CAIGG
CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO
Ministerio Secretaría General de la Presidencia

Guía de Auditoría, Seguridad de la Información y Ciberseguridad N°6

SEGURIDAD EN REDES

ÍNDICE

Nota

PRESENTACIÓN

En cumplimiento con las instrucciones del Presidente de la República, Gabriel Boric Font, sobre fortalecimiento de la Política de Auditoría Interna de Gobierno; el Consejo de Auditoría Interna General de Gobierno, entidad asesora en materias de auditoría interna, control interno, probidad, gestión de riesgos y gobernanza del Supremo Gobierno, presenta a la Red de Auditoría Gubernamental, la GASIC N°6: Seguridad en Redes.

Esta guía es parte de una iniciativa del Consejo de Auditoría Interna General de Gobierno (CAIGG) que busca fortalecer la posición del sector público en materias de Seguridad de la Información y Ciberseguridad, dotando de instrumentos a los Auditores Internos y Servicios Públicos de instrumentos y herramientas que permitan desarrollar un levantamiento de información en base a las mejores prácticas y la legislación vigente.

Santiago, Mayo 2024.

Daniela Caldana Fulss
Auditora General de Gobierno

Capítulo 1

CONCEPTO DE SEGURIDAD EN REDES

¿Qué es la seguridad en redes?
Comprenderemos “seguridad en redes” como un conjunto de *medidas y procedimientos diseñados para salvaguardar la integridad, disponibilidad, confidencialidad, autenticidad y control de la información transmitida y almacenada en entornos informáticos* es decir, en el ciberespacio. Esta disciplina busca proteger los datos y sistemas contra las ciber-amenazas y riesgos de ciberseguridad, como, por ejemplo: Accesos no autorizados, modificaciones no deseadas, interrupciones, malware, entre otros.
Los objetivos principales de la seguridad en redes incluyen garantizar que solo usuarios autorizados tengan acceso a la información, prevenir la pérdida o alteración de datos críticos, mantener la funcionalidad de los sistemas y redes en todo momento y garantizar que las comunicaciones sean seguras y confiables. Para lograr estos objetivos, se implementan políticas, procedimientos, tecnologías y herramientas específicas de seguridad, que pueden variar según las necesidades y el entorno de cada organización.

Nota Importante

Estrictamente hablando, **Seguridad de la Información y Ciberseguridad** son dos conceptos diferentes.

La **“Seguridad de la Información”** es la preservación de la Confidencialidad, Integridad y Disponibilidad de la Información en los activos de información, en cualquier medio (incluso, las personas); por otro lado **“Ciberseguridad”** hace referencia exclusiva al ciberespacio y activos digitales.

En esta guía adoptamos el concepto de “Seguridad de la Información y Ciberseguridad”, pero para evitar la redundancia y el exceso de texto, utilizaremos los conceptos de “Seguridad de la Información”, “Ciberseguridad” o el acrónimo “SIC” como sinónimos para mejorar la comprensión lectora.

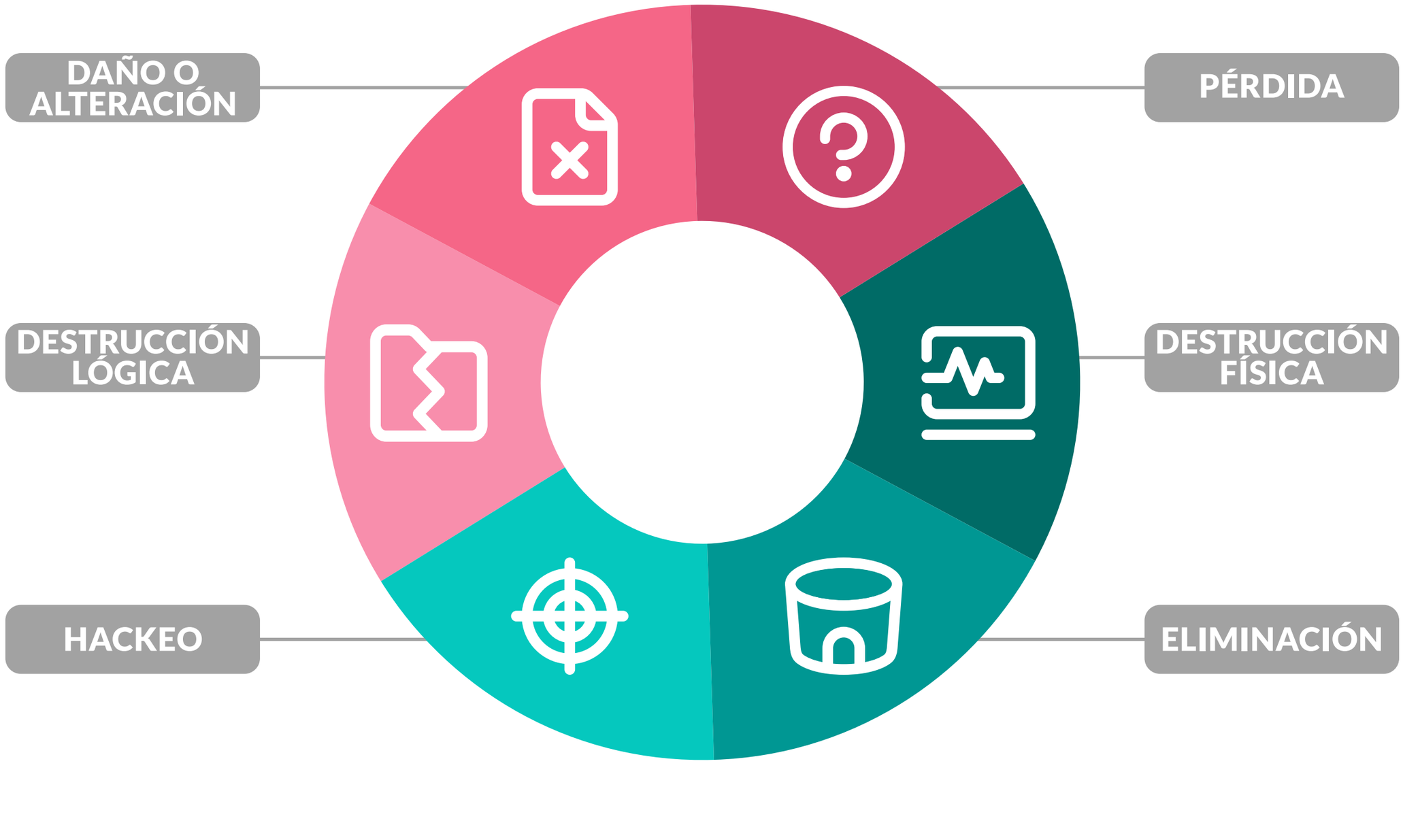

Figura 1. Amenaza a la Seguridad de Datos.

Capítulo 2

TIPOS DE SEGURIDAD

2.1 TIPOS DE SEGURIDAD

La seguridad en redes se puede segmentar en dos categorías principales, cada una de las cuales abarca una serie de aspectos específicos.

2.1.1 Seguridad Física y del Entorno

La seguridad física abarca mucho más que simplemente aplicar barreras y procedimientos de control. Se trata de un conjunto integral de medidas preventivas y contramedidas diseñadas para proteger los recursos y la información confidencial de un organización contra una variedad de amenazas, tanto internas como externas.

En el contexto de los centros de datos y entornos informáticos, se refiere a los controles y mecanismos implementados tanto dentro como alrededor de las instalaciones, así como a los medios de acceso remoto. Estos controles y mecanismos están diseñados para proteger el hardware, los medios de almacenamiento de datos y otros activos críticos de la organización.

Es esencial comprender que la seguridad física es fundamental incluso en entornos donde la ciber-seguridad es sólida. Por ejemplo, aunque una organización pueda tener una defensa robusta contra ataques externos como hackers y virus, la falta de medidas de seguridad física podría dejarla vulnerable ante amenazas como incendios o el simple robo de los computadores.

A menudo, solo algunos aspectos (como la instalación de cerraduras en las puertas y el control de acceso electrónico) son considerados, otros aspectos importantes, como la detección de intrusos internos que intentan acceder físicamente a áreas restringidas pueden ser descuidados. Estos fallos en la seguridad física pueden hacer que sea más fácil para un intruso acceder y comprometer los recursos de la organización, incluso más fácil que intentar hacerlo de manera remota a través de medios lógicos. Por lo tanto, es crucial abordar todos los aspectos de la seguridad física para garantizar la protección completa de los activos de la organización.

¿Por qué es importante la seguridad física?

Protege la Información Confidencial	Salvaguarda los datos sensibles, tales como información personal, registros financieros o secretos industriales, que constituyen objetivos valiosos para los ciberataques. La implementación de medidas de seguridad física y ambiental resulta crucial para impedir accesos no autorizados, prevenir daños o evitar la destrucción de esta información confidencial.
Preserva la Integridad de la Infraestructura	La infraestructura crítica, que abarca desde sistemas informáticos hasta redes de energía y transporte, representa el pilar fundamental para el funcionamiento óptimo de una organización. Es esencial implementar medidas de seguridad física y ambiental para salvaguardar esta infraestructura de posibles daños o actos de destrucción.
Resguarda la Reputación de la Organización	Cualquier incidente relacionado con la seguridad física o ambiental puede tener un impacto negativo en la imagen y reputación de una organización. Por lo tanto, es esencial implementar medidas efectivas de seguridad física y ambiental para reducir el riesgo de enfrentar tales incidentes y proteger así la reputación de la organización.

NOTA IMPORTANTE:

GASIC 4 "Control de Acceso e Identidades" ahonda en este tema con más profundidad y puede ser usado como una referencia para comprender más sobre este tema.

2.1.2 Desastres

Se centra en abordar las amenazas originadas tanto por la acción humana como por los eventos naturales que puedan afectar el entorno físico.

Las amenazas físicas más relevantes son:

- Catástrofes naturales como terremotos, incendios no intencionales, tormentas e inundaciones.
- Incidentes provocados por intervención humana.
- Actos de disturbios, sabotajes internos y externos deliberados.

A continuación, se realiza un análisis detallado de los riesgos más significativos que pueden surgir en un centro de procesamiento, con el propósito de establecer un conjunto de medidas que permitan prevenir, mitigar, recuperarse y corregir los distintos tipos de riesgos de manera efectiva y oportuna.

2.1.3 Incendios

Los incendios son originados por el uso indebido de combustibles, fallas en instalaciones eléctricas deficientes y el almacenamiento y transporte inapropiados de sustancias peligrosas. El fuego representa una amenaza significativa para la seguridad, siendo considerado el principal adversario de los sistemas informáticos debido a su capacidad para destruir fácilmente archivos y programas.

Lamentablemente, los sistemas de extinción de incendios presentan deficiencias significativas, a menudo causando daños similares a los ocasionados por el fuego, especialmente en dispositivos electrónicos. Por ejemplo, el dióxido de carbono, una alternativa al agua puede representar un riesgo para la seguridad de los empleados si quedan atrapados en la sala de servidores.

Para mitigar los riesgos de incendio en un centro de datos, es fundamental considerar diversos factores:

- El área de las computadoras debe ubicarse en un espacio de no combustible o inflamable.
- Evite proximidad con áreas de materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
- Utilice materiales incombustibles para las paredes, que deben extenderse desde el suelo hasta el techo.
- Instale un "falso piso" resistente al fuego sobre el piso real.
- Prohibir fumar en el área de procesamiento.
- Emplea muebles incombustibles y recipientes metálicos para los residuos. Evita materiales inflamables.
- Asegúrese que piso y techo del centro de datos sean impermeables y resistentes al fuego.

2.1.4 Seguridad del Equipamiento

Es esencial salvaguardar los dispositivos informáticos ubicándolos en zonas restringidas de acceso exclusivo para personal autorizado. Asimismo, se requiere que estas áreas estén equipadas con sistemas de ventilación eficientes y dispositivos de detección de incendios adecuados.

Para garantizar su protección, se deben considerar los siguientes aspectos:

- Control riguroso de la temperatura, manteniéndola por debajo de los 18° C, y control de la humedad, asegurando que no exceda el 65%, con el fin de prevenir el deterioro de los equipos.
- Implementación de sistemas de extinción de incendios adaptados al nivel de riesgo y al tipo de fuego que pueda surgir en el entorno.
- Instalación de extintores manuales (portátiles) y/o sistemas automáticos (rociadores) para intervenir en caso de emergencia.

2.1.5 Inundaciones

La inundación se define como el fenómeno en el que el agua se acumula en áreas planas debido al exceso de escorrentía superficial o a la falta de un sistema de drenaje adecuado, ya sea natural o artificial. Esta situación puede provocar graves desastres en las infraestructuras urbanas y rurales.

Además de las causas naturales de inundaciones, como lluvias intensas o deshielo, también pueden ocurrir inundaciones provocadas por eventos como incendios en pisos superiores. Para prevenir estos incidentes, se pueden implementar diversas medidas preventivas, como la instalación de techos impermeables para evitar la filtración de agua desde niveles superiores y la adaptación de puertas para contener el flujo de agua que desciende por las escaleras. Estas acciones ayudan a minimizar el riesgo de daños y protegen la seguridad de las personas y las propiedades.

2.1.6 Instalación Eléctrica

Trabajar con dispositivos informáticos implica manipular electricidad, lo que convierte a la seguridad eléctrica en una de las principales preocupaciones en el ámbito de la seguridad física. Este aspecto cobra relevancia tanto para el usuario doméstico como para las grandes empresas, ya que un mal manejo de la electricidad puede resultar en daños materiales e incluso poner en riesgo la integridad física de las personas.

Conforme los sistemas informáticos se vuelven más complejos y su integración en los procesos empresariales es más profunda, se hace evidente la necesidad de contar con expertos en seguridad. Estos especialistas tienen la tarea de evaluar los riesgos específicos asociados al uso de la electricidad en entornos informáticos y aplicar soluciones que cumplan con los estándares de seguridad industrial establecidos.
Además de identificar y mitigar riesgos para garantizar el cumplimiento de las normativas y regulaciones relacionadas con la seguridad eléctrica en el ámbito informático. Su labor es fundamental para prevenir accidentes, proteger los equipos y salvaguardar la continuidad operativa de las organizaciones.

Cableado:
Los medios utilizados para construir las infraestructuras de redes locales abarcan una amplia gama de opciones, desde el convencional cable telefónico hasta el cable coaxial o la fibra óptica. En la actualidad, muchos edificios de oficinas están siendo construidos con cableado preinstalado, lo que ayuda a reducir tanto el tiempo como el costo asociado con la instalación posterior. Además, esta práctica busca minimizar el riesgo de daños accidentales, como cortes o rozaduras, que puedan afectar la integridad de la red. Los riesgos más comunes asociados con el cableado pueden dividirse en varias categorías. En primer lugar, la interferencia electromagnética puede ser generada por fuentes externas, como cables de alimentación de maquinaria pesada o equipos de radio/microondas. A diferencia de los cables metálicos, los cables de fibra óptica son inmunes a este tipo de interferencia eléctrica, lo que garantiza una transmisión de datos más confiable.
Otro riesgo importante es el corte del cable, que interrumpe la conexión establecida y detiene el flujo de datos. Además, los daños físicos en el cable, como la ruptura del apantallamiento protector o el daño directo al cable en sí, pueden comprometer la integridad de las comunicaciones y afectar la fiabilidad de la red.
En la mayoría de las organizaciones, estos problemas se consideran como daños naturales; sin embargo, también pueden ser utilizados maliciosamente como medio para interferir en el funcionamiento de la red. Por ejemplo, un intruso podría intentar desviar o establecer conexiones no autorizadas en la red, lo que podría comprometer la seguridad de los datos transmitidos. Del mismo modo, el espionaje pasivo, conocido como "escucha", representa otra amenaza potencial, donde los datos pueden ser interceptados y comprometidos sin establecer una conexión directa.

Capítulo 3

SEGURIDAD LÓGICA

3.1 SEGURIDAD LÓGICA

La seguridad lógica abarca los procedimientos y controles específicos destinados a gestionar y proteger el acceso a sistemas informáticos y áreas físicas dentro de un centro de datos. Si bien el uso de puertas cerradas puede ser una práctica común para garantizar la seguridad física, implementar la autenticación de dos factores para acceder a estas áreas representa un nivel adicional de seguridad lógica.

Los controles de seguridad lógica tienen como objetivo principal proporcionar dirección y apoyo a la gestión, alineándose con los requisitos comerciales y los estándares de seguridad. Estos controles reflejan los objetivos empresariales y el compromiso con la protección de los datos, y es fundamental comunicarlos a todos los empleados de la organización.

Este enfoque de seguridad también se aplica a los sistemas informáticos. La utilización de contraseñas y perfiles de usuario es una práctica común para restringir el acceso, asegurando que solo el personal autorizado pueda acceder a los sistemas críticos. Sin embargo, la efectividad de estas medidas depende de la actualización y mantenimiento adecuados de las listas de acceso. Es esencial mantener actualizadas las listas de quién puede acceder a qué en el centro de datos para evitar accesos no autorizados, especialmente después de cambios en el personal.

La seguridad lógica no solo protege contra amenazas cibernéticas, sino que también ayuda a prevenir errores humanos que pueden resultar en tiempo de inactividad y otras consecuencias adversas para el sistema. Al implementar protocolos de seguridad lógica robustos y mantener actualizadas las listas de acceso de usuarios, las empresas pueden garantizar que sus datos valiosos estén protegidos contra accesos no autorizados y posibles amenazas.

Los objetivos establecidos para garantizar la seguridad lógica abarcan una serie de medidas destinadas a proteger la integridad, confidencialidad y disponibilidad de los sistemas de información. Estos incluyen:

01 **Limitar Accesos**
Limitar el acceso a los programas y archivos mediante la implementación de controles de acceso basados en roles y permisos.

02 **Garantizar la Autonomía**
Garantizar que los operadores puedan realizar sus tareas de manera autónoma, sin requerir una supervisión constante, al tiempo que se asegura que no puedan modificar o acceder a programas y archivos que no estén autorizados para ellos.

03 **Verificar Archivos y Programas**
Verificar que los archivos y programas utilizados sean los correctos y que se sigan los procedimientos establecidos para su utilización.

04 **Asegurar la Confidencialidad**
Asegurar la confidencialidad de la información transmitida, garantizando que solo el destinatario previsto pueda acceder a ella y que no sea interceptada por terceros no autorizados.

05 **Asegurar la Integridad**
Garantizar la integridad de la información durante su transmisión, evitando la manipulación o alteración de los datos en tránsito.

06 **Sistemas Alternativos**
Establecer sistemas alternativos de comunicación secundarios entre diferentes puntos para garantizar la continuidad del negocio en caso de fallas o interrupciones en la red principal.

07 **Procedimientos de Contingencia**
Implementar procedimientos de contingencia y planes de recuperación de desastres para garantizar la disponibilidad y el acceso a la información en situaciones de emergencia.

3.2 CONTROL DE ACCESOS

El control de acceso es un elemento esencial de seguridad que determina quién puede acceder a ciertos datos, aplicaciones y recursos, y en qué circunstancias. De la misma forma que las claves y listas de invitados con aprobación previa protegen los espacios físicos, las directivas de control de acceso protegen los espacios digitales.

En otras palabras, permiten a las personas adecuadas entrar y mantener a las personas equivocadas fuera. Las directivas de control de acceso se basan en gran medida en técnicas como autenticación y autorización, que permiten a las organizaciones comprobar explícitamente que los usuarios son quienes dicen ser y que a estos usuarios se les concede el nivel adecuado de acceso en función del contexto, como el dispositivo, la ubicación, el rol y mucho más.

El control de acceso evita que la información confidencial, como los datos de los clientes y la propiedad intelectual, sea robada por delincuentes u otros usuarios no autorizados. También reduce el riesgo de filtrado de datos por parte de los empleados y mantiene a raya las amenazas web. En lugar de gestionar los permisos manualmente, la mayoría de las organizaciones impulsadas por la seguridad recurren a soluciones de gestión de identidades y accesos para implementar directivas de control de acceso.

Estos pueden implementarse en el sistema operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

3.2.1 Identificación y Autenticación

La autenticación digital es un componente esencial de la mayoría de los servicios en línea y las tecnologías de la información y la comunicación (TIC). Por ejemplo, al cargar un video en un servidor, se requiere que el usuario esté registrado en el servicio y se autentique para poder completar la publicación del contenido. Del mismo modo, al utilizar una plataforma de redes sociales, es imprescindible que el usuario se registre y autentique su identidad. Además, los contactos en estas redes también deben ser identificados adecuadamente. Cuando realizamos transacciones como pagos con tarjeta de crédito, utilizamos esta misma tarjeta para autenticarnos. Al llevar a cabo operaciones bancarias en línea, lo primero que hacemos es identificarnos.

La identificación digital puede ser relativamente simple, como utilizar un nombre de usuario o una dirección de correo electrónico como identificador, o emplear el número de tarjeta de crédito para realizar pagos. Sin embargo, para la mayoría de los servicios, además de la identificación digital, se requiere una autenticación de esta identidad para garantizar la seguridad y la legitimidad de las transacciones.

Mediante la Autenticación de la Identidad, el Servicio se Asegura de que el Usuario es Quien Dice Ser

El término "identidad del usuario" se refiere al proceso de verificar y confirmar la autenticidad de un individuo dentro de un sistema o entorno específico. Este proceso se lleva a cabo mediante un identificador de usuario, que consiste en una cadena de caracteres que representa la identidad del individuo en cuestión. Para garantizar la autenticidad de esta identidad, se pueden emplear varias aproximaciones:

Conocimiento Exclusivo:
Un usuario puede demostrar que es quien dice ser si posee información confidencial que solo él conoce, como una contraseña secreta o una frase de acceso.

Características Físicas Únicas:
La identidad de un usuario puede verificarse mediante características físicas distintivas, como la huella dactilar, que son exclusivas de esa persona.

Poseer un Objeto Específico:
La autenticación se puede basar en la posesión física de un objeto único, una tarjeta magnética o una llave. Esta autenticación asemeja al propietario de una casa que posee las llaves correspondientes.

Comportamiento Único:
Algunas personas pueden autenticarse a través de acciones o comportamientos únicos, como un patrón de escritura o una forma particular de caminar.

Por Ejemplo:

- *Contar con una tarjeta de autenticación con códigos dinámicos para autorizar transacciones financieras en línea (como una tarjeta de coordenadas) podría interpretarse como una combinación de los dos escenarios anteriores:*

  El usuario posee físicamente la tarjeta, pero también se considera depositario de un conocimiento, aunque en este contexto esté registrado por escrito. Este método de autenticación multifactorial refuerza la seguridad al requerir que el usuario presente tanto un objeto físico (la tarjeta) como un conocimiento único (los códigos dinámicos), lo que hace que sea más difícil para los posibles infractores acceder de manera no autorizada a las cuentas bancarias en línea.

Además, todas estas metodologías para gestionar la autenticación no están libres de desafíos en términos de seguridad. Por ejemplo, la tarjeta de códigos podría ser objeto de sustracción y utilizada por un tercero no autorizado. Asimismo, existe el riesgo de que un atacante obtenga una contraseña de acceso mediante el phishing, una técnica que implica el envío de correos electrónicos fraudulentos para engañar a los usuarios y obtener información confidencial. Es importante considerar estas vulnerabilidades al implementar medidas de seguridad para proteger los sistemas y los datos.

Identificación V/S Autenticación

Es importante diferenciar estos dos conceptos, pues en ocasiones dan lugar a confusión

Identificación

La identificación es el proceso de garantizar que una persona es quien dice ser.

El proceso comienza el día en el que el usuario inicia su relación con la Institución de Tecnología Financiera (ITF) y se prolonga durante el ciclo de vida hasta que la persona deja de utilizar sus servicios.

- *Cómo se Registra*
- *Cómo lo va Conociendo la ITF con los Días*
- *Cómo Contrata y Consume los Servicios*

Esto forma parte de un proceso continuado donde se va conociendo al usuario y se intenta construir una relación de mutuo beneficio. En el argot del cumplimiento normativo y negocio financiero el proceso es conocido como *Know Your Customer (KYC)*

Autenticación

La autenticación se refiere a los mecanismos utilizados para acceder a los servicios, apps y/o transacciones.

Tiene como misión garantizar que el usuario accede a los servicios de base electrónica de una forma segura y debe garantizar que los mecanismos y/o secretos que usa para acceder a las apps y para la ejecución de transacciones financieras, son seguros para ingresar.

- *Cómo Ingresa a la Plataforma o Servicio*

¿Por qué la Identificación?

Confianza

La confianza es requerida para realizar los negocios y evitar un mal uso del capital.

¿Por qué la Autenticación?

Seguridad

La seguridad es necesaria para asegurar que los usuarios que realizan las operaciones se encuentran autorizados.

La identidad digital, es tan importante como la identidad física, inclusive se perfila como una tendencia que jurídicamente puede tener más peso por la interacción que tenemos en el mundo virtual que en el mundo físico, el “yo digital” es un ente con reconocimiento legal y ética digital.

Figura 2. Diferencias Entre Identificación y Autenticación.

3.2.2 Inicio de Sesión Único (SSO)

Es una funcionalidad que permite a los usuarios acceder a múltiples dispositivos, servicios y servidores con una sola autenticación. En lugar de ingresar credenciales en cada plataforma por separado, el SSO permite a los usuarios iniciar sesión una vez y acceder a todas las aplicaciones y recursos autorizados sin la necesidad de repetir el proceso de inicio de sesión.

3.2.3 Autenticación Multifactor (MFA)

La autenticación multifactor (MFA) es una medida de seguridad que requiere que los usuarios pasen por dos o más métodos de verificación de identidad para acceder a los sistemas. Estos métodos pueden incluir algo que el usuario conoce (como una contraseña), algo que el usuario tiene (como un token de hardware) y algo que el usuario es (como la autenticación biométrica). Al requerir múltiples formas de autenticación, el MFA aumenta la seguridad al hacer más difícil para los atacantes comprometer las cuentas de usuario.

3.2.4 Autenticación Basada en Riesgos

Es un método de autenticación que evalúa el nivel de riesgo asociado con un intento de inicio de sesión antes de requerir la autenticación adicional del usuario. Si se detecta un riesgo elevado, como un intento de inicio de sesión desde una ubicación inusual o con un dispositivo desconocido, se puede solicitar al usuario que pase por pasos de autenticación adicionales para verificar su identidad.

3.2.5 Gestión de Accesos: Autorización

La autorización es el proceso de determinar qué recursos puede acceder un usuario y qué acciones puede realizar en esos recursos una vez que ha sido autenticado. Esto incluye definir los derechos de acceso mínimos y estrictos para cada usuario, lo que garantiza que solo tengan acceso a la información y las funciones que son necesarias para realizar sus tareas laborales.

3.2.6 Gestión de Accesos con Privilegios (PAM)

Se utiliza para controlar y supervisar el acceso a sistemas, aplicaciones y datos confidenciales que requieren privilegios especiales. Estos privilegios suelen estar reservados para personal de TI, como administradores de sistemas y desarrolladores, que necesitan acceder a recursos críticos para realizar cambios y mantener la infraestructura de TI de la organización.

3.2.7 Gestión de Accesos Basada en Roles (RBAC)

La gestión de acceso basada en roles (RBAC) es un enfoque para la administración de accesos que asigna privilegios de acceso a los usuarios según los roles que desempeñan dentro de la organización. En lugar de asignar privilegios específicos a usuarios individuales, los privilegios se asignan a roles predefinidos y los usuarios se asignan a esos roles según sus responsabilidades laborales.

3.2.8 Restricción de Servicios

Estos controles se refieren a las limitaciones que están determinadas por parámetros específicos relacionados con la utilización de la aplicación, ya sea establecidos por defecto o por el administrador del sistema. Un ejemplo claro sería el caso en el que una organización cuenta con licencias que permiten la utilización simultánea de un determinado software por parte de cinco usuarios. En este escenario, se implementaría un control a nivel del sistema que impediría que un sexto usuario acceda al producto.

3.2.9 Formas de Acceso

La modalidad de acceso se refiere al tipo de permisos que se otorgan al usuario sobre los recursos y la información disponibles.
Estas modalidades pueden incluir:

Lectura:
Permite al usuario visualizar o leer la información, pero no realizar cambios en ella. Sin embargo, se debe tener en cuenta que la información puede ser copiada o impresa.

Escritura:
Con este tipo de acceso, el usuario puede agregar, modificar o eliminar información.

Ejecución:
Otorga al usuario el privilegio de ejecutar programas o procesos.

Eliminación:
Permite al usuario eliminar recursos del sistema, como programas, datos o archivos. El acto de borrar se considera una forma de modificación.

Además de estas modalidades básicas, existen otras formas de acceso que son más específicas y que generalmente se encuentran dentro de los sistemas de aplicación:

Creación:
Permite al usuario crear nuevos archivos, registros o campos en el sistema.

Búsqueda:
Facilita al usuario la capacidad de listar los archivos contenidos en un directorio específico para encontrar la información deseada.

3.3 CONTROL DE ACCESO INTERNO

3.3.1 Contraseñas

La autenticación mediante contraseñas es una forma común y relativamente sencilla de verificar la identidad de un usuario en un sistema informático. En este proceso, el usuario A proporciona su identificador (IDA) y su contraseña (CSA) al sistema. La implementación de este protocolo de identificación puede variar: puede requerir que ambos datos se envíen juntos en un mismo mensaje, o que primero se solicite el nombre de usuario y luego la contraseña.

La contraseña proporcionada por el usuario se utiliza para validar su identidad ante el servicio. Si el usuario A es el único que conoce la contraseña CSA, es altamente probable que sea realmente el usuario A. En el siguiente diagrama, se muestra cómo el usuario utiliza su contraseña para autenticarse ante el servicio. El servicio mantiene una lista de pares de usuarios y contraseñas para verificar las identidades. Cuando se proporciona una contraseña correcta, el servicio envía un mensaje de autenticación exitosa al equipo del usuario. Es importante destacar que este mensaje incluye un tiempo de caducidad para la autenticación, después del cual el usuario deberá volver a autenticarse.

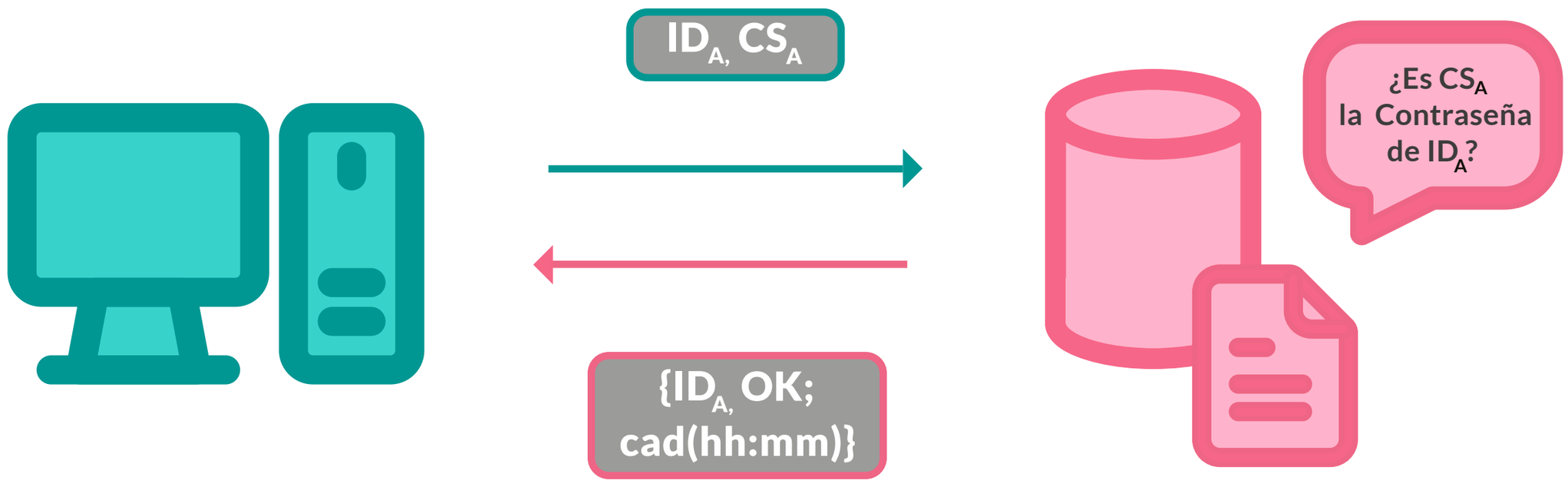

Figura 3. Esquema de Funcionamiento de Autenticación Mediante Contraseña

- **Sincronización de contraseñas:**

Implica permitir que un usuario acceda con la misma contraseña a varios sistemas interconectados y que esta se actualice automáticamente en todos ellos si se modifica. Esta funcionalidad puede percibirse inicialmente como una vulnerabilidad para la seguridad del sistema, ya que una vez que se descubra la contraseña de un usuario, se podría obtener acceso a los múltiples sistemas a los que este tiene privilegios. Sin embargo, investigaciones realizadas sugieren que las personas suelen utilizar una sola contraseña para todos los servicios a los que acceden, y cuando se les exige utilizar diferentes contraseñas, tienden a anotarlas para no olvidarlas, lo que representa un riesgo aún mayor. Para implementar la sincronización de contraseñas entre sistemas, es fundamental que todos ellos mantengan un alto nivel de seguridad y protección.

- **Caducidad y control:**

Este mecanismo regula cuándo los usuarios pueden y deben cambiar sus contraseñas. Se establece un período mínimo durante el cual los usuarios pueden cambiar sus contraseñas y un período máximo después del cual estas expiran. Esto ayuda a garantizar la seguridad al obligar a los usuarios a actualizar sus contraseñas periódicamente, reduciendo así el riesgo de que las contraseñas comprometidas se utilicen de manera prolongada. Además, proporciona un control sobre la gestión de contraseñas dentro del sistema, lo que contribuye a mantener la seguridad de la información y los datos sensibles.

3.3.2 Criptografía

Los controles criptográficos se centran en salvaguardar la información en situaciones donde un intruso podría obtener acceso físico a los datos. Es esencial establecer un sistema de cifrado para aumentar la seguridad de la confidencialidad e integridad de los datos.

En primer lugar, en una política integral de implementación y administración de claves de cifrado de datos, se debe designar a un responsable encargado de su implementación y gestión.

La piedra angular de la política de controles criptográficos radica en:

- **Identificar qué información y en qué situaciones requiere el uso de claves criptográficas.**
- **Determinar los métodos adecuados para su implementación.**
- **Gestionar, mantener y actualizar de manera efectiva estos recursos de seguridad.**

3.3.3 Políticas de acceso

Se refiere a un registro que contiene los nombres de usuarios autorizados para acceder a un recurso específico del sistema, así como las modalidades de acceso permitidas. Estas políticas varían en su alcance y flexibilidad, pudiendo adaptarse a diferentes entornos y necesidades organizativas.

3.3.4 Restricciones en la interfaz de usuario

Estas restricciones, por lo general, se complementan con las políticas de acceso y limitan las acciones que los usuarios pueden realizar. Principalmente se dividen en tres tipos: restricciones de menú, de visualización en bases de datos y físicas en la interfaz del usuario.
Por ejemplo, en los cajeros automáticos, donde los usuarios solo pueden realizar ciertas operaciones presionando teclas específicas.

3.3.5 Etiquetas de seguridad

Son designaciones asignadas a recursos, como archivos, que sirven para diversos fines, como control de acceso y especificación de medidas de protección. Estas etiquetas son inalterables y ayudan a garantizar la seguridad y la integridad de los datos en todo momento.

3.4 CONTROL DE ACCESOS INTERNOS

3.4.1 Etiquetas de seguridad

Estos dispositivos regulan y gestionan el acceso a puertos específicos y pueden ser fácilmente independientes o integrados en otro dispositivo de comunicación, como por ejemplo un enrutador.

En este contexto, los dispositivos de gestión de puertos controlan qué dispositivos o usuarios tienen permiso para acceder a puertos específicos de la red, lo que contribuye a reforzar la seguridad y proteger los activos de la organización contra posibles amenazas externas.

3.4.2 Firewall o cortafuegos

Los firewalls, también conocidos como cortafuegos, son dispositivos o programas diseñados para bloquear o filtrar el tráfico entre dos redes, típicamente una red privada y una red externa, como Internet.

Los firewalls examinan el tráfico de red entrante y saliente en busca de posibles amenazas y aplican reglas predefinidas para permitir o bloquear el acceso a recursos específicos. Estas reglas pueden basarse en direcciones IP, puertos, protocolos o aplicaciones.

3.4.3 Gestión de acceso para personal externo o consultores

Dado que el personal externo o los consultores suelen tener acceso temporal a los sistemas de la organización, es crucial establecer políticas y procedimientos claros para administrar y controlar sus perfiles de acceso.

Esto implica definir qué recursos y datos pueden acceder, así como establecer medidas para garantizar que se respeten los requisitos de seguridad y privacidad de la organización durante el tiempo que estén activos. Además, se debe implementar un proceso efectivo de desactivación de cuentas una vez que el acceso ya no sea necesario.

Capítulo 4

SEGURIDAD EN REDES

4.1 INFRAESTRUCTURA DE RED

La red necesita una infraestructura sólida, ya que es la base de las comunicaciones digitales incluye el hardware, el software, los sistemas y los dispositivos que posibilitan el flujo de los datos en toda la empresa para conectar a los usuarios, los dispositivos, las aplicaciones y el Internet. Además, engloba los softwares y servicios tales como sistemas operativos y cortafuegos.

Debido a su relación con el exterior, es un punto débil que necesita protección, por lo que es esencial tener en cuenta medidas de seguridad, como segmentación de red, sistemas de detección de intrusiones y políticas de acceso. Esto contribuye a reducir los riesgos y resguardar los activos de la empresa ante posibles amenazas y vulnerabilidades.

A medida que las empresas avanzan en el desarrollo o uso de aplicaciones, el aumento del uso de datos requiere respuestas rápidas a eventos específicos, lo cual conlleva a aumentar la importancia de contar con la infraestructura de red adecuada, para tener una mayor conectividad, comunicación, acceso a los recursos compartidos, escalabilidad y eficiencia.

En cambio, la falta de la infraestructura de red y prácticas de seguridad podría generar una mala experiencia para los usuarios y ataques a la red que perjudicarían la productividad y la eficiencia de los empleados

4.2 CONFIGURACIÓN Y SEGURIDAD DE LOS ACTIVOS

La gestión de activos en redes es un factor fundamental para implementar como una solución de seguridad que nos ayude a conocer el alcance y complejidad de nuestros dispositivos. Un inventario permite tener una fuente única actualizable y completa de información. La mayoría de las nuevas instalaciones de sistemas operativos o aplicaciones vienen con ajustes preconfigurados que suelen ser inseguros o no suelen estar configurados adecuadamente teniendo en cuenta la seguridad.

Una defectuosa Gestión de los Activos expone rápidamente a la organización a una multiplicidad de amenazas de seguridad. Por un lado, conlleva a riesgos asociados al extravío o robo de activos críticos, que podrían suponer otros peligros, como la pérdida de la propiedad intelectual o de dinero para sustituir dichos equipos. Es necesario prevenir los accesos no autorizados, proteger los datos confidenciales, aplicar parches de seguridad, desactivar servicios innecesarios y utilizar cifrado para proteger la comunicación y prevenir ataques internos.

4.3 POLÍTICAS DE CONFIGURACIÓN, INSTALACIÓN DE SOFTWARE Y DE CONECTIVIDAD

Son conjuntos de directrices que la organización debe establecer para regular el manejo de dispositivos, software y conexiones de red dentro de su infraestructura. Es necesario establecer las medidas para la instalación y la utilización de software en equipos computacionales y servidores, pertenecientes a la organización, con el fin de asegurar la continuidad operativa, y prevenir fallas de los sistemas y ataques debido a malware.

En los procedimientos se establecen las restricciones para la instalación de programas en los dispositivos, debido a la probabilidad de que los programas sean descargados desde páginas dudosas y/o realicen acciones como ocupar una puerta trasera o backdoor. Es crucial definir roles y responsabilidades a los diferentes empleados de la organización, para asignar un control de acceso, establecer diferentes estándares para la configuración de dispositivos de red y sistemas, asegurando que estén correctamente configurados para resistir los ataques.

4.4 COMUNICACIONES DE RED

Las redes de comunicaciones es un aspecto esencial de TI en organizaciones de cualquier tamaño y tipo, son las que permiten la interconexión entre diferentes sistemas finales, lo que involucra no solo a los equipos de comunicaciones, sino también a los medios físicos por donde se transporta la información digital, es decir, que puede ser tanto cableada como inalámbrica y es crucial para el funcionamiento de cualquier red de computadoras, ya sea una red local (LAN) o una red de área amplia (WAN). Por otro lado, las técnicas de protección usadas en la actualidad no se restringen solo a mecanismos defensivos, por lo cual no se limitará únicamente a una perspectiva de seguridad de la información o ciberseguridad, sino a una combinación de ambas.

Las comunicaciones de las redes seguras garantizan que la información transmitida entre dispositivos solo sea accesible para aquellos que estén autorizados a verla. Esto se logra mediante técnicas de cifrado que protegen los datos de ser interceptados por terceros no autorizados, es fundamental que los datos transmitidos no sean alterados durante su tránsito a través de la red.

El no seguir las pautas de buenas prácticas o recomendaciones otorgadas, también influye en debilidades que pueda tener una infraestructura de comunicaciones. Adicionalmente a las condiciones accidentales, hay que agregar acciones deliberadas que pueden poner en riesgo los dispositivos y los medios de comunicación.

4.5 DATOS E INFORMACIÓN

La seguridad de datos e información es crucial para cualquier organización que maneje información sensible o confidencial, ya que implica una serie de medidas que garantizan la integridad, confidencialidad y disponibilidad de los datos en reposo y en tránsito. Se trata de un aspecto que tiene que ver con la protección de datos contra accesos no autorizados y para protegerlos de una posible corrupción durante todo su ciclo de vida.

Esto incluye el enmascaramiento de datos mediante técnicas como la seudonimización, anonimización y encriptación, asegurando que solo los usuarios autorizados tengan acceso a la información necesaria. También se deben cifrar los datos en dispositivos de usuario final y segmentar el procesamiento y almacenamiento de datos según su sensibilidad, manteniendo entornos separados para desarrollo, pruebas y producción. Esto es de suma importancia porque protege la privacidad de los individuos y la propiedad intelectual de la empresa, también evitar la interrupción o degradación al acceso a los datos. Cuando se implementa correctamente, las estrategias de seguridad de datos de forma sólida se protegerán los activos de información de una organización contra actividades de ciberdelincuentes, además de contra amenazas internas y errores humanos, que siguen siendo una de las causas principales de la vulneración de datos.

4.6 REGLAS Y CONTROLES

Los controles de seguridad son parámetros implementados en la organización para proteger diversos formatos de datos e infraestructuras importantes. Se considera un control o regla de seguridad cualquier tipo de protección o contramedida utilizada para evitar, detectar, contrarrestar o minimizar los riesgos de seguridad de la propiedad física, la información, los sistemas informáticos u otros activos.

La implementación de reglas y controles es crucial para prevenir y detectar el uso de software no autorizado y protegerse contra amenazas maliciosas. Esto implica aplicar medidas como la validación periódica de software y datos, establecer protecciones contra la obtención de archivos desde redes externas, instalar y actualizar regularmente herramientas de detección y reparación de malware, y escanear todo el tráfico entrante en busca de posibles amenazas.Es vital filtrar el tráfico de entrada, como el correo electrónico y las descargas, para protegerse contra información no solicitada y contenidos maliciosos, como el phishing. Esto se logra mediante el uso de servicios de filtrado DNS, filtros de URL basados en la red y bloqueando el acceso a sitios web conocidos o sospechosos de ser maliciosos, entre otras medidas.

Debido a la creciente tasa de ataques cibernéticos, los controles de seguridad de los datos son más importantes hoy que nunca. Al mismo tiempo, las regulaciones de privacidad de datos están creciendo de forma potencial en Chile por lo que es fundamental que las organizaciones refuercen sus políticas de protección de datos o se enfrenten a posibles multas.

4.7 MONITOREO Y REGISTRO

El monitoreo y registro en la seguridad de redes son fundamentales por varias razones cruciales. Primero, el monitoreo constante permite detectar actividades o condiciones inusuales, así como tráfico no autorizado, tanto entrante como saliente. Esto proporciona una capa de defensa anticipada, permitiendo a los equipos de seguridad responder rápidamente.

El monitoreo de red proporciona la información que los administradores de redes necesitan para determinar, en tiempo real, si la red está funcionando de manera óptima en la organización. Con herramientas como el software de monitoreo de redes, los administradores pueden identificar deficiencias y optimizar la eficiencia de manera proactiva, y más, también para detectar rápidamente las fallas de dispositivos o conexiones, o los problemas como los cuellos de botella de tráfico que limitan el flujo de datos. Estos sistemas pueden alertar a los administradores de los problemas por correo electrónico o mensaje de texto, y enviar informes mediante la analítica de red. Por último, la centralización de alertas y la implementación de un sistema de gestión de información y eventos de seguridad (SIEM) facilitan la correlación y el análisis de registros en todos los activos empresariales. Todas estas técnicas e implementaciones son piedras angulares en la defensa cibernética moderna, proporcionando una visibilidad crítica y capacidad de respuesta ante las amenazas en constante evolución.

4.8 PRUEBAS DE VULNERABILIDAD DEL SISTEMA

La prueba de seguridad de la red es el proceso de buscar posibles problemas de seguridad, esto pueden contener vulnerabilidades de software, protocolos inseguros, configuraciones incorrectas y otros errores que ponen a la organización en riesgo de explotación. Primero y principal, permiten identificar y evaluar posibles puntos débiles en la infraestructura de TI, aplicaciones y sistemas, para prevenir potenciales brechas de seguridad que podrían ser aprovechadas por actores maliciosos, ya sean internos o externos. Al analizar exhaustivamente los controles de seguridad implementados, las pruebas de vulnerabilidad proporcionan una visión clara de la postura de seguridad de una organización y ayudan a priorizar las medidas correctivas necesarias. Por ejemplo, una organización puede elegir una prueba de caja blanca o de caja negra para lograr diferentes objetivos de seguridad. Esta información permite a una empresa evaluar con mayor precisión su exposición al riesgo de ciberseguridad y tomar decisiones basadas en datos sobre la inversión en seguridad.

Las pruebas de vulnerabilidad proporcionan una base sólida para el cumplimiento normativo y regulatorio, como GDPR, HIPAA o PCI DSS, que requieren evaluaciones regulares de seguridad y la corrección oportuna de cualquier vulnerabilidad identificada. El incumplimiento de estas normativas puede resultar en sanciones financieras significativas y dañar la reputación de la organización. Por lo tanto, las pruebas de vulnerabilidad son una herramienta fundamental para garantizar el cumplimiento normativo y proteger la integridad de los datos de la organización y la confianza del cliente.

Capítulo 5

USO DE LA GUÍA PARA LA AUDITORÍA INTERNA

5.1 CÓMO UTILIZAR LA GUÍA PARA LA AUDITORÍA INTERNA

Para que el auditor interno pueda aprovechar al máximo esta publicación, es conveniente que se refiera a los instrumentos complementarios: Las preguntas de auditoría temáticas y el modelo de madurez general. Cada GASIC se compone de tres componentes:

Guía de Auditoría de la Seguridad de la Información y Ciberseguridad (GASIC):
Este es el cuerpo teórico y consiste en el marco contextual necesario para que el auditor interno comprenda el alcance y del dominio de seguridad que está evaluando. Es un instrumento con los conceptos fundamentales recopilados de mejores prácticas.

Modelo de Madurez:
Recopila controles desde las mejores prácticas asociadas al tema central de Guía de Auditoría, organiza los controles en una propuesta de madurez y permite al auditor conocer los requisitos que debería evaluar.

Ejemplos de Preguntas de Auditoría:
Complementa el modelo de madurez a través de una serie de preguntas organizadas en varios documentos. Cada documento representa un control que pertenece a uno de los ejes temáticos definidos al interior de la Guía de Auditoría.

La ilustración a continuación presenta esta estructura documental:

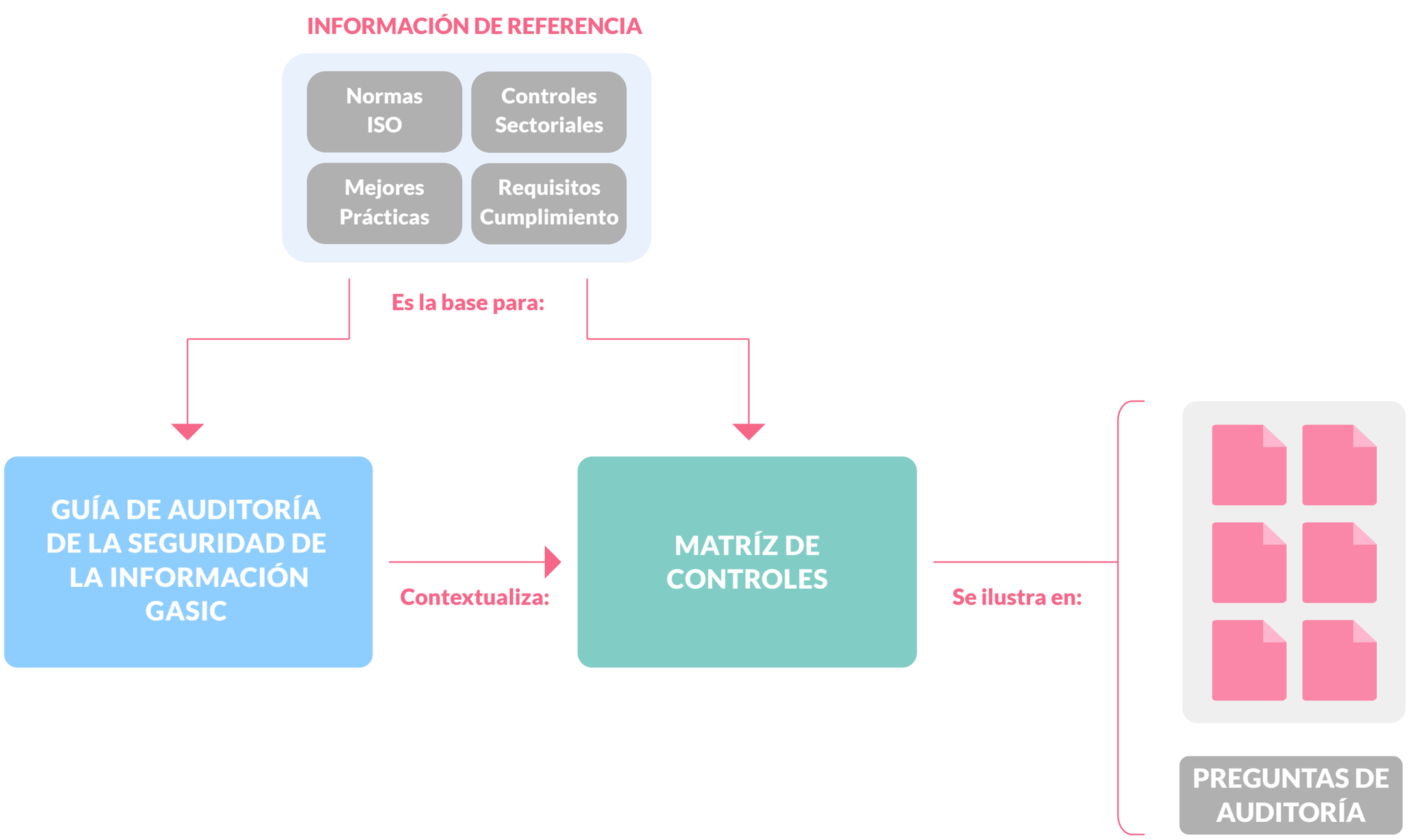

Figura 4. Modo de uso y Estructura Documental GASIC.

El método de trabajo sugerido es el siguiente:

01 **El auditor interno debe estudiar cada Guía de Auditoría y su contexto para tener plena comprensión del tema a trabajar.**

02 **A continuación, puede utilizar el Modelo de Madurez para seleccionar los controles que sean apropiados para la organización. La selección de controles debe estar alineados con:**

- **a. La estrategia de la organización.**
- **b. Los resultados de la evaluación de riesgos.**
- **c. Los requisitos de cumplimiento.**
- **d. La estrategia de auditoría interna, expresada en el plan.**

03 **Por último, puede utilizar los documentos de ejemplo para la planificación de las preguntas y pruebas que fuese a realizar. El formato del programa, plan, instrumentos, pruebas y reportería debe ser aquel solicitado en el contexto de cada auditoría, que está fuera del alcance de esta guía.**