grupo de personas que dirige y controla una organización al más alto nivel. Tiene el poder de delegar autoridad y proporcionar recursos dentro de la organización.
- **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Disponibilidad**: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- **No Conformidad:** Incumplimiento de un requisito.
- **Riesgo:** Los riesgos de seguridad de la información pueden expresarse como un efecto de incertidumbre sobre los objetivos de seguridad de la información. El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.
- **Vulnerabilidad:** Es cualquier fallo o error en el software o en el hardware que permite a un atacante o hacker comprometer la integridad y confidencialidad de los datos que procesa un sistema.

7. Aspectos organizativos de la seguridad de la información

Se deberá crear un comité de riesgos o comité de seguridad de la información, a continuación, se definen los roles y responsabilidades que tendrían en cuanto a la implementación de la política de seguridad de la información.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.1, A5.2)

- Junta Directiva

Es responsabilidad de la junta directiva aprobar una estrategia general y política de seguridad de la información que esté en concordancia con la estrategia y objetivos de negocio de la cooperativa de ahorro y crédito.

- Alta Gerencia

La creación y revisión de la presente política es responsabilidad de la alta gerencia de la cooperativa apoyados por el responsable de Seguridad de la información y el comité de riesgos y deberá ser presentada a la Junta Directiva para su aprobación. La alta gerencia deberá proporcionar recursos adecuados y establecer los objetivos y metas del plan de seguridad. También, designará un responsable de seguridad de la información, así como comité de riesgos o comité de seguridad de la información.

- Responsable de la Seguridad de la Información y comité de riesgos

El responsable de seguridad de la información con el apoyo del comité de riesgos serán los responsables de velar por la implementación y mantenimiento de los controles de seguridad de la información de acuerdo con los requisitos de esta política y otras regulaciones legales existentes. Se recomienda que los integrantes de este comité sean personas en puestos de mando de las distintas áreas que tenga la cooperativa, incluyendo y principalmente el área de TI. El comité de seguridad es responsable de monitorear cambios significativos en los riesgos que afecten a los activos de información. El responsable de la seguridad de la información apoyado por el comité de riesgos, son responsables de asignar las funciones específicas para la implementación de esta política.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.3)

El responsable de la seguridad de la información deberá preparar reportes periódicamente para la alta gerencia y junta directiva, así como revisar y proponer actualizaciones a la política de seguridad de la información para promover la mejora continua.

El comité de riesgo será responsable de la divulgación de la política a todos los empleados, socios, y otros que tengan acceso a los activos de información. Para ello podrá hacer uso de programas de capacitación y divulgación por ej. garantizando que la política es accesible en los sistemas de la cooperativa, a través de intranet o correo electrónico.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.4, A5.24)

Otra función de este comité es vigilar que las configuraciones de seguridad de hardware, software, servicios y redes, se establezcan, documenten, implementen, monitorean y se revisen periódicamente.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.9)

— Responsable de Activos

Se deberá definir un responsable o propietario por área para cada uno de los activos de información de la cooperativa.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.9, A7.9)

8. <u>Gestión de Riesgos</u>

Se establecerá un proceso formal de gestión de riesgos para identificar, evaluar y tratar los riesgos de la seguridad de la información (SGSI) relacionados con operaciones financieras, clientes y socios, dicho proceso se revisará y actualizará regularmente.

El SGSI debe garantizar lo siguiente:

- Eventualmente se debe hacer un análisis de riesgo, donde se identifiquen las vulnerabilidades técnicas de los sistemas de información y se analice el riesgo de ocurrencia de estas.

  Referencia: Anexo A. ISO 27001:2022 Controles (A8.8)

- Se deben desarrollar otras políticas, normativas y procedimientos para apoyar la política de seguridad de la información.
- La definición de una metodología para la identificación y tratamiento de los riesgos
- El establecimiento de criterios para medir el cumplimiento del SGSI.
- La revisión del nivel de cumplimento del SGSI.
- La corrección de no conformidades mediante la implementación de las medidas necesarias.

9. <u>Gestión de Incidentes</u>

Se establecerá un proceso de gestión de incidentes para detectar, investigar y responder a incidentes de seguridad de la información que afecten las operaciones financieras y la privacidad de los clientes y socios. El comité de riesgos junto con el responsable del comité, serán responsables de coordinar las acciones de respuesta y se documentarán los procedimientos a seguir.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.25, A5.26)

- Los incidentes deberán ser comunicados a los encargados tan pronto sea posible, para lo que se deberán dedicar canales de comunicación (email, teléfono, chat, etc).

Referencia: Anexo A. ISO 27001:2022 Controles (A5.24)

- Se deberá monitorear constantemente las actividades en red y sistemas además de mantener logs, de manera que se puedan identificar incidentes lo más pronto posible.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.9)

- Se establecerán procedimientos para la recolección y preservación de evidencia de incidentes de seguridad de la información para su posterior análisis.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.28)

- Se deberán Implementar controles detallados de las acciones de recuperación y corrección de fallas.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.26)

- Cualquier ocurrencia de incidentes o amenazas relacionado con la seguridad de la información debe ser documentado y analizado para generar medidas correctivas a futuro.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.7, A5.27)

10. Clasificación de Activos

Se deben identificar los activos que se deben proteger y en qué dimensión. Estos se pueden clasificar de la siguiente manera:

- Servicios
- Datos
- Información
- Hardware
- Redes
- Software

11. Identificación y Clasificación de la información

Toda la información de la cooperativa deberá identificarse, clasificarse y etiquetarse, de manera que la información crítica o sensible sea identificada y pueda ser protegida y respaldada adecuadamente.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.12, A5.13)

La clasificación de la información puede basarse en los niveles siguientes:

- Información restringida: Información crítica o con mayor grado de sensibilidad. El acceso a este tipo de información deberá ser autorizado por la alta gerencia en casos específicos. Ej. Podrían ser estados financieros de la cooperativa, transferencias de dinero, planes estratégicos, etc.
- Información confidencial, información sensible sólo accesible para los empleados que lo necesitan para sus funciones. Ej. Podrían ser contratos con clientes, empleados y

proveedores, bases de datos de clientes, bases de datos de proveedores. Transacciones diarias.

- Uso Interno, estos serían datos de operaciones diarias, que deben ser manejadas de forma discreta. Ej. Comprobantes de crédito fiscal, facturas de clientes, etc.
- Información General, Información pública, como promociones, reglamentos, etc.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.12)

Se debe implementar un sistema de etiquetado que abarque todos los documentos, y todos los empleados deben conocer y aplicar este etiquetado en la información que produzcan en el desempeño de sus funciones.

La información crítica de la cooperativa como lo sería la información transaccional y de los clientes, no se transmitirá por medios que no sean los de la cooperativa. Debe ser almacenada de forma cifrada, y respaldada regularmente. Se deberá crear un manual de procedimientos para cualquier transferencia interna o externa por ej. información enviada a clientes.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.14)

12. <u>Acceso a información financiera y datos de los usuarios/clientes</u>

Se implementarán controles de acceso físicos y tecnológicos para proteger los sistemas y datos financieros de la cooperativa contra accesos no autorizados.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.10, A5.15)

Estos controles incluyen los siguientes:

— **<u>Perímetro de Seguridad Física</u>**

Esto comprende la creación de diversas barreras o medidas de control físicas alrededor de las oficinas de la cooperativa y específicamente de las áreas de procesamiento de información.

- En el local de la cooperativa de ahorro y crédito se definirán los espacios de acceso a los clientes, el área de empleados de acuerdo con sus funciones y se restringirá el

acceso a las áreas donde se encuentran servidores y otros sistemas informáticos, solo el personal responsable de estos equipos podrá tener acceso a ellos.

Referencia: Anexo A. ISO 27001:2022 Controles (A7.1, A7.3)

- Las entradas y puntos de acceso deberán ser protegidas y monitoreadas para evitar acceso no autorizado.

Referencia: Anexo A. ISO 27001:2022 Controles (A7.2, A7.4)

- Se implementarán medidas contra riesgos físicos y ambientales, como terremotos, inundaciones e incendios, será necesario contar con salidas de emergencia, extinguidores, y organizar simulacros de evacuación en caso de emergencia al menos una vez al año.

Referencia: Anexo A. ISO 27001:2022 Controles (A7.5, A7.6)

— **Control de Acceso a Datos**

El control de acceso consiste en establecer reglas sobre protección y acceso a la información, controlar cambios en los permisos de usuarios, definir niveles de aprobación para acceso a datos.

- Se proveerá acceso a la información y sistemas únicamente si es necesaria para sus funciones dentro de la organización, observando la regla del mínimo privilegio. Además, dichos privilegios serán modificados o eliminados inmediatamente haya algún cambio en la situación del empleado, ya sea promociones, cambios de área, renuncia/despidos entre otros.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.18, A8.2, A8.3, A8.18)

- Se deberá implementar la autenticación segura, mediante autenticación multifactorial, la segregación de funciones y la supervisión de actividades de acceso.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.5)

- Se establecerán reglas que requieran la aprobación del administrador para tener acceso a datos.
- Se concientizará al personal en el manejo adecuado de credenciales. (5.17)

Referencia: Anexo A. ISO 27001:2022 Controles (A5.17)

- El acceso a datos deberá ser bloqueado o eliminado inmediatamente el empleado deje de trabajar en la cooperativa.
- Se capturarán registros de intentos fallidos de inicio de sesión y otras actividades o eventos relevantes, estos registros se almacenarán y protegerán para su posterior análisis y determinar si se trató de algún tipo de amenaza. (A8.15)

Referencia: Anexo A. ISO 27001:2022 Controles (A8.15)

— **Manejo de la Información**

- La información almacenada en los sistemas de información será eliminada cuando ya no sea necesaria.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.10)

- Se implementarán medidas de prevención de fuga de datos, para ello las actividades de los equipos deberán ser monitoreadas constantemente.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.12)

- Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso y publicación no autorizada.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.33)

- Se harán copias de respaldo de la información restringida, confidencial y de uso interno. Estas copias deberán ser incrementadas y realizadas diariamente.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.13)

- Se harán pruebas periódicas de restablecimiento de la información mediante copias de seguridad para evaluar la eficiencia de estas. (A8.13)

Referencia: Anexo A. ISO 27001:2022 Controles (A8.13)

13. Documentación de procedimientos operativos

La documentación de procedimientos operativos deberá ponerse a disposición del personal que los necesite. Se deberá incluir:

- Instrucciones para el manejo de errores que ocurran en las actividades diarias.
- Canales de comunicación con personal de soporte en caso de imprevistos técnicos u operativos
- Reinicio de sistemas y servidores y procedimientos de recuperación en caso de ocurrencia de fallas.
- Monitoreo de procesos y comunicaciones
- Gestión del servicio
- Resguardo de información

Referencia: Anexo A. ISO 27001:2022 Controles (A5.37)

14. Gestión de Equipos

Los equipos de punto final de usuarios deben manejarse de forma segura de manera que se proteja la información contra riesgos específicos de este tipo de dispositivo.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.1)

- Los equipos se entregarán a los empleados hasta que el proceso de contratación sea completado y se asignarán equipos acordes a sus funciones.
- Los empleados (u otros como contratistas o socios) devolverán los equipos que estén en su poder al terminar su empleo, contrato o acuerdo.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.11)

- Los equipos informáticos deberán ser sometidos a mantenimiento preventivo en periodos regulares, acordes con las especificaciones técnicas del proveedor.

Referencia: Anexo A. ISO 27001:2022 Controles (A7.13)

- Se deberá mantener un inventario actualizado del equipamiento, incluyendo la bitácora de mantenimiento preventivo y correctivo y con los detalles del responsable del equipo.

  Referencia: Anexo A. ISO 27001:2022 Controles (A5.9)

- Solo el personal de IT puede brindar mantenimiento preventivo y correctivo.
- Los equipos deberán ser dispuestos en cumplimiento con los estándares de red de área local, con sus correspondientes protectores de voltaje.

  Referencia: Anexo A. ISO 27001:2022 Controles (A7.8, A7.11, A7.12)

- Los medios extraíbles solo serán permitidos si el puesto del empleado lo necesita para sus funciones, los medios extraíbles no deberán ser dejados sobre el escritorio u otros muebles de forma descuidada. Se debe aplicar la política de escritorio limpio, esto aplica también para cualquier documento que contenga información de la cooperativa. Para puestos como cajas donde no es necesario el uso de dispositivos extraíbles, estos serán deshabilitados y no se instalarán lectores de CD/DVD, tarjetas SD, etc.

  Referencia: Anexo A. ISO 27001:2022 Controles (A7.7)

- Al momento de levantarse de su escritorio el empleado deberá bloquear la pantalla de su equipo.

  Referencia: Anexo A. ISO 27001:2022 Controles (A7.7)

- Discos Duros, CD de datos, Memoria USB y otros dispositivos de almacenamiento deben ser debidamente formateados antes de ser debidamente desechados. (A7.10, A7.14)

  Referencia: Anexo A. ISO 27001:2022 Controles (A7.10, A7.14)

- Todo el software instalado deberá estar debidamente licenciado, o buscar soluciones Open Source o de comunidad que sean seguras, el software solo puede ser instalado por personal de TI. Se debe hacer énfasis a los usuarios a no instalar software que no sea el provisto por la cooperativa.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.7)

- Los empleados deberán usar cuentas estándares y no administrativas de manera que la instalación de software o cambios importantes en el equipo estén restringidos. Únicamente el personal de TI podrá usar cuentas administrador para configuración y mantenimiento de los equipos.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.19)

— **Seguridad de equipos fuera de las instalaciones**

- Se deberá preparar los equipos para trabajo remoto, ya sea para trabajo regular o situaciones extraordinarias
- Se deberá habilitar la encriptación (Cifrado) del disco duro de los equipos e instalar las herramientas necesarias como el cliente VPN, antivirus, el agente de monitoreo, que permita capturar los logs de las actividades realizadas en la computadora, una herramienta de comunicación con la empresa como zoom, slack, Windows teams, además de las herramientas necesarias para sus funciones como procesadores de texto y hoja de cálculo. Además, se deberá configurar el acceso a través de una cuenta estándar para uso del empleado.

Referencia: Anexo A. ISO 27001:2022 Controles (A7.9, A6.7, A8.24)

- El uso de equipo fuera de las instalaciones deberá ser aprobado por el gerente del área, y se deberá firmar una carta compromiso de manejar el dispositivo adecuadamente por parte del empleado al que se le entrega el equipo.
- Registrar entradas y salidas de equipos para mantenimiento, trabajo remoto, etc.

15. Utilización de servicios de red

Las Redes de datos y los dispositivos de red deben estar debidamente protegidas contra accesos no autorizados.

El personal de TI controlará el otorgamiento a los servicios y recursos de red tanto internos como externos. Se deberán establecer procedimientos de autorización y controles de acceso lógicos.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.20, A8.21)

- Las conexiones externas se deberán realizar mediante una conexión cliente VPN, la autenticación de la conexión se deberá implementar métodos de doble autenticación.
- Las redes inalámbricas utilizan métodos de autenticación fuertes. Si hay acceso para el público, esta red deberá estar en un segmento de red diferente a la usada por la cooperativa.
- Implementar políticas de autenticación segura para todas las conexiones. (cambios de contraseñas en periodos regulares, contraseñas con mínimo 12 caracteres y combinación de caracteres especiales y alfanuméricos, entre otros).

  Referencia: Anexo A. ISO 27001:2022 Controles (A8.5, A8.24)
- Se deberá implementar segregación de redes para mantener las transacciones aisladas del resto de actividades.

  Referencia: Anexo A. ISO 27001:2022 Controles (A8.22)
- Las redes, sistemas y aplicaciones deberán ser monitoreadas para identificar comportamientos anómalos, estos serán analizados para la identificación de incidentes.

  Referencia: Anexo A. ISO 27001:2022 Controles (A8.16)
- Se limitará el acceso a sitios web externos, mediante reglas apropiadas en el firewall de la cooperativa.

  Referencia: Anexo A. ISO 27001:2022 Controles (A8.23)
- Se deberá instalar sistemas redundantes para garantizar la disponibilidad de la información.

  Referencia: Anexo A. ISO 27001:2022 Controles (A8.14)

- Las configuraciones de red deberán documentarse, monitorearse y revisarse periódicamente.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.9)

16. <u>Gestión de Personal en cuanto a la seguridad de la información</u>

Se deberá asegurar que los empleados conozcan y apliquen la política de seguridad de la información en su área de funciones.

- El área de recursos humanos debe contar con controles para verificar los antecedentes laborales y solvencia de antecedentes penales. Estos deberán ser verificados previo a la incorporación del trabajador.

Referencia: Anexo A. ISO 27001:2022 Controles (A6.1)

- El contrato laboral y de servicios debe incluir cláusulas que garanticen el compromiso de guardar la confidencialidad de la información por parte del empleado o proveedor, también se debe establecer que dichas cláusulas continuarán vigentes aun cuando el contrato sea finalizado.

Referencia: Anexo A. ISO 27001:2022 Controles (A6.2, A6.5, A6.6)

- Se debe capacitar y concientizar al personal en seguridad de la información al menos dos veces al año, y como parte del proceso de inducción del empleado. Las políticas y regulaciones deberán estar accesibles para referencia.

Referencia: Anexo A. ISO 27001:2022 Controles (A6.3)

- El cumplimiento de las políticas de seguridad de la información debe ser obligatorio para los empleados y debería ser considerado en la evaluación anual del desempeño, así como incurrir en sanciones administrativas por su incumplimiento.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.4, A6.4)

- El Personal podrá y deberá reportar incidentes de seguridad de la información mediante un correo electrónico y/o un número telefónico. Los reportes serán investigados y

analizados por el comité de riesgos, los que le darán seguimiento para su corrección de acuerdo con la gravedad de estos.

Referencia: Anexo A. ISO 27001:2022 Controles (A6.8)

17. **Gestión de proveedores y contratistas**

Se establecerán procedimientos para manejo de información con los proveedores y terceros.

- Deberán incluirse cláusulas contractuales que garanticen el compromiso con la confidencialidad por parte de proveedores y terceros por el periodo contratado y una vez el servicio sea finalizado.

  Referencia: Anexo A. ISO 27001:2022 Controles (A5.19, A5.20)

- También se deberán incluir en el contrato condiciones que garanticen la seguridad de la información a través de la cadena de suministro.

  Referencia: Anexo A. ISO 27001:2022 Controles (A5.21)

- Se deberán establecer parámetros para determinar que el nivel de servicio acordado en cuanto a la seguridad de la información se mantiene en caso de que haya cambios en los servicios.

  Referencia: Anexo A. ISO 27001:2022 Controles (A5.22, A8.32)

- Se deberá monitorear, revisar y evaluar la prestación de servicios por parte del proveedor para garantizar el que se mantenga el nivel acordado de seguridad de la información.

  Referencia: Anexo A. ISO 27001:2022 Controles (A5.22)

18. **Seguridad de la Información para el uso de servicios en la Nube**

Si la cooperativa decide hacer uso de servicios de la nube, los aspectos de esta política deben ser implementados en la adquisición, uso, gestión y salida de los servicios en la nube.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.23)

19. **Relaciones con autoridades y otras entidades**

- El comité de riesgo deberá establecer y mantener el contacto con las autoridades pertinentes para reportar incidentes de seguridad cuando sea necesario.

  Referencia: Anexo A. ISO 27001:2022 Controles (A5.5)

- Es conveniente que se mantenga comunicación estrecha con organizaciones como INSAFOCOOP y otras cooperativas para ayuda mutua.

  Referencia: Anexo A. ISO 27001:2022 Controles (A5.6)

- Se deberá tener accesible los números de emergencia de entidades como policía, bomberos, hospitales, para reaccionar a una situación imprevista que afecte la cooperativa.

20. <u>Cumplimiento Legal y Regulatorio</u>

La cooperativa identificará y cumplirá con todas las leyes y regulaciones aplicables en El Salvador relacionadas con la privacidad y protección de la información de identificación personal y protección de datos financieros. Se realizarán evaluaciones periódicas de cumplimiento y se tomarán medidas correctivas en caso de desviaciones.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.31, A5.34)

21. <u>Continuidad del Negocio</u>

Se deberá elaborar una estrategia de continuidad de las actividades de la cooperativa priorizando los procesos críticos de la misma, a la vez se debe asegurar que los empleados, socios y directivos comprendan que el impacto de una interrupción puede tener consecuencias tanto económicas como de reputación y estabilidad de la cooperativa.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.30)

- Se deberán definir acciones correctivas a implementar dependiendo el caso.
- Diseñar procedimientos de emergencia, para la recuperación y restablecimiento de los sistemas tan pronto sea posible. Estableciendo parámetros máximos de tiempo para que el sistema vuelva a estar en funcionamiento.

- Capacitar al personal sobre los procedimientos de emergencia y recuperación.
- Se deberán hacer pruebas de los planes de contingencia para garantizar su buen funcionamiento y medir tiempos de respuesta.
- Durante todo momento se deberá resguardar la seguridad de la información (A5.29)

Referencia: Anexo A. ISO 27001:2022 Controles (A5.29)

22. <u>Adquisición de software</u>

La adquisición o contratación de software para uso de la cooperativa, deberá incluir el análisis de factores de seguridad del software. La cooperativa puede hacer uso de software Open Source o versiones de comunidad que cumplan con los requisitos de seguridad de esta política. Si se subcontrata el desarrollo de software, por ej. Sitio web, el responsable de seguridad y comité de seguridad de la información deberán vigilar que la política de seguridad se incluya en los requerimientos para el software, y que estos formen parte de los criterios de aceptación del producto. Lo que se establecerá en el contrato del servicio.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.26, A8.30)

23. <u>Revisión y Mejora Continua</u>

Esta política se revisará periódicamente para garantizar su relevancia y eficacia en el contexto de la cooperativa. Se llevarán a cabo auditorías internas regulares para evaluar el cumplimiento de los controles de seguridad y se tomarán medidas para mejorar el sistema de gestión de seguridad de la información.

- Las pruebas de auditoría de seguridad de sistemas de información deberán realizarse al menos una vez al año.
- Se deberá establecer un documento contractual entre el evaluador y la cooperativa, donde se comprometan a guardar la adecuada confidencialidad y seguridad de la información.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.34)

5.2 Política de Control de Acceso e Información de Datos para las Cooperativas de Ahorro y Crédito de San Vicente, El Salvador.

La presente política de control de acceso a datos tiene como objetivo establecer las directrices y procedimientos para proteger la información sensible y confidencial de la Cooperativa de Ahorro y Crédito, en conformidad con los estándares establecidos por la norma ISO 27001:2022.

Política de Control de Acceso de Datos e Información para las Cooperativas de Ahorro y Crédito de San Vicente, El Salvador.

Mayo, 2024

Objetivo

- Establecer medidas y procedimientos en el control de acceso de datos para asegurar la protección de la información y los activos digitales de la cooperativa de Ahorro y Crédito, así como para cumplir con requisitos regulatorios aplicables.
- Garantizar la confidencialidad, integridad y disponibilidad de los datos de los socios y clientes.
- Prevenir el acceso no autorizado y proteger la información financiera.
- Diseñar lineamientos y medidas de gestión de activos de información acordes con el estándar ISO 27001:2022 y otras regulaciones de ley aplicables

Alcance

Esta política se aplica a todos los empleados, socios, contratistas y terceros que requieran acceso a los sistemas de información y datos de la cooperativa, así también a los usuarios con acceso a sistemas, están obligados a conocer, cumplir y hacer cumplir su responsabilidad respecto a los riesgos en el manejo de la información que se tiene de la cooperativa.

La gestión de la seguridad es una actividad propia de la cooperativa y no puede ser ejecutada por personal ajeno a esta o terceras personas sin previa autorización.

Responsables de implementación.

- Consejo de Administración o Junta Directiva: Es responsable de aprobar la Política de Control de Acceso a Datos y asegurar que se cumplan las normativas legales y regulatorias.
- Gerencia General: El gerente general o CEO tiene la responsabilidad de supervisar la implementación de las políticas aprobadas por el consejo. Asegurar que todos los departamentos cumplan con los procedimientos establecidos y que se destinen los recursos adecuados para la gestión de la seguridad de los datos.
- Departamento de Tecnología de la Información (TI): El equipo de TI implementa las medidas técnicas necesarias para controlar el acceso a los datos. Esto incluye la

configuración de sistemas de gestión de identidades y accesos (IAM), firewalls, sistemas de detección de intrusos y otras herramientas de seguridad cibernética.

- Empleados y Usuarios: Todos los empleados son responsables en adherirse a las políticas de control de acceso y reportar cualquier incidente de seguridad.

Términos y Definiciones

- **Acceso**: La capacidad o el derecho de un individuo, programa o proceso de interactuar con un sistema de información y sus recursos.
- **Autenticación**: El proceso de verificar la identidad de un usuario, proceso o dispositivo, a menudo como una condición previa para permitir el acceso a los recursos en un sistema de información.
- **Autorización**: Proceso de conceder o denegar permisos a un usuario, programa o proceso para acceder a ciertos recursos o realizar ciertas acciones en un sistema de información.
- **Auditoría de Acceso:** El proceso de revisar y analizar los registros de acceso para asegurar el cumplimiento de las políticas de seguridad y detectar cualquier actividad inusual o no autorizada.
- **Credenciales de Acceso**: Información que permite la autenticación de un usuario en un sistema de información, como nombres de usuario, contraseñas, tokens de seguridad ó certificados digitales.
- **Control de Acceso Basado en Roles (RBAC):** Un enfoque de control de acceso en el que los permisos se asignan a roles específicos en lugar de a individuos. Los usuarios son asignados a roles con base en sus responsabilidades laborales.
- **Confidencialidad**: Asegurar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso.
- **Control de Acceso Físico:** Medidas de seguridad destinadas a proteger los sistemas de información y sus recursos contra el acceso físico no autorizado.

- **Control de Acceso Lógico:** Medidas de seguridad destinadas a proteger los sistemas de información y sus recursos contra el acceso lógico no autorizado, como firewalls, sistemas de gestión de identidades y accesos (IAM), y autenticación multifactor (MFA).
- **Disponibilidad**: Asegurar que la información y los recursos estén disponibles para los usuarios autorizados cuando se necesiten.
- **Incidente de Seguridad:** Un evento que indica que la seguridad de un sistema de información ha sido comprometida o que existe una amenaza de que pueda ser comprometida.
- **Integridad**: La protección de la exactitud y completitud de los datos contra modificaciones no autorizadas.
- **Política de Mínimos Privilegios:** Un principio de seguridad que establece que los usuarios, programas o sistemas solo deben tener los privilegios mínimos necesarios para realizar sus funciones.
- **Roles**: Conjuntos de permisos y privilegios asignados a usuarios o grupos de usuarios en función de sus responsabilidades laborales y necesidades de acceso.
- **Privilegios**: Derechos y permisos específicos otorgados a un usuario o proceso para realizar acciones en un sistema de información, como leer, escribir, modificar o eliminar datos.
- **Seguridad de la Información:** La práctica de proteger la información y los sistemas de información contra accesos no autorizados, usos indebidos, divulgación, interrupción, modificación o destrucción.
- **Sistema de Información:** Un conjunto de componentes interrelacionados que recopilan, procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control en una organización.
- **Usuario**: Cualquier persona o entidad que utiliza un sistema de información. Puede incluir empleados, contratistas, socios y clientes.

Provisionamiento de Acceso

El área de Tecnología de la Información, TI, será responsable de gestionar el proceso de provisionamiento de acceso, que incluye la creación, modificación, eliminación o desactivación de cuentas de usuario.

Se definirán los perfiles de usuarios con determinados accesos a la información, basado en los siguientes criterios:

- En función al área que pertenece el empleado(roles).
- En función al tipo de información que accederá para cumplir con sus funciones (pública, privada, confidencial)
- En función de las acciones permitidas sobre la información a la que tiene acceso (consulta, registro, modificación, eliminación).

Se establecerá un procedimiento formal para solicitar y aprobar el acceso a sistemas de información, el proceso incluirá la verificación de la necesidad de acceso y la aprobación por parte de un gerente autorizado.

Se mantendrá un registro actualizado de todos los usuarios autorizados, sus roles y privilegios de acceso, así como de las solicitudes de acceso y las aprobaciones correspondientes.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.2)

Autenticación y Autorización

Se definirán mecanismos de autenticación adecuados para permitir el acceso a la información de la cooperativa. Se requerirá autenticación de dos factores para todos los usuarios que accedan a los sistemas de información, utilizando una combinación de credenciales únicas, como nombre de usuario y contraseña y un segundo factor de autenticación, como un token de seguridad o aplicación de autenticación móvil.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.15, A5.16, A5.17, A5.18, A8.5)

Los privilegios de acceso se asignarán según el principio de privilegio mínimo necesario, lo que significa que los usuarios solo tendrán acceso a la información y funcionalidades necesarias para llevar a cabo sus responsabilidades laborales.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.18, A8.2, A8.3)

Se establecerán controles de autorización para restringir el acceso a los datos confidenciales y críticos, utilizando listas de control de acceso (ACL), roles y grupos de seguridad, de acuerdo con la segregación de funciones de la cooperativa.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.3)

Monitoreo de Acceso

Se implementará un sistema de registro de auditoría para registrar todos los intentos de acceso a los sistemas de información, incluidos los éxitos y los fallos, así como cualquier actividad relacionada con los privilegios de administración y cambios de configuración.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.34)

El comité de seguridad de la información supervisará regularmente los registros de acceso para detectar actividades sospechosas o no autorizadas, y tomará medidas correctivas según sea necesario.

Se realizarán revisiones periódicas de los registros de acceso para garantizar el cumplimiento de las políticas y procedimientos de control de acceso, y se documentarán las acciones correctivas tomadas en caso de incumplimientos.

Referencia: Anexo A. ISO 27001:2022 Controles (A5.34)

Gestión de Cuentas de Administración

Las cuentas de administración deben ser gestionadas con mayor precaución debido a que permiten realizar cualquier acción sobre los sistemas, por lo que se tendrá en cuenta los siguientes aspectos:

- Estas cuentas solo se utilizarán cuando sea necesario una acción con permiso de administrador. Es decir, no se harán tareas comunes utilizando cuentas de administrador.
- El acceso con cuenta de administrador requerirá un factor de doble autenticación en todos los casos.
- Se deberán mantener registros o logs de acciones de los usuarios
- Las claves deben ser robustas y cambiadas con frecuencia
- Serán incluidos en las auditorías periódicas

Referencia: Anexo A. ISO 27001:2022 Controles (A5.17, A8.5)

Gestión de Cuentas de Usuario

Se implementarán procedimientos de gestión de cuentas de usuario para garantizar la creación, modificación y eliminación o desactivación adecuadas de cuentas de usuario, de acuerdo con los cambios en el estado laboral o las responsabilidades del usuario.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.1, A8.7)

Se llevará a cabo una revisión periódica de las cuentas de usuario inactivas o no utilizadas, y se tomarán medidas para desactivarlas o eliminarlas según sea necesario para reducir el riesgo de acceso no autorizado.

Se implementarán controles de cambio de contraseña para garantizar contraseñas seguras, incluyendo la complejidad mínima, la caducidad periódica, procedimientos de bloqueo y la prohibición de reutilización de contraseñas anteriores.

Referencia: Anexo A. ISO 27001:2022 Controles (A8.4)

Responsabilidades

El área de TI es responsable de implementar y mantener los controles de acceso, así como de monitorear el cumplimiento de esta política, incluyendo la gestión de cambios y la respuesta a incidentes de seguridad.

Los empleados y usuarios autorizados son responsables de cumplir con las políticas y procedimientos de control de acceso, así como de informar cualquier actividad sospechosa o violación de seguridad a los canales adecuados.

Revisiones y Actualizaciones

Esta política será revisada y actualizada periódicamente por el comité de seguridad de la información y el área de TI para garantizar su efectividad y cumplimiento continuo con los estándares de seguridad de la información y las regulaciones aplicables. Las revisiones se llevarán a cabo al menos una vez al año o según sea necesario en respuesta a cambios en el entorno de amenazas, tecnológicos o regulatorios.

5.3 Política de Auditoría y Revisión de Seguridad de la Información para las Cooperativas de Ahorro y Crédito en San Vicente, El Salvador.

La presente política establece las directrices y procedimientos para la auditoría y revisión de la seguridad de la información en la Cooperativa de Ahorro y Crédito, conforme a los estándares de la norma ISO 27001:2022.

Política de Auditoría y Revisión de Seguridad de la Información para las Cooperativas de Ahorro y Crédito en San Vicente, El Salvador

Mayo, 2024

Objetivo

- Establecer procedimientos para auditar y revisar periódicamente las medidas y controles de seguridad de la información de las Cooperativas de Ahorro y Crédito de San Vicente, con el fin de asegurar la eficacia de estas para proteger la confidencialidad, integridad y disponibilidad de la información y garantizar la mejora continua.
- Cumplir con las leyes, regulaciones y estándares aplicables.
- Detectar y corregir vulnerabilidades y riesgos de seguridad

Alcance

Todos los empleados, directivos y partes interesadas involucradas en la gestión de la seguridad de la información, dispositivos y procesos de las Cooperativas de Ahorro y Crédito.

Términos y Definiciones

- **Auditoría de Seguridad de la Información**: Proceso sistemático e independiente para examinar las políticas, procedimientos y controles de seguridad de la información con el fin de evaluar su efectividad y cumplimiento con las normativas y estándares establecidos.
- **Auditoría Interna**: Un examen independiente y objetivo de las actividades de una organización, realizado por sus propios empleados, para evaluar la efectividad de los controles internos y la gestión de riesgos.
- **Auditoría Externa**: Un examen realizado por una entidad independiente fuera de la organización para evaluar la efectividad de los controles y el cumplimiento con las normativas y estándares de seguridad de la información.
- **Cumplimiento**: Adherirse a leyes, regulaciones, políticas y normas de seguridad de la información aplicables.
- **Control de Seguridad**: Medidas implementadas para proteger la confidencialidad, integridad y disponibilidad de la información y los sistemas de información.

- **Controles Preventivos**: Medidas diseñadas para evitar que ocurra un incidente de seguridad.
- **Controles Detectivos**: Medidas diseñadas para identificar y alertar sobre un incidente de seguridad una vez que ha ocurrido.
- **Evaluación de Riesgos**: El proceso de identificar, analizar y evaluar riesgos potenciales para la seguridad de la información, con el objetivo de implementar controles adecuados para mitigarlos.
- **Evaluación de Vulnerabilidades**: El proceso de identificar, clasificar y priorizar las vulnerabilidades en un sistema de información.
- **Incidente de Seguridad**: Un evento que indica que la seguridad de la información ha sido comprometida o que existe una amenaza de que pueda ser comprometida.
- **Informe de Auditoría**: Un documento que detalla los hallazgos, conclusiones y recomendaciones de una auditoría de seguridad de la información.
- **Política de Seguridad de la Información**: Un conjunto de directrices y procedimientos establecidos para proteger la información y los sistemas de información de accesos no autorizados, uso indebido, divulgación, alteración y destrucción.
- **Plan de Acción Correctiva**: Un plan desarrollado para corregir las deficiencias y debilidades identificadas durante una auditoría o revisión de seguridad.
- **Plan de Continuidad del Negocio (BCP):** Un plan que establece procedimientos y recursos necesarios para continuar las operaciones críticas en caso de una interrupción significativa.
- **Plan de Recuperación de Desastres (DRP):** Un plan diseñado para restaurar los sistemas y operaciones de una organización tras un evento catastrófico.
- **Revisión de Cumplimiento**: Una evaluación para asegurar que las prácticas de seguridad de la información cumplen con las leyes, regulaciones y políticas internas aplicables.

- **Revisión de Seguridad**: Análisis periódico y detallado de los controles de seguridad de la información y sus prácticas para identificar áreas de mejora y asegurar la adecuación continua de las medidas de seguridad.
- **Gestión de Incidentes**: El proceso de identificar, gestionar y responder a eventos de seguridad de la información para limitar su impacto y restaurar la normalidad de las operaciones.

Procedimientos

1. Auditoría de Seguridad de la Información:

- Se realizará una auditoría de seguridad de la información una vez al año, la auditoría podría ser realizada por un auditor o grupo de auditores interno designado por el comité de seguridad de la información o contratar auditores externos. En ambos casos las personas designadas deberán contar con experiencia en auditoría de seguridad de la información y estudios especializados en el área.
- La auditoría evaluará la configuración de redes e infraestructura de TI, las políticas de seguridad, los controles de acceso, la gestión de riesgos, la detección y respuesta a incidentes y otros aspectos mencionados en la política de seguridad de la información.
- El auditor preparará un informe detallado de auditoría que incluya hallazgos, recomendaciones y planes de acción correctiva.
- El auditor o grupo de auditores se comprometerán a guardar la confidencialidad de la información, durante y después de la auditoría. Esto deberá establecerse en un acuerdo contractual del servicio antes de iniciar la auditoría.
- La Junta Directiva y alta dirección revisará y aprobará el informe de auditoría de seguridad de la información y decidirán si se implementarán los planes de acción correctiva recomendados y en qué periodo, de acuerdo con su criticidad y los recursos necesarios.

2. Revisiones Periódicas:

- Se llevarán a cabo revisiones trimestrales de los controles de seguridad de la información por parte del comité de seguridad de la información de la Cooperativa.
- Las revisiones se centrarán en áreas específicas identificadas como críticas o de riesgo, como la gestión de contraseñas, la creación de copias de respaldo, la actualización de parches, la seguridad de la red, el inventario de activos, y otras que sean consideradas críticas.
- Se elaborará un informe de revisión que resuma los hallazgos, las áreas de mejora y las recomendaciones.
- El área de tecnología de la Información (TI) será responsable de incorporar las medidas necesarias que lleven a mejorar la situación actual de seguridad de la información, en base a los hallazgos y recomendaciones en las áreas identificadas.

3. Seguimiento y Cumplimiento:

- El comité de seguridad de la información será responsable de vigilar la implementación de las recomendaciones obtenidas de las auditorías y revisiones.
- Se establecerá un sistema de seguimiento para garantizar que las acciones correctivas se completen dentro de los plazos establecidos.
- Se brindará informes regulares a la Junta Directiva y a la alta Gerencia sobre el avance en la implementación de las recomendaciones y el estado general de la seguridad de la información de la cooperativa.

Responsabilidades

- La Junta Directiva es responsable de supervisar las auditorías de seguridad de la información, revisar y aprobar los informes, y garantizar que se asignen recursos adecuados para implementar las medidas correctivas o de mejora.

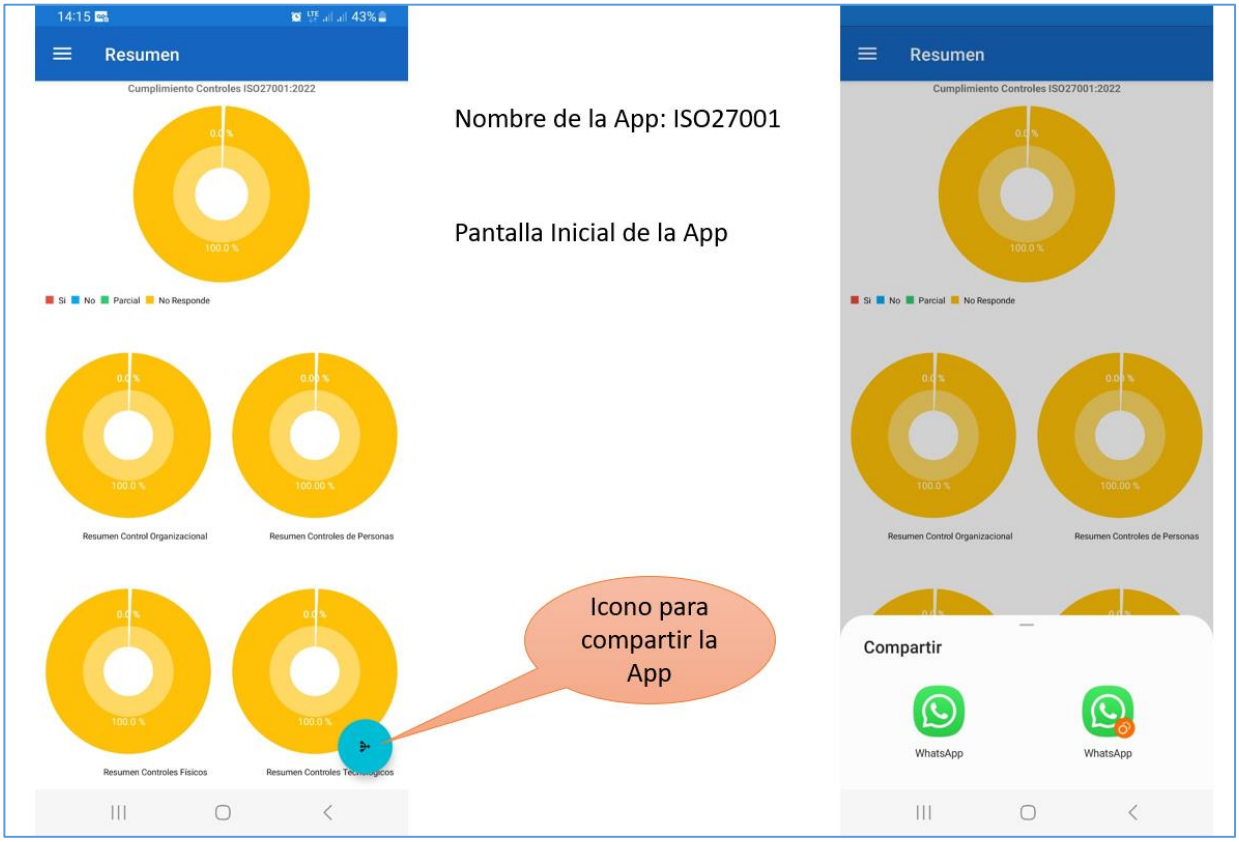
- El comité de seguridad de la información y la Gerencia de TI son responsables de llevar a cabo las revisiones periódicas, implementar las recomendaciones y asegurar el cumplimiento continuo de las políticas y estándares de seguridad.

5.4 Desarrollo de Aplicación Móvil para la verificación de cumplimiento de los controles de la ISO 27001:2022.

Pantalla de la Aplicación ISO 27001, desarrollada para verificar el nivel de cumplimiento de los controles de la ISO 27001:2022.

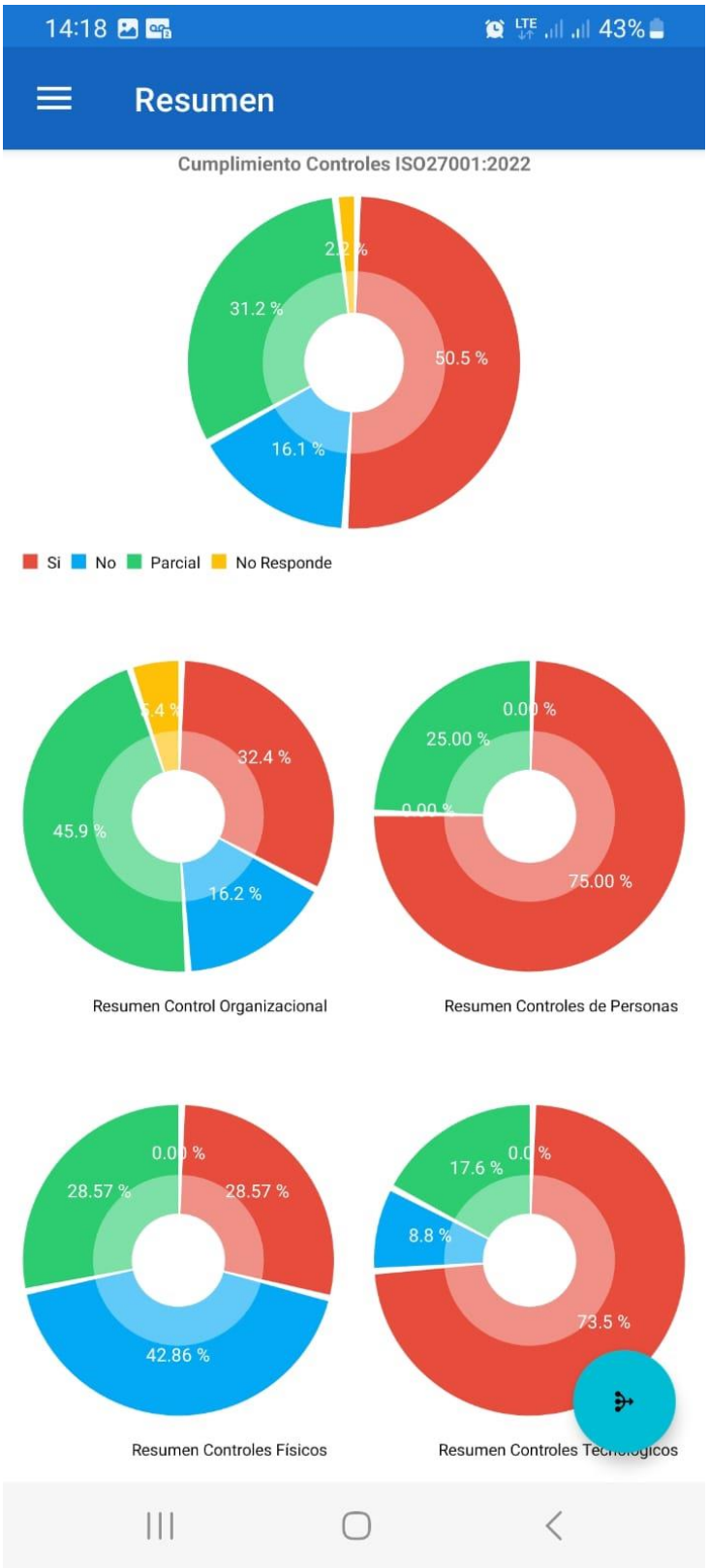
Esta Aplicación Móvil esta disponible para todo tipo de empresa que desee verificar su estado de cumplimiento de la normativa.

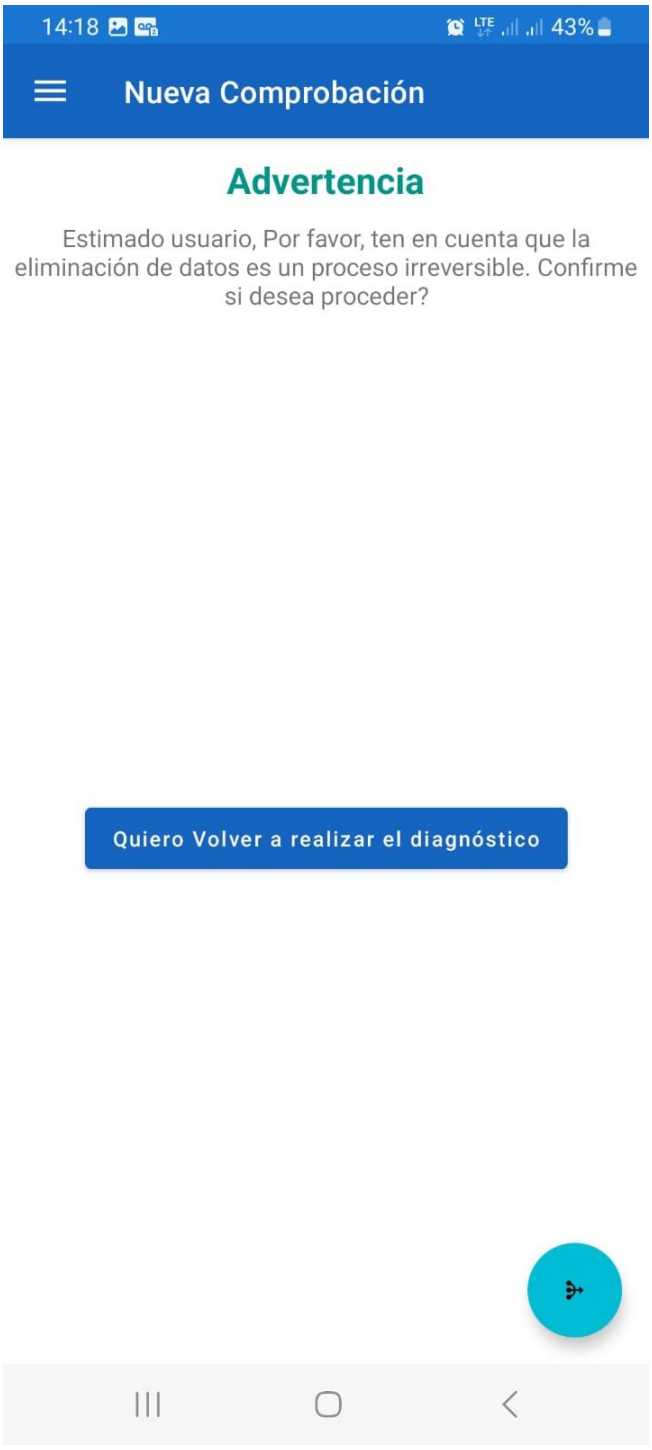
La aplicación está disponible para versiones Android 8.0 a posterior.



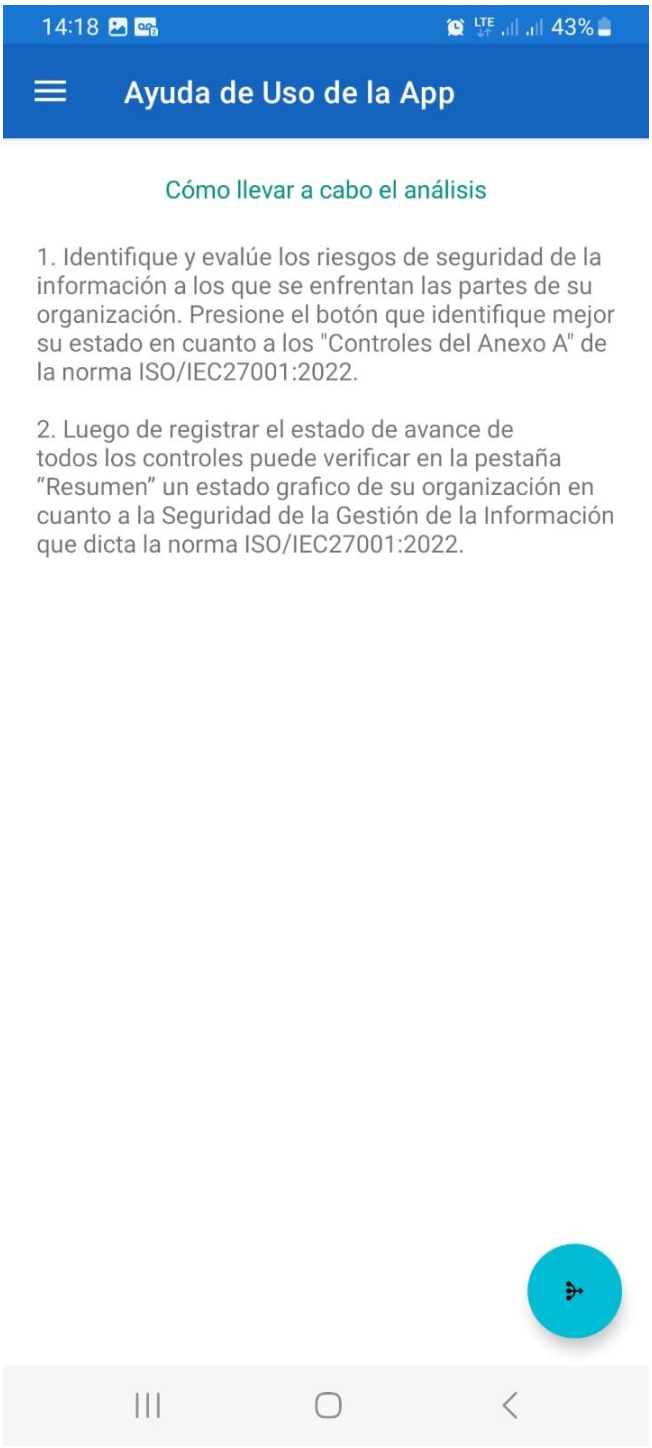
Menú Principal

Lista de Controles


14:18
43%
Resumen
Cumplimiento Controles ISO27001:2022
2.2 %
31.2 %
50.5 %
16.1 %
Si
No
Parcial
No Responde
32.4 %
45.9 %
16.2 %
Resumen Control Organizacional
0.00 %
25.00 %
75.00 %
Resumen Controles de Personas
0.00 %
28.57 %
28.57 %
42.86 %
Resumen Controles Físicos
17.6 %
0.0 %
8.8 %
73.5 %
Resumen Controles Tecnológicos


14:18
43%
Nueva Comprobación
Advertencia
Estimado usuario, Por favor, ten en cuenta que la eliminación de datos es un proceso irreversible. Confirme si desea proceder?
Quiero Volver a realizar el diagnóstico


14:18
43%
Acerca de
Todos los contenidos de esta Aplicación son propiedad de la Universidad Don Bosco. Pueden ser reproducidos libremente para fines no lucrativos por cualquier persona o entidad, siempre que se indique claramente la fuente. Los escudos, logotipos, fotografías y otros gráficos institucionales son propiedad de la Universidad Don Bosco. El diseño gráfico de esta Aplicación de la Universidad Don Bosco. Prohibida su reproducción total o parcial por cualquier medio sin permiso escrito de las autoridades universitarias.
Desarrollado por:
Eliseo Eulises Romero Ayala
Claudia Valentina Salazar Ruano
Trabajo de Graduación Titulado:
Modelo de políticas de seguridad y gestión de la información, basados en la ISO27001, aplicables a las cooperativas de Ahorro y Crédito del municipio de San Vicente, departamento de San Vicente, El Salvador.
Propuesta de Trabajo de Grado para Optar el Título de Maestro(a) en Seguridad y Gestión de Riesgos Informáticos.
2024 - Derechos Reservados para Universidad Don B


14:18
43%
Ayuda de Uso de la App
Cómo llevar a cabo el análisis
1. Identifique y evalúe los riesgos de seguridad de la información a los que se enfrentan las partes de su organización. Presione el botón que identifique mejor su estado en cuanto a los "Controles del Anexo A" de la norma ISO/IEC27001:2022.
2. Luego de registrar el estado de avance de todos los controles puede verificar en la pestaña “Resumen” un estado grafico de su organización en cuanto a la Seguridad de la Gestión de la Información que dicta la norma ISO/IEC27001:2022.

Enlace de descarga de la Aplicación para Android 8.0 o superior.

6 Conclusiones

En un mundo cada vez más dependiente de la información digital, la seguridad de los datos es fundamental para proteger la integridad y confidencialidad de la información, tanto como para mantener la confianza de los clientes y la reputación de la organización.

Es evidente que existe una brecha en la preparación y conciencia sobre seguridad informática en las cooperativas de ahorro y crédito del municipio de San Vicente. Aunque podemos resaltar que en su mayoría los empleados reciben asesoramiento ocasional y perciben la seguridad de la información como útil, hay una serie de incertidumbre sobre la preparación de las instituciones para hacer frente a las amenazas cibernéticas actuales.

El hecho de que los empleados estén abiertos a recibir capacitaciones sobre políticas de seguridad informática, acceso a datos y auditoría de revisión de la seguridad de la información resalta en ellos la preocupación que se tiene sobre los peligros a que enfrentan como usuarios y las cooperativas como entes que manejan dicha información tan sensible e importante, el mantener la privacidad, confidencialidad e integridad de la información.

La ausencia de una seguridad en el acceso a los datos de los empleados, socios o de la organización misma, conlleva riesgos significativos para cualquier organización financiera, dada la privacidad y confidencialidad que estos presentan. Esto incluye la posibilidad de brechas de seguridad, pérdida de información sensible, violaciones de la privacidad y exposición a ciberataques. A esto también se le puede sumar la generación de pérdidas financieras, daño a la reputación y repercusiones legales. Además, puede erosionar la confianza de los clientes y socavar la competitividad de la organización en un entorno empresarial cada vez más digitalizado y competitivo.

Por tanto, la ausencia de políticas claras en una organización puede conducir a una serie de peligros, como la falta de dirección y coherencia en las operaciones, la confusión entre

los empleados sobre expectativas y procedimientos, la toma de decisiones inconsistentes y la exposición a riesgos legales y de cumplimiento.

7 Recomendaciones

El incesante desarrollo de tecnologías conlleva también un continuo crecimiento en las amenazas y riesgos que las cooperativas y cualquier organización deben enfrentar para garantizar la Confidencialidad, Integridad y Disponibilidad de la información, para afrontar este reto se recomienda que las cooperativas implementen políticas de seguridad basadas en estándares reconocidos internacionalmente como lo es la ISO 27001, dado que estas políticas con sus respectivos controles serían los pilares fundamentales que permitirían el desarrollo de la organización en una forma estable, segura, brindar confianza a sus clientes, y mejorar o mantener la reputación de la cooperativa.

La implementación de controles y auditorías periódicas permitirá verificar el cumplimiento de las políticas, y las prácticas de seguridad como copias de respaldo, pruebas de restablecimiento y simulacros de emergencia son indispensables para que la cooperativa sea resiliente, ya que no se pueden eliminar completamente los riesgos de una falla en los sistemas.

Es recomendable que las cooperativas implanten una sólida política de seguridad desde temprano en su crecimiento, pero además es necesario que estas políticas sean analizadas, revisadas y actualizadas regularmente, para que vayan adaptándose al desarrollo de la cooperativa, cambios tecnológicos y surgimiento nuevos riesgos y amenazas, y, solo así se podría garantizar una eficiencia de las políticas y la mejora continua de la cooperativa.

Uno de los factores clave en la seguridad de la información es el factor humano, por ende, las cooperativas deben cuidar que los empleados, socios y terceros sean conscientes del daño que puede hacer una vulneración de la seguridad de datos a toda la cooperativa y que

adquieran el compromiso de manejar con la debida cautela la información a la que tienen acceso, además de hacerles ver las implicaciones administrativas o legales que puede tener un mal manejo de ella, o el no cumplimento con las políticas establecidas.

Por último, se recomienda a las cooperativas aquí estudiadas, el continuo mejoramiento de los controles de seguridad de la información, así como también la adaptación de los modelos de políticas planteadas en este documento, para que estas le sirvan de base para futuras medidas de control en cuanto a la seguridad.

8 Bibliografía

[1] «ESET Security Report 2023: el panorama de la seguridad en las empresas de América Latina». [En línea]. Disponible en: https://www.welivesecurity.com/es/informes/eset-security-report-2023-seguridad-empresas-america-latina/. [Accedido: 07-feb-2024].

[2] «INSAFOCOOP». [En línea]. Disponible en: https://www.insafocoop.gob.sv/?page_id=1722. [Accedido: 18-may-2024].

[3] «Cuál es la diferencia entre banco y cooperativa | Financiera Comultrasan». [En línea]. Disponible en: https://www.financieracomultrasan.com.co/es/5-diferencias-entre-las-cooperativas-y-los-bancos. [Accedido: 08-abr-2024].

[4] R. D. Estrada-Esponda, J. L. Unás-Gómez, O. E. Flórez-Rincón, R. D. Estrada-Esponda, J. L. Unás-Gómez, y O. E. Flórez-Rincón, «Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá», *Rev. Logos Cienc. & Tecnol.*, vol. 13, n.º 3, pp. 98-110, oct. 2021.

[5] «Nc-Iso-Iec 2382-1 PDF | PDF | Programa de computadora | Programación». [En línea]. Disponible en: https://es.scribd.com/document/488864641/NC-ISO-IEC-2382-1-pdf. [Accedido: 07-feb-2024].

[6] «Política y objetivos de seguridad - Documentación de IBM». [En línea]. Disponible en: https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives. [Accedido: 07-feb-2024].

[7] «¿Qué es un ciberataque? | IBM». [En línea]. Disponible en: https://www.ibm.com/es-es/topics/cyber-attack. [Accedido: 07-feb-2024].

[8] «ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements». [En línea]. Disponible en: https://www.iso.org/standard/27001. [Accedido: 03-feb-2024].

[9] «Certificación ISO 27001 - Sistema de seguridad de la información | NQA». [En línea]. Disponible en: https://www.nqa.com/es-pe/certification/standards/iso-27001-2022. [Accedido: 03-feb-2024].

[10] «ISO 27001 Última Versión 2022: Novedades y Cambios Más Importantes». [En línea]. Disponible en: https://blog.innevo.com/ISO 27001-2022. [Accedido: 03-feb-2024].

[11] «Nueva ISO 27002:2022». [En línea]. Disponible en: https://www.ide-solution.com/nueva-iso-27002-2022/. [Accedido: 03-feb-2024].

[12] «¿Qué es PCI DSS? | PCI Hispano». [En línea]. Disponible en: https://www.pcihispano.com/que-es-pci-dss/. [Accedido: 03-feb-2024].

[13] «¿Qué es Los 12 requisitos PCI DSS? - Definición en Computer Weekly». [En línea]. Disponible en: https://www.computerweekly.com/es/definicion/Los-12-requisitos-PCI-DSS. [Accedido: 03-feb-2024].

[14] «COBIT: Modelo para Auditoría y Control de Sistemas de Información».

[15] «ITIL 4: Las mejores prácticas en Gestión de Servicios de TI». [En línea]. Disponible en: https://www.itil.com.mx/. [Accedido: 03-feb-2024].

[16] «Ley de Protección de Datos», *Gastroenterología y Hepatología Continuada*, vol. 7, n.º 2. pp. 95-99, 2008.

[17] «Ley de Bancos cooperativas y sociedades de ahorro y crédito». [En línea]. Disponible en: https://ssf.gob.sv/wp-content/uploads/2023/02/Ley-de-Bancos-Cooperativos-y-Sociedades-de-Ahorro-y-Credito.pdf. [Accedido: 03-feb-2024].

[18] «Ley Especial Contra Delitos Informaticos y Conexos». [En línea]. Disponible en: https://www.fiscalia.gob.sv/medios/portal-transparencia/normativas/normativas-de-interes/ley-especial-contra-delitos-ciberneticos.pdf. [Accedido: 18-may-2024].

[19] «Marco Legal - Firma Electrónica». [En línea]. Disponible en: https://firmaelectronica.economia.gob.sv/marco-legal/. [Accedido: 18-may-2024].

[20] «DSS05 Gestionar Servicios de Seguridad – Procesos Cobit 5». [En línea]. Disponible en: https://adminsisuc201701.wordpress.com/dss05/. [Accedido: 18-may-2024].

[21] R. Hernandez Sampieri, C. Fernandez Collado, y P. Baptista Lucio, «Metodología de la Investigación». [En línea]. Disponible en: https://www.icmujeres.gob.mx/wp-content/uploads/2020/05/Sampieri.Met.Inv.pdf. [Accedido: 07-feb-2024].

[22] L. Gürtler y G. L. Huber, «MODOS DE PENSAR Y ESTRATEGIAS DE LA INVESTIGACION CUALITATIVA».

9 Anexos

Anexo 1. Encuesta a Empleados de la Institución

Universidad Don Bosco

Maestría en Seguridad y Gestión de Riesgos Informáticos

EMPLEADOS DE LA INSTITUCIÓN

Nombre institución: **ANÓNIMA**

Tema: Modelo de políticas de seguridad y gestión de la información, basados en la ISO 27001, aplicables a las cooperativas de Ahorro y Crédito del municipio de San Vicente, departamento de San Vicente, El Salvador.

Indicaciones: La información aquí recolectada será de estricta confidencialidad y para usos de la investigación sobre actual en cuanto a las políticas de seguridad y gestión de la seguridad de la información de las cooperativas del municipio de San Vicente.

A continuación, se presentan una serie de aspectos relevantes, que debes contestar con la mayor sinceridad posible, marcando con una X sobre lo que consideres mejor tu opinión.

Objetivo 1

1. ¿Cuál o cuáles normativas en seguridad de la información conoce?

( ) ISO 27001 ( ) ISO27002 ( ) NIST
( ) COBIT ( ) ITIL ( ) MAGERIT ( ) Ninguna

2. En la gestión de seguridad de la empresa ¿Qué normativa o marco de trabajo se aplica en la gestión de seguridad de la información?

( ) ISO 27001 ( ) ISO27002 ( ) NIST
( ) COBIT ( ) ITIL ( ) MAGERIT ( ) No se

Objetivo 2

3. ¿Qué tan frecuente recibe asesoría o capacitación sobre seguridad y riesgos informáticos?

( ) Muy frecuentemente ( ) Frecuentemente ( ) Ocasionalmente ( ) Raramente ( ) Nunca
Otro, especifique: _____

4. ¿Considera adecuado el asesoramiento y/o capacitación que ha recibido en relación con la seguridad de la información y los riesgos informáticos?

( ) Totalmente de acuerdo ( ) De acuerdo ( ) Indeciso ( ) En desacuerdo ( ) Totalmente en desacuerdo

5. ¿Considera que la institución está preparada para enfrentar amenazas informáticas actuales como Phishing, Malware, Hacking, Ransomware?

( ) Totalmente de acuerdo ( ) De acuerdo ( ) Indeciso ( ) En desacuerdo ( ) Totalmente en desacuerdo

6. ¿Considera que la seguridad en materia de riesgos informáticos de la institución es la adecuada?

( ) Totalmente de acuerdo ( ) De acuerdo ( ) Indeciso ( ) En desacuerdo ( ) Totalmente en desacuerdo

7. ¿Le gustaría recibir capacitación y/o asesoría en el área de políticas de seguridad informática aplicables a las necesidades de la institución, que contribuya a la mejora continua?

( ) Totalmente de acuerdo ( ) De acuerdo ( ) Indeciso ( ) En desacuerdo ( ) Totalmente en desacuerdo

8. ¿La institución cuenta personal informático dedicado al área de la ciberseguridad?

( ) SI ( ) NO ( ) No se

9. ¿En la institución existe un departamento de TI?

( ) SI ( ) NO ( ) No se

10. ¿La institución cuenta con directrices o políticas para el uso seguro de los equipos y datos informáticos por parte de los empleados?

( ) SI ( ) NO ( ) No se

11. ¿Cada cuanto cambia la contraseña de correo electrónico?

( ) Nunca la cambio ( ) Cada mes ( ) Cada dos meses ( ) Cada 6 meses

12. ¿Qué método usa para NO olvidar las contraseñas?

( ) La anoto de un papelito ( ) La escribo en el escritorio de la computadora ( ) La tengo escrita en la cartera
( ) Uso un baúl de contraseñas ( ) Uso una contraseña maestra

13. ¿Qué tan frecuente recibe capacitaciones sobre Phishing, Malware, Hacking, Ransomware?

( ) Muy frecuentemente ( ) Frecuentemente ( ) Ocasionalmente ( ) Raramente ( ) Nunca

14. ¿Tiene conocimiento si existe una política de control de acceso a la información en la institución?

( ) SI ( ) NO ( ) No se

15. ¿Tiene conocimiento de la existencia de políticas de seguridad de la información?

( ) SI ( ) NO ( ) No se

Objetivo 3

16. ¿La institución cuenta con directrices para el manejo de contraseñas? por ej. El uso de contraseñas fuertes, uso de autenticación de doble factor

( ) SI ( ) NO ( ) No se

17. ¿La institución cuenta con procedimientos para dar de baja/alta a un empleado?, Ej. cuando un empleado es despedido, sus credenciales son deshabilitadas inmediatamente

( ) SI ( ) NO ( ) No se

18. ¿Dentro de la institución existen lineamientos para el acceso a datos por parte de los empleados de forma que cada empleado tiene acceso solamente a la información requerida para su trabajo?

( ) SI ( ) NO ( ) No se

19. ¿Existen medidas de seguridad en computadoras y móviles dentro de la empresa?

( ) SI ( ) NO ( ) No se

20. ¿Puede instalar cualquier software en la computadora?

( ) SI ( ) NO ( ) No se

21. ¿Existen restricciones al momento de instalar software que no pertenecen a la institución?

( ) SI ( ) NO ( ) No se

Objetivo 4

22. ¿Tiene conocimiento, si las operaciones realizadas en los sistemas informáticos están debidamente registradas mediante logs o registros?, Ej. Bitácora de acciones

( ) SI ( ) NO ( ) No se

23. ¿Qué tan frecuente se realizan revisiones de las medidas de seguridad de la información con que cuenta la institución?

( ) Muy frecuentemente ( ) Frecuentemente ( ) Ocasionalmente ( ) Raramente ( ) Nunca

24. ¿Qué tan frecuente es capacitado o se le sensibiliza acerca de la importancia de la protección de datos de la institución?

( ) Muy frecuentemente ( ) Frecuentemente ( ) Ocasionalmente ( ) Raramente ( ) Nunca

25. ¿Qué tan frecuente se realizan auditorías a la información dentro de la institución?

( ) Muy frecuentemente ( ) Frecuentemente ( ) Ocasionalmente ( ) Raramente ( ) Nunca

Objetivo 5

26. ¿Tiene conocimiento su se utilizan mecanismos de encriptación para proteger la información sensible de la institución y sus clientes?

( ) SI ( ) NO ( ) No se

27. ¿Con que frecuencia se realizan copias de seguridad de la información de los clientes y empresa?

( ) Muy frecuentemente ( ) Frecuentemente ( ) Ocasionalmente ( ) Raramente ( ) Nunca

28. ¿La red esta segmentada de tal manera que haya distinción de acceso entre unidades?

( ) SI ( ) NO ( ) No se

29. ¿Considera que es importante que haya una segmentación de la red?

( ) Muy importante ( ) Importante ( ) Moderadamente ( ) Poco importante ( ) Sin importancia

30. ¿La red inalámbrica disponible para los invitados está separada de la red de los empleados de la institución.?

( ) SI ( ) NO ( ) No se

Gracias por valiosa colaboración