Gestión de procesos de ciberseguridad en las organizaciones

Breve descripción:

En este componente se reconocerá la importancia sobre la responsabilidad y acciones que se deben asumir cuando se trata de salvaguardar los activos informáticos ante ataques de ciberseguridad que cada vez son más frecuentes.

Agosto 2023

Tabla de contenido

Introducción

Los marcos de gestión de riesgos de ciberseguridad deben basarse en los estándares y las mejores prácticas de la industria; por tanto, su cumplimiento debe ser fundamental. Se debe tener en cuenta en su establecimiento las pautas y las metodologías de prueba de penetración presentadas en los marcos comunes de gestión de riesgos, como el Estándar de seguridad de datos PCI (“PCI Security Standards Council”, 2018), ISO/IEC 27001 y 27002 (Organización internacional de normalización, 2013a, 2013b), los Controles de seguridad críticos de CIS (Centro para la seguridad de Internet, 2021) y el Marco NIST para mejorar la ciberseguridad de la infraestructura crítica (Instituto Nacional de Estándares y Tecnología, 2018). Basado en lo anterior, el siguiente video expone la importancia de la gestión de riesgos en una organización:

Video 1. La gestión de riesgos

Enlace de reproducción del video

Síntesis del video: La gestión de riesgos
Mantener la ciberseguridad en una organización no es algo que los equipos de TI deban manejar solos. Para prevenir de manera efectiva las infracciones, todos los empleados de una organización deben ser conscientes de los posibles riesgos. Entonces, ¿por dónde iniciar? El primer paso en toda gestión de riesgo consiste en su evaluación. Es necesario analizar el panorama actual de la empresa y a partir de allí revisar y establecer las políticas de seguridad de la información, con el fin de evitar infracciones de seguridad e interrupciones de la red. Luego, se presentan estas políticas en un documento para garantizar que todos los empleados estén al tanto de las ciber-amenazas relevantes. El objetivo es aumentar la conciencia de los empleados sobre los riesgos en curso para mantener una postura de seguridad óptima. La formación en gestión de riesgos garantiza que todo el equipo sepa cómo utilizar los sistemas y herramientas necesarios para mitigar los riesgos de ciberseguridad. Se deben asignar políticas y tareas a diferentes departamentos para crear una estrategia optimizada que describa qué equipos son responsables de qué acciones en caso de una intrusión. Finalmente, implementar un plan de ciberseguridad a nivel organizacional requiere personal experimentado que comprenda que entre todos los factores, el factor humano es uno de los más urgentes de atender.

1. Seguridad informática en la organización

Los problemas de seguridad cibernética son cada vez más problemáticos para las empresas de todos los tamaños, el delito cibernético aumentó en un 600 % durante la pandemia de COVID-19 y los costos del delito cibernético están aumentando a un ritmo alarmante. La implementación de un programa eficaz de gestión de riesgos es un componente esencial de la defensa contra los ataques cibernéticos y una prioridad para los directores de seguridad de la información y las organizaciones en general.

La gestión de riesgos de seguridad cibernética es el proceso de identificar, analizar y abordar los riesgos de seguridad de TI de una organización para prevenir futuros ataques cibernéticos y dar cuenta de las amenazas cibernéticas en curso.

Para prevenir el delito cibernético, los profesionales de TI deben desarrollar un marco sólido de seguridad cibernética que se adhiera estrictamente a las pautas, los estándares y las mejores prácticas relevantes. Mantener un programa eficaz de gestión de riesgos de ciberseguridad es complejo pero esencial.

Examinar los riesgos y su impacto potencial permite a las organizaciones crear objetivos estratégicos y disminuir el riesgo de ciberamenazas. Cuando un marco de gestión de riesgos se implementa correctamente, permite a las organizaciones comprender mejor la gama completa de riesgos a los que se enfrentan.

Cuanto mayor sea el conocimiento de una organización sobre estos riesgos, mejor podrá implementar medidas proactivas.

1.1 Privilegios de acceso y seguridad de la información

Los controles de acceso autentican y autorizan a las personas a acceder a la información que pueden ver y usar. El uso indebido de privilegios es una de las principales amenazas de seguridad cibernética en la actualidad, que a menudo resulta en pérdidas costosas e incluso puede paralizar las empresas. También es uno de los vectores de ataque más populares entre los piratas informáticos, porque cuando se lleva a cabo con éxito, brinda acceso gratuito a la parte más vulnerable de una empresa, a menudo sin generar ninguna alarma hasta que el daño ya está hecho. Existen "software" que empoderan a las empresas que buscan adelantarse a este riesgo creciente con un sólido programa de administración de acceso privilegiado que garantice que ninguna vía de acceso privilegiado a los activos de misión crítica quede sin administrar, sin conocer o sin monitorear. De ahí que todo proceso parta de las siguientes preguntas base:

Figura 1. Preguntas sobre la seguridad de la información

1. ¿Quién debe acceder a los datos de su empresa?
2. ¿Cómo se asegura de que a quienes intentan acceder realmente se les haya concedido ese acceso?
3. ¿Bajo qué circunstancias niega el acceso a un usuario con privilegios de acceso?

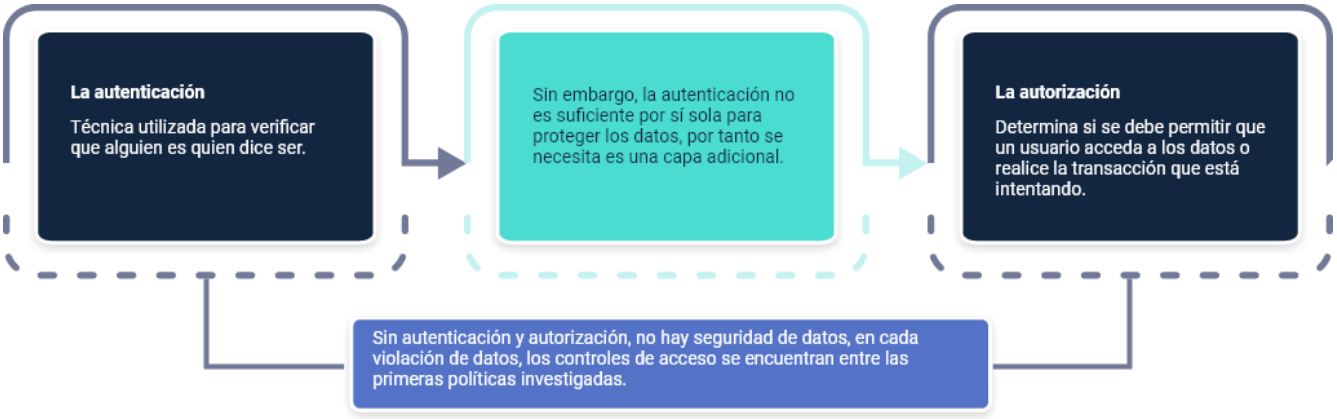
PDPA. Para proteger eficazmente sus datos, la política de control de acceso de su organización debe abordar estas (y otras) preguntas.

Lo que sigue es una guía de los conceptos básicos del control de acceso: qué es, por qué es importante, qué organizaciones lo necesitan más y los desafíos que pueden enfrentar los profesionales de la seguridad.

El control de acceso es un método para garantizar que los usuarios son quienes dicen ser y que tienen el acceso adecuado a los datos de la empresa. A un alto nivel, el control de acceso es una restricción selectiva del acceso a los datos. Consta de dos componentes principales: autenticación y autorización:

Ya sea la exposición inadvertida de datos confidenciales protegidos incorrectamente por un usuario final o la violación de un “software”, donde los datos confidenciales fueron expuestos a través de un servidor web público que opera con una vulnerabilidad de “software”, los controles de acceso son un componente clave. Cuando no se implementan o mantienen adecuadamente, el resultado puede ser catastrófico.

Figura 2. Autenticación y autorización de datos



- ✓ **La autenticación**

  Técnica utilizada para verificar que alguien es quien dice ser. Sin embargo, la autenticación no es suficiente por sí sola para proteger los datos, por tanto se necesita es una capa adicional.

- ✓ **La autorización**

  Determina si se debe permitir que un usuario acceda a los datos o realice la transacción que está intentando.

  Sin autenticación y autorización, no hay seguridad de datos, en cada violación de datos, los controles de acceso se encuentran entre las primeras políticas investigadas.

Cualquier organización cuyos empleados se conecten a Internet (en otras palabras, todas las organizaciones de hoy) necesita cierto nivel de control de acceso. Eso es especialmente cierto en el caso de las empresas con empleados que trabajan fuera de la oficina y requieren acceso a los recursos y servicios de datos de la empresa.

Dicho de otra manera: si sus datos pueden ser de algún valor para alguien sin la debida autorización para acceder a ellos, entonces su organización necesita un fuerte control de acceso.

Cualquier sistema de control de acceso, ya sea físico o lógico, tiene cinco componentes principales, descritos de esta manera:

1. **Autenticación**

   El acto de probar una afirmación, como la identidad de una persona o usuario de una computadora. Puede implicar la validación de documentos de identidad personal, la verificación de la autenticidad de un sitio web con un certificado digital o la verificación de las credenciales de inicio de sesión con los detalles almacenados.

2. **Autorización**

   La función de especificar derechos de acceso o privilegios a los recursos. Por ejemplo, el personal de recursos humanos normalmente está autorizado para acceder a los registros de los empleados y esta política suele formalizarse como reglas de control de acceso en un sistema informático.

3. **Acceso**

   Una vez autenticado y autorizado, la persona o computadora puede acceder al recurso.

4. **Administrar**

   Administrar un sistema de control de acceso incluye agregar y eliminar la autenticación y autorización de usuarios o sistemas. Algunos sistemas se

sincronizarán con G Suite o Azure Active Directory, lo que agilizará el proceso de administración.

5. **Auditoría**

   Se utiliza con frecuencia como parte del control de acceso para hacer cumplir el principio de privilegio mínimo. Con el tiempo, los usuarios pueden terminar con un acceso que ya no necesitan, por ejemplo, cuando cambian de rol. Las auditorías periódicas minimizan este riesgo.

Otra razón para un fuerte control de acceso es la minería de acceso. La recopilación y venta de descriptores de acceso en la "Dark web" es un problema creciente.

Por ejemplo, nuevos informes en la web describen cómo una "botnet" de criptominería, Smominru, extrajo no solo criptomonedas, sino también información confidencial, incluidas en direcciones IP internas, información de dominio, nombres de usuario y contraseñas. Los investigadores de este tipo de delitos creen que es altamente plausible que este actor de amenazas vendiera esta información en un mercado de acceso a otros, que luego podrían lanzar sus propios ataques por acceso remoto.

Estos mercados de acceso proporcionan una forma rápida y fácil para que los ciberdelincuentes compren acceso a sistemas y organizaciones. Estos sistemas pueden usarse como "zombis" en ataques a gran escala o como punto de entrada para un ataque dirigido. Un mercado de acceso, Ultimate Anonymity Services (UAS) ofrece 35 000 credenciales con un precio de venta promedio de $6.75 por credencial, por citar ejemplo de precios de este tipo de accesos sin control.

Los investigadores de estos ciberataques creen que los ciberdelincuentes aumentarán el uso de los mercados de acceso y la minería de acceso porque pueden ser altamente lucrativos para ellos. El riesgo para una organización aumenta si sus credenciales de usuario comprometidas tienen más privilegios de los necesarios.

La mayoría de los profesionales de seguridad entienden cuán crítico es el control de acceso para su organización, pero no todos están de acuerdo en cómo se debe aplicar, debido a los múltiples factores, que se evidencian en el siguiente video:

Video 2. Factores de control

Enlace de reproducción del video

Síntesis del video: Factores de control
El control de acceso requiere la aplicación de políticas persistentes en un mundo dinámico sin fronteras tradicionales. En entornos híbridos donde los datos se mueven desde los servidores locales o desde la nube a las oficinas, los hogares, los hoteles, los automóviles y las cafeterías con puntos de acceso Wi-Fi abiertos, la aplicación del control de acceso se torna más difícil. Al riesgo se suma que el acceso está disponible para una gama cada vez más amplia de dispositivos, que incluye PC, computadoras portátiles, teléfonos inteligentes, tabletas, parlantes inteligentes y otros dispositivos de Internet de las cosas (IoT). Esa diversidad hace que sea un verdadero desafío crear y asegurar la persistencia en las políticas de acceso. En el pasado, las metodologías de control de acceso a menudo eran estáticas. Hoy en día, el acceso a la red debe ser dinámico y fluido y admitir casos de uso basados en identidad y aplicaciones. Una política de control de acceso sofisticada se puede adaptar dinámicamente para responder a los factores de riesgo en evolución, lo que permite que una empresa cuya seguridad haya sido violada aísle a los empleados y los recursos de datos relevantes para minimizar el daño. Las empresas deben asegurarse de que sus tecnologías de control de acceso sean compatibles de manera constante a través de sus activos y aplicaciones en la nube y que se pueden migrar sin problemas a entornos virtuales como nubes privadas.

Las reglas de control de acceso deben cambiar en función del factor de riesgo, lo que significa que las organizaciones deben implementar capas de análisis de seguridad utilizando inteligencia artificial y aprendizaje automático que se asientan sobre la red y la configuración de seguridad existentes. También necesitan identificar amenazas en tiempo real y automatizar las reglas de control de acceso en consecuencia.

Por lo tanto, en una correcta gestión de control de acceso se deben tener presentes los factores involucrados, su evolución y la dinámica organizacional para buscar alcanzar las medidas más adecuadas de acuerdo con los activos que se buscan proteger y gestionar.

Las organizaciones deben determinar el modelo de control de acceso apropiado a adoptar según el tipo y la sensibilidad de los datos que están procesando. Los modelos de acceso más antiguos incluyen control de acceso discrecional (DAC) y control de acceso obligatorio (MAC), el control de acceso basado en roles (RBAC) es el modelo más común en la actualidad, así como el modelo más reciente se conoce como control de acceso basado en atributos (ABAC). Al respecto:

1. **Control de acceso discrecional (DAC):** con los modelos DAC, el propietario de los datos decide el acceso. DAC es un medio para asignar derechos de acceso en función de las reglas que especifican los usuarios.
2. **Control de acceso obligatorio (MAC):** MAC se desarrolló utilizando un modelo no discrecional, en el que a las personas se les otorga acceso en función de una autorización de información. MAC es una política en la que

los derechos de acceso se asignan con base en las regulaciones de una autoridad central.

3. **Control de acceso basado en funciones (RBAC):** RBAC otorga acceso en función de la función de un usuario e implementa principios de seguridad clave, como privilegio mínimo y separación de privilegios. Por lo tanto, alguien que intente acceder a la información solo puede acceder a los datos que se consideren necesarios para su función.
4. **Control de acceso basado en atributos (ABAC):** en ABAC, a cada recurso y usuario se le asigna una serie de atributos, explica Wagner. En este método dinámico, se utiliza una evaluación comparativa de los atributos del usuario, incluida la hora del día, la posición y la ubicación, para tomar una decisión sobre el acceso a un recurso.

Es imperativo que las organizaciones decidan qué modelo es el más apropiado para ellas en función de la sensibilidad de los datos y los requisitos operativos para el acceso a los datos. En particular, las organizaciones que procesan información de identificación personal (PII) u otros tipos de información confidencial, incluida la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA) o datos de Información no clasificada controlada (CUI), deben hacer del control de acceso una capacidad central en su arquitectura de seguridad, Wagner aconseja.

Varias tecnologías pueden admitir los diversos modelos de control de acceso. En algunos casos, es posible que varias tecnologías deban trabajar en conjunto para lograr el nivel deseado de control de acceso. La realidad de los datos distribuidos entre los proveedores de servicios en la nube, las aplicaciones y todos aquellos conectados al perímetro de la red tradicional dictan la necesidad de orquestar una solución segura.

Existen varios proveedores que brindan acceso privilegiado y soluciones de administración de identidades que se pueden integrar en una construcción tradicional de Active Directory. La autenticación multifactorial puede ser un componente para mejorar aún más la seguridad.

Hoy en día, la mayoría de las organizaciones se han vuelto expertas en autenticación, especialmente con el uso creciente de la autenticación multifactorial y la autenticación basada en biometría (como el reconocimiento facial o del iris). En los últimos años, dado que las violaciones de datos de alto perfil han resultado en la venta de credenciales de contraseñas robadas en la web oscura, los profesionales de la seguridad se han tomado más en serio la necesidad de la autenticación de múltiples factores (aunque a menudo, sigue siendo un área en la que los profesionales de la seguridad se equivocan).

Puede ser un desafío determinar y monitorear permanentemente quién obtiene acceso a qué recursos de datos, cómo deberían poder acceder a ellos y bajo qué condiciones se les otorga acceso, para empezar. Pero los protocolos de autorización inconsistentes o débiles pueden crear agujeros de seguridad que deben identificarse y taparse lo más rápido posible.

Así mismo, independientemente de cómo se defina implementar un control de acceso, este debe ser monitoreado constantemente, tanto en términos de cumplimiento de su política de seguridad corporativa como operativamente, para identificar posibles agujeros de seguridad. Se debe realizar, entonces, periódicamente una revisión de la gobernanza, el riesgo y el cumplimiento. Se necesitan escaneos de vulnerabilidad recurrentes contra cualquier aplicación que ejecute sus funciones de

control de acceso y debe recopilar y monitorear registros en cada acceso para detectar violaciones de la política.

En los complejos entornos de TI de la actualidad, el control de acceso debe considerarse como una infraestructura tecnológica viva que utiliza las herramientas más sofisticadas, refleja los cambios en el entorno de trabajo, como una mayor movilidad, reconoce los cambios en los dispositivos que usamos y sus riesgos inherentes, y toma en cuenta el creciente movimiento hacia la nube.

1.2 Monitoreo del almacenamiento de la información

La gestión o monitoreo del almacenamiento de la información, también denominada gestión del almacenamiento de datos, implica el seguimiento y la optimización del componente central de los grandes datos que recopila y conserva información digital mediante computadoras y otros dispositivos. La gestión del almacenamiento de datos se refiere al proceso de gestionar los datos de forma más eficaz. Requiere una comprensión adecuada de los dispositivos de almacenamiento y la disponibilidad de varios tipos de datos. La información digital puede incluir protocolos, documentos, preferencias de usuario, libretas de direcciones y más. Los tipos comunes de almacenamiento de datos son el almacenamiento de objetos, el almacenamiento de archivos, el almacenamiento definido por “software” y el almacenamiento de bloques. Cada uno de estos tipos de almacenamiento se utiliza para diferentes propósitos:

A. **Almacenamiento en la nube**

El almacenamiento en la nube permite a las organizaciones almacenar datos en la nube, lo que facilita el acceso a los usuarios autorizados a través de Internet. Algunos de los almacenamientos en la nube más utilizados incluyen Google, Microsoft y más.

B. **Almacenamiento definido por "software"**

El almacenamiento definido por "software" es un enfoque que se utiliza para administrar datos a través de la abstracción. Funciona extrayendo datos del almacenamiento físico organizado para uso en red. También funciona bien con contenedores y micro servicios que incluyen datos no estructurados.

C. **Almacenamiento de archivos**

El almacenamiento de archivos es uno de los enfoques de almacenamiento de datos más comunes utilizados por las organizaciones. Almacena datos en un formato jerárquico como una sola pieza de información. Esto ayuda a los usuarios a acceder a los datos mediante identificadores únicos o rutas, como nombres, ubicaciones y direcciones URL.

D. **Almacenamiento en bloque**

El almacenamiento en bloque divide el almacenamiento en bloques independientes. Cada bloque tiene su propia identidad única que garantiza la seguridad de los datos y brinda la libertad de colocar pequeños fragmentos de información de manera conveniente para una recuperación más rápida. Los bloques son comparativamente más rápidos e ideales para bases de datos de medios enriquecidos. También pueden proporcionar a los usuarios una completa autonomía de configuración.

E. Almacenamiento de objetos

En el almacenamiento de objetos, los datos o archivos se dividen en piezas de información conocidas como objetos. Cada objeto es un repositorio autónomo con un identificador único. Esto ayuda a los usuarios a localizar y acceder a la información incluso en un sistema distribuido.

La gestión del almacenamiento de datos implica la supervisión de activos de "software" y "hardware", como matrices de almacenamiento, servidores físicos y servicios de almacenamiento en la nube. La gestión del almacenamiento de datos puede implicar la resolución de problemas de rendimiento, como posibles cuellos de botella, y el análisis de la capacidad de almacenamiento en tiempo real para ayudar a mejorar la experiencia del usuario final. Con esta información, los administradores pueden reasignar los recursos de almacenamiento para satisfacer las necesidades de almacenamiento empresarial. El monitoreo del almacenamiento de datos también puede incluir análisis de tráfico, automatización de procesos, gestión de memoria, virtualización de redes, replicación y aprovisionamiento de almacenamiento. Con el uso de un "software" confiable de administración de almacenamiento de datos, las organizaciones pueden configurar y rastrear más fácilmente el almacenamiento e informar las actividades de almacenamiento relacionadas.

Las funcionalidades comunes de la gestión del almacenamiento de datos incluyen:

A. Rendimiento y confiabilidad

El objetivo de la administración del almacenamiento de datos es administrar los datos para que estén disponibles para las operaciones comerciales. El acceso fácil y rápido a los datos aumenta el rendimiento, la

eficiencia y la productividad de los empleados y mejora la experiencia del usuario final. Para agilizar el proceso, los equipos pueden usar medios y niveles automáticos para optimizar diferentes niveles de almacenamiento.

B. Seguridad y protección de datos

Al utilizar el almacenamiento en la nube, es importante comprender la importancia de la protección de datos. Proteja los datos críticos para el negocio utilizando soluciones de copia de seguridad de datos, encriptación para datos almacenados y en tránsito, autenticación multifactorial para restringir el acceso no autorizado y más.

C. Control y cumplimiento

Aproveche varios niveles de organización en niveles o automática para almacenar los activos de datos más valiosos. Esto ayuda a administrar y almacenar datos y ayuda a las organizaciones a demostrar el cumplimiento de las regulaciones.

Ahora bien, frente a las herramientas para el monitoreo del almacenamiento de datos contribuyen en el apoyo de la asignación de recursos más fácilmente según sea necesario. Estas herramientas también pueden:

Figura 3. Herramientas para el monitoreo del almacenamiento

- ✓ Proporcionar a los administradores una visibilidad detallada de las capas de la aplicación para comprender los activos de almacenamiento y su rendimiento.
- ✓ Mantener los datos en una jerarquía, para que sean más fácilmente accesibles para los equipos.
- ✓ Proporcionar métricas e informes clave para ayudar a los administradores a adaptarse al almacenamiento de datos según sea necesario.
- ✓ Enviar alertas a los equipos relevantes para notificarles sobre el almacenamiento agotado para ayudar a brindar una experiencia de usuario final sin inconvenientes.

Cabe resaltar que existen “software” de administración de datos que están diseñados para ayudar a las organizaciones a monitorear la capacidad actual de

almacenamiento de datos a través de un tablero centralizado, para que pueda optimizar más fácilmente las políticas de almacenamiento de datos, administrar el estado del entorno de almacenamiento y abordar aspectos clave del proceso de administración de datos.

Además, las herramientas de monitoreo de datos pueden proporcionar información crucial sobre el estado de los dispositivos de almacenamiento, el riesgo de capacidad y la detección de puntos de acceso para garantizar que se tomen las medidas correctas.

1.3 Procesos de mejora para el tratamiento de la información

La protección de una organización contra los ataques cibernéticos a veces puede parecer un juego interminable de golpes de seguridad. Tan pronto como haya asegurado una debilidad, aparece otra. Esto puede desmoralizar a cualquier organización y hacerle creer que las buenas prácticas de seguridad de la información son imposibles. Sin embargo, hay una solución, pero requiere una forma diferente de pensar. Las organizaciones deben dejar de mirar cada amenaza individual a medida que surge y, en su lugar, construir defensas que estén equipadas para manejar cualquier cosa que los ciberdelincuentes les arrojen. Hacer eso es más simple de lo que parece. Esto se debe a que, por mucho que evolucionen las tácticas de los ciberdelincuentes, tienden a seguir la misma metodología básica. Si sus medidas de seguridad tienen en cuenta las formas en que se le ataca, en lugar de formas específicas de ataque, se defenderá de manera efectiva de una variedad de ataques.

Aprovechar cantidades masivas de datos brinda a las empresas una ventaja competitiva y las ayuda a comprender sus estrategias de ventas/“marketing” y las necesidades de los consumidores. Sin embargo, no se puede acceder a los datos sin someterse a un procesamiento de datos. Las empresas grandes y pequeñas necesitan comprender la importancia del procesamiento de datos.

¿Qué es el procesamiento de datos?

El procesamiento de datos ocurre cuando los datos se recopilan y transforman en información utilizable. Por lo general, es un proceso del que un científico de datos es responsable solo o en equipo, y es importante ejecutarlo correctamente para no afectar negativamente el resultado final (datos de salida). El procesamiento de datos primero transforma los datos en su forma original en formatos legibles (gráficos, documentos, etc.). Esto brinda a las computadoras el formato y el contexto que necesitan para interpretar los datos y aprovecharlos para los empleados de toda la organización.

Las etapas del procesamiento de datos son:

1. **Recopilación de datos**

   La recopilación de datos es el primer paso en el procesamiento de datos. Los datos provienen de fuentes disponibles, como lagos de datos y almacenes de datos. Es importante que las fuentes de datos disponibles sean fidedignas y estén bien construidas. Esto asegura que los datos recopilados (y luego utilizados para la información) tengan la mejor calidad posible.

2. **Preparación de datos**

   Los datos recopilados entran en la etapa de preparación de datos. La preparación de datos, también conocida como “pre-procesamiento”, es la etapa en la que se limpian y organizan los datos sin procesar. Esto hace que los datos estén disponibles para etapas posteriores del procesamiento de datos. Durante la preparación, los datos sin procesar se verifican minuciosamente en busca de errores. El propósito de este paso es eliminar datos incorrectos (datos redundantes, incompletos o inexactos) y crear datos de alta calidad para una mejor inteligencia comercial.

3. **Entrada de datos**

   Los datos limpios se introducen en su objetivo (un CRM como Salesforce o un almacén de datos como Redshift) y se interpretan en un lenguaje que pueda procesar. La entrada de datos es la primera etapa en la que los datos sin procesar toman la forma de información utilizable.

4. **Procesamiento**

   En esta etapa, los datos ingresados en la computadora desde la etapa anterior se procesan para su interpretación. El procesamiento se realiza mediante algoritmos de aprendizaje automático, pero el proceso en sí depende de la fuente de los datos que se procesan (lagos de datos, redes sociales, dispositivos conectados, etc.) y su uso previsto (estudio de patrones publicitarios, diagnósticos médicos de dispositivos conectados, Puede diferir ligeramente según la evaluación de las necesidades del cliente, etc.).

5. **Salida/interpretación de datos**

   Salida/Interpretación es la etapa en la que los datos finalmente se ponen a disposición de los que no son científicos de datos. Los datos se interpretan y se hacen legibles, a menudo en forma de gráficos, videos, imágenes, texto sin formato, etc. Los miembros de la organización podrán autoservicio de datos para sus propios proyectos de análisis de datos.

6. **Almacenamiento de datos**

   La etapa final del procesamiento de datos es el almacenamiento. Todos los datos procesados se almacenan para uso futuro. Parte de la información se puede usar inmediatamente, pero la mayoría se usará más tarde. Además, se requiere que los datos almacenados correctamente cumplan con las leyes de protección de datos como GDPR. Cuando los datos se almacenan correctamente, los miembros de su organización pueden acceder a ellos rápida y fácilmente según sea necesario.

La nube jugará un papel clave en el futuro del procesamiento de datos. La tecnología de la nube se basa en las prácticas actuales de procesamiento electrónico de datos para aprovechar esa conveniencia y mejorar la velocidad y la eficiencia. Con velocidades más rápidas y datos de mayor calidad, puede aprovechar más datos y extraer información más valiosa. A medida que los grandes datos se trasladan a la nube, las empresas obtienen importantes beneficios. La tecnología de nube de “big data” permite a las empresas combinar todas las plataformas en un sistema fácilmente adaptable. A medida que el “software” cambia y se actualiza (como es común en el mundo de los grandes datos), la tecnología de la nube integra a la perfección elementos antiguos y nuevos.

Las grandes empresas no son las únicas que se benefician del procesamiento de datos en la nube. De hecho, las pequeñas y medianas empresas también pueden beneficiarse enormemente entre sí. La plataforma en la nube se puede utilizar a bajo costo y se puede expandir/extender de manera flexible de acuerdo con el crecimiento de la empresa. Esto permite a las empresas ganar escalabilidad sin incurrir en costos significativos.

Sumado a esto, se pasa del procesamiento de datos a la analítica. El "big data" está cambiando la forma en que se hacen negocios, y las empresas de todos los tamaños necesitan estrategias sólidas de procesamiento de datos para obtener una ventaja competitiva. Los seis pasos del procesamiento de datos seguirán siendo los mismos, pero la nube hará avanzar mucho la tecnología, convirtiéndola en el método más económico, moderno y rápido. Una vez que se completa el procesamiento de datos, luego de su recopilación, lo que se espera es la utilización real de los mismos por medio de su análisis; de esta forma, se puede tomar decisiones comerciales más rápidas e inteligentes.

A medida que las fuentes de datos se expanden y diversifican, el procesamiento de datos debe enfrentar varios desafíos nuevos. El "hardware" Intel® está reforzado para un procesamiento de datos rápido y rentable y se puede escalar para cumplir con las cargas de trabajo más exigentes.

No existe un enfoque único para el procesamiento de datos; pues diferentes tipos de cargas de trabajo y aplicaciones requieren distintos enfoques para aumentar su rendimiento y rentabilidad. Los métodos de procesamiento de datos son los siguientes:

A. **El procesamiento por lotes**

El procesamiento por lotes es la clasificación de datos en grupos o lotes, que se procesan a medida que los recursos están disponibles. Durante el procesamiento por lotes, los lotes de datos se procesan en serie uno tras otro. El procesamiento por lotes puede manejar grandes cantidades de datos de manera eficiente, pero generalmente es más adecuado para los datos que no necesitan ser usados de inmediato.

B. **Procesamiento de flujo**

El procesamiento de flujo se realiza durante el procesamiento continuo de datos a medida que ingresan en la canalización de datos. Este tipo de procesamiento es mucho más rápido que el procesamiento por lotes, debido a que el análisis se da en pequeñas cantidades de datos. Por lo general, se usa para procesar datos que requieren una ejecución rápida.

C. **Procesamiento de datos distribuido**

A medida que la tecnología de red ha evolucionado, las tareas de procesamiento de datos ya no necesitan completarse dentro del mismo nodo. En el procesamiento de datos distribuidos, varios nodos que se ejecutan en el mismo "clúster" funcionan en paralelo para procesar cargas de trabajo de datos en una red. El uso del procesamiento de datos distribuido permite que las cargas de trabajo de análisis avanzado se procesen en "hardware" de bajo costo y bajo consumo.

Según el tipo de datos que se procesen y su uso, varias de estas operaciones estratégicas se pueden realizar en una sola canalización de datos, lo que da como resultado una salida de datos final unificada.

El procesamiento de datos, uno de los procesos con mayor uso de recursos en una canalización de datos, está fuertemente influenciado por las optimizaciones de "hardware" y "software". Muchos de los principales proveedores de "software" hoy en día optimizan sus productos para el "hardware" Intel®. Así mismo, el ecosistema Intel® de soluciones y socios tecnológicos garantiza que muchas soluciones de "software" se ejecuten de manera óptima en el "hardware" Intel®, lo que lo ayuda a aprovechar al máximo su inversión en tecnología. Intel, entonces, ofrece la siguiente amplia cartera de tecnologías de "hardware" y "software" para acelerar las cargas de trabajo de procesamiento de datos actuales:

A. Procesadores Intel® Xeon

Los procesadores Intel Xeon ofrecen la flexibilidad para hacer frente a una amplia gama de cargas de trabajo de diversas fuentes, con procesadores Intel® optimizados para tareas como la normalización de datos y la reducción de ruido para el procesamiento de IA.

B. SSD Intel Optane

Las SSD Intel® Optan están diseñadas para ofrecer estabilidad y están construidas para optimizar el almacenamiento y el rendimiento de la memoria caché de datos. Ayuda a acelerar la transmisión y el procesamiento de datos en tiempo real mientras mantiene una alta confiabilidad del sistema.

C. **Tecnologías de código abierto**

Intel ofrece una amplia gama de bibliotecas y plataformas de código abierto que aceleran el procesamiento y el análisis de datos. Esto incluye Intel® oneAPI Toolkit, Intel® oneAPI Math Kernel Library (Intel® oneMKL), Intel® oneAPI Data Analytics Library (Intel® oneDAL) y más.

D. **Seguridad mejorada**

La tecnología Intel® QuickAssist (Intel® QAT) permite a los equipos de datos acelerar el rendimiento del cifrado y descifrado y mejorar la seguridad de las aplicaciones de procesamiento de datos.

Las tecnologías Intel® están diseñadas para permitir que cada organización cree una flexibilidad única y canalizaciones de procesamiento de datos únicas para nuevas fuentes de datos y aplicaciones. La aceleración basada en "software" y "hardware" de Intel permite el procesamiento de datos a la velocidad y eficiencia requeridas por las aplicaciones de análisis más avanzadas de la actualidad.

1.4. Gestión de las copias de seguridad

Para mantener la disponibilidad de los activos de información, dentro de una empresa u organización, es necesario contar con copias de seguridad adecuadas de la información que se posee. El personal de administración de la información debe operar una copia de seguridad que pueda restaurarse rápidamente con el menor impacto posible en el negocio, en caso de una falla de la computadora o de la red o un error de operación del sistema. Para garantizar que los usuarios de una empresa u organización puedan usar sus computadoras personales de manera segura, se deben recomendar copias de seguridad periódicas. En las computadoras cliente, no solo se deben

respaldar los archivos de documentos creados con el "software" de procesamiento de texto y el "software" de hoja de cálculo, sino también los correos electrónicos, las URL de los sitios web de uso frecuente y varias configuraciones.

Los diversos tipos de información que manejan las empresas deben ser estrictamente protegidos y una forma de protegerla es a través de una copia de seguridad de sus datos. La pérdida de estos dificulta las actividades comerciales. Por ello, es esencial que aquellos que están en condiciones de proteger la información corporativa comprendan los puntos relacionados con la copia de seguridad y su respectiva gestión.

La gestión de copias de seguridad incluye la eliminación de copias de seguridad innecesarias y la realización de comprobaciones periódicas para garantizar que las copias de seguridad se puedan utilizar. Por ello, se debe tener en cuenta lo siguiente:

A. Copias de seguridad

Las copias de seguridad registradas en el repositorio tienen uno de los siguientes valores de estado:

- ✓ **Uso posible:** esto significa que las copias de seguridad registradas en el repositorio aún existen en disco o cinta.
- ✓ **Venció:** esto significa que la copia de seguridad ya no existe en el disco o la cinta y todavía se incluye en el repositorio.
- ✓ **Es imposible de usar:** esto significa que las copias de seguridad no se pueden usar temporalmente para las operaciones de recuperación de datos (por ejemplo, porque se almacenan fuera del sitio en cintas o en discos que no están montados actualmente).

- ✓ **Innecesarias:** es posible que ya no se requieran copias de seguridad. Las copias de seguridad obsoletas son copias de seguridad que ya no se necesitan para satisfacer los propósitos de recuperación de datos, según la política de retención configurada actualmente.

B. Mantenimiento

Las tareas de mantenimiento que puede realizar son:

- ✓ Ver detalles de la copia de seguridad del repositorio: se realiza una verificación cruzada (si las copias de seguridad enumeradas en el repositorio existen, están disponibles y marque las copias de seguridad no disponibles como caducadas durante la verificación cruzada).
- ✓ Eliminación de registros de copia de seguridad caducados del repositorio.
- ✓ Eliminación de copias de seguridad obsoletas de repositorios y medios de copia de seguridad.
- ✓ Verificación de copia de seguridad para garantizar que se pueda utilizar y no esté dañada.

Sin un registro preciso de las copias de seguridad disponibles, es posible que descubra que no existe una copia de seguridad completa de su base de datos cuando necesite realizar una recuperación. Las tareas como la verificación cruzada periódica de las copias de seguridad deben programarse regularmente como parte de su estrategia de copia de seguridad.

Cuando se utiliza el área de recuperación rápida para el almacenamiento de copias de seguridad, se eliminan o reducen muchas actividades de mantenimiento. Los archivos de respaldo y otros archivos se eliminan según sea necesario, mediante el mecanismo de administración de almacenamiento automático para cumplir con las demandas de almacenamiento de las operaciones en curso de la base de datos sin violar las políticas de retención. Sin embargo, debe monitorear el uso del espacio en el área de recuperación rápida para asegurarse de que sea lo suficientemente grande para almacenar copias de seguridad y otros archivos relacionados con la recuperación.

El personal de gestión de la información es responsable de realizar copias de seguridad de los datos compartidos almacenados en servidores de bases de datos y servidores de archivos. Para realizar una copia de seguridad, se utiliza la utilidad de copia de seguridad proporcionada con el sistema operativo o el "software" de copia de seguridad dedicado; usualmente se realizan tarde en la noche o temprano en la mañana cuando los usuarios no están operando.

Los datos que los empleados y el personal almacenan en cada cliente también son uno de los activos de información importantes. Por lo tanto, los usuarios dentro de la organización también deben recibir instrucciones para realizar una copia de seguridad de la información almacenada en cada cliente. Al hacerlo, se comprende correctamente la importancia de los activos de información de cada usuario, como el destino de almacenamiento de la copia de seguridad (medios, servidor de copia de seguridad, etc.), el "software" y el método de copia de seguridad utilizados, la frecuencia de la copia de seguridad, etc. Se debe tener en cuenta que, si el usuario utiliza un medio de almacenamiento externo para la copia de seguridad, existe una gran posibilidad de que se filtre información confidencial o información personal debido a la

eliminación de datos. Si se recomiendan medios de almacenamiento externo para la copia de seguridad, también es importante implementar minuciosamente reglas para la gestión de la información, como prohibir la eliminación innecesaria de datos y estipular ubicaciones de almacenamiento, en una política de seguridad de la información.

Los datos que manejan las empresas incluyen datos como información de clientes, información relacionada con la contabilidad e información de socios comerciales. En el improbable caso de que estos datos se dañen o se pierdan, la empresa perderá credibilidad social y, además, existe la posibilidad de que se produzca una pérdida de clientes y se deteriore el rendimiento empresarial. La ocurrencia de pérdida económica por recibir una reclamación por daños también es un riesgo que no puede ser ignorado. Proteger sus datos con copias de seguridad es una forma eficaz de evitar la pérdida de datos.

Si ocurre una falla de datos y la información en poder de la empresa se vuelve ilegible, será difícil continuar con las actividades corporativas.

Es necesario conocer la causa de la falla de los datos para poder realizar una copia de seguridad adecuada. A continuación, se presenta un vistazo a las principales causas de esta falla de datos:

1. **Errores de operación por parte de los empleados**

   Una cierta cantidad de error humano es inevitable porque son las personas, como los empleados, quienes realmente manejan los datos. Por ejemplo, el error de un empleado al operar una computadora personal puede hacer que los datos importantes se sobrescriban con otros datos o se eliminen. También es importante proporcionar una formación adecuada

a los empleados para que no se produzcan errores operativos. Pero si sucede lo peor, puede restaurar con una copia de seguridad.

2. **Infección por virus**

   Las empresas están rodeadas de diversas amenazas. Uno de ellos es la existencia de piratas informáticos que atacan los datos corporativos e infectan con virus las redes de las empresas y los terminales individuales. No es exagerado decir que el riesgo de piratear datos corporativos aumenta cada día que pasa. Como empresa, debe ser plenamente consciente del riesgo de piratería y preparar un sistema de defensa.

3. **Obstáculos físicos**

   Los obstáculos físicos, como fallas en discos duros o daños en los datos, representan una tercera causa de pérdida de datos. Aunque en algunos casos se pueden recuperar, a menudo estos problemas quedan sin resolver, dificultando la continuidad del negocio. Además, el robo de computadoras personales también implica una pérdida física de datos. Para prepararse ante estas situaciones, es crucial contar con copias de seguridad.

Existen tres métodos para hacer una copia de seguridad: guardar en un medio de almacenamiento externo, almacenamiento en línea y almacenamiento en red:

A. **Almacenamiento externo**

   En el primer método de copia de seguridad, que utiliza medios de almacenamiento externos, se utilizan CD, DVD, Discos Duros, o “pendrive” como medios de almacenamiento. Dependiendo de la capacidad de almacenamiento, se suele utilizar la memoria “flash”. La capacidad de los medios de copia de seguridad ha crecido

considerablemente. Es necesario tener un medio de almacenamiento adecuado y hacer copias de seguridad regularmente para proteger los datos. Utilizar un dispositivo externo facilita este proceso.

B. Almacenamiento en línea

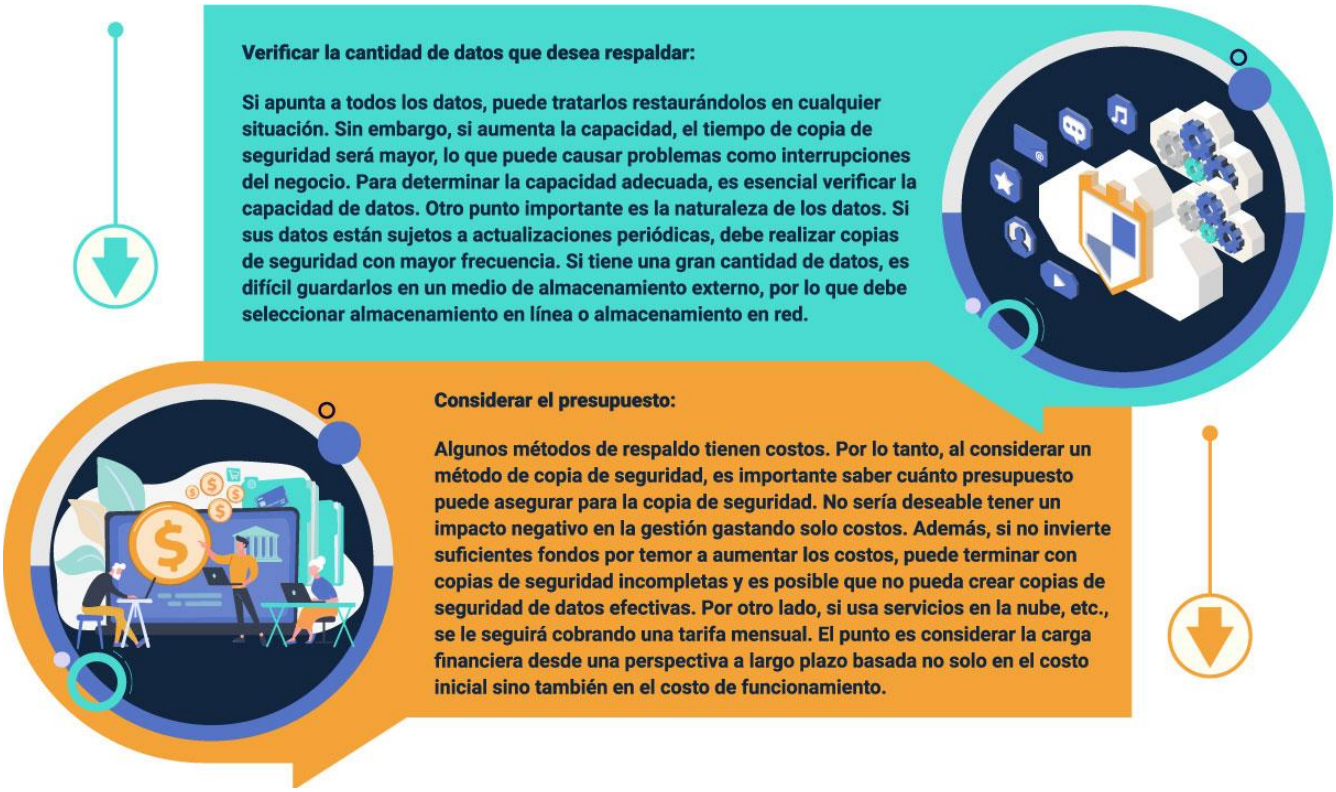
El almacenamiento en línea se refiere al almacenamiento de datos en Internet. Es común hacer una copia de seguridad de los datos utilizando servicios en la nube. La ventaja del almacenamiento en línea es que puede almacenar grandes cantidades de datos. Otra característica del almacenamiento en línea es que, incluso en este caso, los datos en Internet pueden protegerse sin daños. También es efectivo almacenar datos importantes en una red confiable fuera de la empresa utilizando servicios en la nube.

C. Almacenamiento externo

El almacenamiento en red tiene una forma llamada NAS (Network Attached Storage) y debe entenderse que es un servidor de archivos dedicado. Hay muchos discos de gran capacidad, por lo que puede usarse sin preocuparse por el límite de capacidad de almacenamiento. Otra ventaja de utilizar el almacenamiento en red es que se pueden realizar copias de seguridad automáticas a altas horas de la noche o durante los días festivos mediante la configuración por adelantado.

Por otro lado, hay dos puntos a considerar al decidir cuál de los múltiples métodos de copia de seguridad de datos es mejor para una empresa. Uno es la cantidad de datos que desea respaldar y el otro es el costo.

Figura 4. Puntos a considerar en las copias de seguridad



- ✓ **Verificar la cantidad de datos que desea respaldar:**

  Si apunta a todos los datos, puede tratarlos restaurándolos en cualquier situación. Sin embargo, si aumenta la capacidad, el tiempo de copia de seguridad será mayor, lo que puede causar problemas como interrupciones del negocio. Para determinar la capacidad adecuada, es esencial verificar la capacidad de datos. Otro punto importante es la naturaleza de los datos. Si sus datos están sujetos a actualizaciones periódicas, debe realizar copias de seguridad con mayor frecuencia. Si tiene una gran cantidad de datos, es difícil guardarlos en un medio de almacenamiento externo, por lo que debe seleccionar almacenamiento en línea o almacenamiento en red.

- ✓ **Considerar el presupuesto:**

  Algunos métodos de respaldo tienen costos. Por lo tanto, al considerar un método de copia de seguridad, es importante saber cuánto presupuesto puede asegurar para la copia de seguridad. No sería deseable tener un impacto negativo en la gestión gastando solo costos. Además, si no invierte suficientes fondos por temor a aumentar los costos, puede terminar con copias de seguridad incompletas y es posible que no pueda crear copias de seguridad de datos efectivas. Por otro lado, si usa servicios en la nube, etc., se le seguirá cobrando una tarifa mensual. El punto es considerar la carga financiera desde una perspectiva a largo plazo basada no solo en el costo inicial sino también en el costo de funcionamiento.

De forma adicional, hay algunas notas a tener en cuenta al administrar las copias de seguridad de datos por parte, tanto de la persona a cargo como del gerente de la empresa:

A. **Aclarar el propósito de la copia de seguridad**

   Realizar copias de seguridad sin un propósito claro dificulta su eficiencia. Es importante definir el propósito, como proteger la credibilidad de la empresa frente a pérdidas de información. Una vez definido, se puede establecer el rango y la frecuencia adecuados de respaldo. También se puede reducir el tiempo de copia al eliminar datos innecesarios.

B. **Tenga cuidado al manipular medios de almacenamiento externos**

   Al hacer copias de seguridad en medios externos como CD o memorias “flash”, es importante manejarlos con cuidado para evitar pérdidas. Después de respaldar los datos, guárdelos en una caja fuerte ignífuga para

protegerlos de robos o incendios. Además, es necesario educar a los empleados sobre no sacar los medios de almacenamiento de la empresa.

C. **Indique a los empleados que retrocedan**

Es importante garantizar que cada empleado realice copias de seguridad adecuadas. Aunque el personal de TI puede respaldar la base de datos compartida, cada empleado debe respaldar sus propios datos en sus computadoras. Se deben proporcionar instrucciones precisas sobre el método y el destino de almacenamiento. Al hacer que los empleados asuman la responsabilidad de las copias de seguridad, se mejora el nivel de seguridad de la empresa en general.

D. **La copia de seguridad puede tardar mucho tiempo**

Si la cantidad de datos a respaldar es grande, llevará tiempo completar la copia de seguridad. Durante la copia de seguridad, es necesario restringir el acceso a dichos datos. Los tiempos de respaldo más prolongados pueden afectar negativamente las operaciones comerciales. Al realizar copias de seguridad de grandes cantidades de datos, es eficaz establecer copias de seguridad automáticas fuera del horario laboral, por la noche o en días festivos.

E. **Preparar un sistema de gestión de datos de copia de seguridad**

Además de realizar copias de seguridad periódicas, es crucial asegurarse de que los datos respaldados sean utilizables en caso de emergencia. Al restaurar los datos, es importante designar a un empleado responsable y tener un sistema de gestión efectivo. Sin embargo, es importante controlar el número de administradores para evitar confusiones sobre quién restauró los datos y cuándo. Construir un sistema adecuado de gestión es fundamental.

F. **Gestione copias de seguridad periódicas de los datos de su empresa**

Es crucial gestionar correctamente los datos corporativos para proteger su confidencialidad y activos. Se debe realizar copias de seguridad de manera activa para salvaguardar la credibilidad de la empresa. Los datos y programas son activos valiosos, por lo que es necesario hacer copias de seguridad regularmente y administrarlos adecuadamente para evitar pérdidas en caso de daños o accidentes.

Ahora bien, también se debe contemplar las fallas y la recuperación de los datos que se puedan presentar, clasificándolos de la siguiente manera:

A. **Fallo de los datos en sí**

La falla más común es la eliminación o sobrescritura de los datos necesarios debido a errores operativos por parte de administradores o usuarios. También puede ocurrir sobrescritura (manipulación) o eliminación debido a una infección de "malware". Como contramedida, se hacen copias de los datos de varias generaciones y luego se guardan.

B. **Obstáculos físicos**

Es una falla del dispositivo (principalmente del disco duro) donde se almacenan los datos, e incluye fallas, daños (choque, terremoto o colisión, incendio, inundación) y robo del propio dispositivo. Como contramedida, los datos deben almacenarse en una ubicación diferente y en un medio diferente.

A modo genérico se puede decir, entonces, que las operaciones de copia de seguridad se determinan teniendo en cuenta el uso y la importancia de los datos a replicar, así como el costo de recuperación en el improbable caso de falla.

Adicional a esto, para la gestión de la operación, es necesario determinar el tipo de medio de almacenamiento, frecuencia y método, período de almacenamiento y lugar de almacenamiento, entre otros:

1. **Tipo de medio de almacenamiento**

   Se selecciona qué medio usar, como cinta, disco externo, CD/DVD, memoria "flash" (memoria USB), almacenamiento en red, etc. Es deseable considerar múltiples combinaciones también.

2. **Frecuencia (intervalo) y método**

   Intervalo de tiempo de copia de seguridad. Es necesario decidir si hacerlo todos los días, semanalmente, mensualmente, etc. Debe seleccionar si se desea utilizar Copia de seguridad completa, Copia de seguridad diferencial o Copia de seguridad incremental. Se puede lograr una copia de seguridad eficiente mediante el uso de múltiples métodos en combinación con intervalos.

3. **Periodo de almacenamiento**

   Es el período de almacenamiento de datos, que se ve afectado por la gestión de la frecuencia y la generación. Dependiendo del tipo de datos, como datos financieros, datos relacionados con aprobaciones y notificaciones, datos médicos y de seguros, etc., pueden existir períodos legales de conservación.

4. **Ubicación de almacenamiento**

   Dependiendo del propósito de uso, se selecciona el mismo lugar que el sistema, el mismo edificio, un edificio separado, el exterior de corta distancia, el exterior de larga distancia, etc. Las combinaciones de múltiples

medidas y rotaciones son el método preferido. La selección y combinación de medios externos y medios de red también es un punto. Las redes externas también facilitan relativamente el uso de ubicaciones remotas.

2. Gestión de la información

La gestión de la información significa administrar adecuadamente la información, protegerla para que pueda recuperarse cuando sea necesario y evitar que se filtre. Es por esto que se hace necesario realizar una gestión de forma centralizada sobre la información interna utilizando herramientas adecuadas, ya que aunque algunas se especializan en facilitar la recuperación de información tienen problemas de seguridad y por ende, presentan riesgo de fuga de información. Por tanto, a la hora de gestionar la información es necesario tener en cuenta la compatibilidad entre la facilidad de extracción y uso de la información y la seguridad.

Mientras los escándalos de fugas de información corporativa continúan día tras día, muchos dueños de negocios deben entender que esto no es un incendio al otro lado del río. En particular, incluso las pequeñas y medianas empresas, que hasta ahora solían quedar excluidas de los ciberataques, continúan sufriendo daños debido a los ataques indiscriminados. En tales circunstancias, ¿qué tipo de gestión de la información se requiere de las empresas? Diariamente, se genera y gestiona diversa información en las empresas. La cantidad de datos de ventas, datos de ventas, datos de compras, datos de clientes, materiales de reuniones, documentos de aprobación, planes comerciales, etc. es enorme. Dicha información a menudo incluye información personal e información confidencial, y nunca debe filtrarse fuera de la empresa. Sin embargo, de

vez en cuando, los activos de información de una empresa pueden sufrir daños como fugas, daños o desaparición, los cuales se tienden a pensar en ellas como incidentes causados por ataques cibernéticos, pero, en realidad, los factores internos como pérdida/extravío, mal funcionamiento y mala gestión representan por sí solos altos porcentajes de errores internos.

Es cierto que muchas empresas se han beneficiado de la difusión de las computadoras personales en los hogares en general, el desarrollo de entornos de Internet de alta velocidad y el aumento explosivo de usuarios de teléfonos inteligentes. Por otro lado, sin embargo, también es cierto que pueden producirse incidentes de fuga de información por ligeros errores de gestión o por laxitud de la seguridad. En estas circunstancias, en lo que deben trabajar las empresas es en tomar las medidas de seguridad adecuadas y conocer con precisión el tipo, la calidad y la cantidad de los activos de información que posee la empresa. Esto ahora se posiciona como una de nuestras responsabilidades sociales. Además de las medidas de seguridad, las empresas necesitan trabajar en planes comerciales y presupuestos para el próximo año fiscal, trabajo diario de gestión y servicio al cliente, y no quedan muchos recursos excedentes. Especialmente para las pequeñas y medianas empresas, hay muchos casos en los que no se pueden tomar medidas de seguridad suficientes desde un punto de vista financiero. Es por eso que no se puede esperar incidentes de fuga de información. Por lo tanto, lo que debe considerar activamente es una contramedida que refuerce las medidas de seguridad mientras se usa los servicios de otras compañías.

Recientemente, se han proporcionado varios servicios web y también se proporcionan muchos sistemas comerciales que son indispensables para las actividades

de gestión. Muchos de estos servicios web cumplen con altos requisitos de seguridad y, en algunos casos, las medidas de seguridad pueden reforzarse simplemente usándolos.

Al utilizar los servicios web, muchas pequeñas y medianas empresas no solo buscan reducir la carga operativa y la inversión inicial, sino que también están considerando fortalecer las medidas de seguridad. En casos extremos, si todos los sistemas comerciales internos se convierten en servicios web, solo eso puede proporcionar suficientes medidas de seguridad. A través de prueba y error, incluso las pequeñas y medianas empresas pueden satisfacer completamente los requisitos de alta seguridad. Otro método efectivo es utilizar la subcontratación para crear recursos humanos y de tiempo internos y asignarlos a medidas de seguridad.

Las empresas que creen que es seguro adoptar medidas de seguridad internas no construyen sistemas comerciales utilizando los servicios de otras empresas, sino que subcontratan parte de sus operaciones internas y crean nuevos recursos para mejorar la seguridad. Considere tomar precauciones. Las medidas de seguridad para la gestión de la información nunca son fáciles. Sin embargo, si se apela al exterior de que se está gestionando minuciosamente la información, esto se convierte en un elemento de gestión que aumenta el valor corporativo.

A continuación, se explican aspectos que hacen evidente la importancia de la gestión de la información para las empresas:

A. Mantener la imagen de la marca

La gestión inadecuada de la información puede conducir fácilmente a la pérdida o fuga de información; y si este escenario llegase a ocurrir, el hecho debe anunciarse al público y, es muy probable e inevitable, un

deterioro de la imagen de marca de la empresa. Motivo por el cual será necesario tomar medidas encaminadas a mejorar el posicionamiento de la marca, lo que a su vez no solo aumentan los costos, sino que también es posible que no se puedan obtener nuevas transacciones y las ya comprometidas pueden quedar en blanco.

B. Prevenir accidentes causados por infección de virus

Si se utilizan herramientas y se gestiona minuciosamente la información, se pueden prevenir accidentes provocados por infecciones de virus. Por ejemplo, si una computadora en una empresa está infectada con un virus que invade desde el exterior, todo el sistema de la empresa puede funcionar mal. Además, si un sitio web es desfigurado por un virus, existe el riesgo de que afecte tanto interna, como externamente a la empresa. Si ocurre un accidente de este tipo, no solo se retrasará el negocio, sino que, si la operación se ve obligada a detenerse, se pueden perder oportunidades de venta. Las herramientas utilizadas para la gestión de la información mantienen un alto nivel de seguridad debido a la naturaleza de estar conectadas a Internet. Por lo tanto, dicha infección por virus se puede prevenir y manejar en un estado seguro en todo momento.

C. Fortalecer la competitividad de las empresas

La información en poder de las empresas incluye no solo información como la información del cliente, sino también información técnica de sus propios productos y/o servicios. Si dicha información técnica se filtra, podría conducir a la proliferación de productos falsificados que utilizan la tecnología y la salida de la tecnología al extranjero. No importa cuán especial sea la tecnología, si la tecnología se filtra, aparecerán muchos

productos de imitación en el mercado y la competitividad inevitablemente disminuirá. El manejo adecuado de la información es importante para prevenir tal situación y continuar aumentando la competitividad de la empresa.

Por lo anterior, se detallan las medidas de seguridad que las empresas deben implementar para proteger su información. Al implementar de manera confiable las tres medidas de seguridad, puede administrar los activos de información de su empresa de manera adecuada y segura:

1. **Contramedidas técnicas**

   Las medidas técnicas se refieren a las mejoras de seguridad desde la perspectiva del "software". Por ejemplo, las medidas técnicas incluyen la introducción de "software" de seguridad y actualizaciones del mismo. A medida que avanza la digitalización, muchas empresas poseen uno o más terminales digitales por persona, pero se debe mejorar la seguridad desde la perspectiva del "software" para todos estos terminales. Otra medida técnica es establecer reglas para la descarga de datos para prevenir la infección por virus. Hay muchos otros métodos, así que se debe combinar varias medidas para aumentar la seguridad.

2. **Medidas físicas**

   Las medidas físicas se refieren al fortalecimiento de la seguridad desde la perspectiva del “hardware”. Por ejemplo, para mejorar la seguridad de la propia oficina, las medidas físicas incluyen la introducción de un sistema de autenticación biométrica y el uso de tarjetas de identificación de los empleados al entrar y salir de una sala de seguridad. La toma de medidas físicas tiene la implicación de evitar que se saque información de la empresa. Si es difícil introducir herramientas de inmediato debido a problemas de costo, etc., se puede manejar aclarando las áreas de seguridad a las que los visitantes y contratistas no pueden ingresar. Sin embargo, dado que esta es solo una medida temporal, es necesario considerar cómo fortalecer continuamente la seguridad del “hardware”.

3. **Medidas humanas**

   Las medidas humanas son medidas para prevenir incidentes de seguridad causados por personas. No importa cuántas medidas técnicas y físicas se tomen, si la alfabetización y la moralidad de los empleados que los manejan son bajas, pueden ocurrir incidentes de seguridad y fraude. Para prevenir tales accidentes, llevemos a cabo educación sobre seguridad de la información y capacitación sobre moral y cumplimiento. También es importante crear un manual de trabajo y establecer procedimientos para prevenir incidentes de seguridad causados por errores inesperados.

De manera adicional, se presentan algunos puntos que se debe tener en cuenta para asegurarse de que la información se gestione correctamente. Después de planificar minuciosamente las medidas de seguridad, se debe definir cómo las empresas pueden garantizar una gestión completa de la información:

A. Formular una política de seguridad de la información

La política de seguridad de la información se refiere a las políticas en la gestión de la información. Al establecer una política de seguridad de la información, las empresas podrán determinar la dirección de la gestión de la información y podrán establecer qué tipo de sistema se debe utilizar para la gestión de la información. Además, si la política básica está bien definida, incluso cuando se establecen reglas para el manejo de la información, las reglas se pueden seleccionar en función del juicio de "si se ajustan o no a la política", por lo que es posible establecer reglas consistentes que puede construir un sistema de gestión de la información que tenga.

B. **Aclarar dónde recae la responsabilidad**

A la hora de gestionar la información, es muy importante saber quién es el responsable de gestionarla. Esto se debe a que, si la ubicación de la responsabilidad no está clara, la conciencia de seguridad de cada persona será baja. Para aclarar dónde recae la responsabilidad, se recomienda establecer un departamento de gestión de seguridad de la información. Al crear estos departamentos, incluso en el improbable caso de que ocurra un incidente de seguridad, será posible responder sin problemas. Además, si el departamento toma la delantera en la educación de los empleados, es posible promover la permeación de las reglas.

C. **Determinar reglas para la gestión de la información**

A la hora de gestionar la información, también es importante evitar los errores de los empleados. Para evitar errores humanos causados por los empleados, es importante establecer reglas detalladas para la gestión. Si las reglas se establecen correctamente de antemano, incluso los empleados con poca alfabetización informática podrán manejar la información sin cometer errores. Por ejemplo, establezcamos reglas detalladas según el nivel del sitio, como; No instalar “software” sin permiso.

Ahora bien, si la gestión de la información de una empresa no está funcionando como se esperaba, hay que verificar si alguna de las siguientes situaciones se aplica y por ende se efectúa sus respectivas mejoras:

A. **Revisión periódica del sistema de gestión**

En el mundo de la seguridad de la información, todos los días surgen nuevos riesgos y amenazas. Por lo tanto, incluso si se establece un sistema de gestión una vez, no siempre se puede decir que es el mejor sistema. Por este motivo, es importante revisar periódicamente el sistema y realizar los cambios necesarios. En particular, es necesario realizar modificaciones, como agregar contramedidas apropiadas contra cosas que se pueden prevenir de antemano, como ataques cibernéticos y virus informáticos.

B. **La operación es más importante que la implementación de herramientas**

Las herramientas pueden centralizar la información interna, por lo que la introducción de herramientas es fundamental para la gestión de la información. Sin embargo, no se puede decir que la gestión de la información se esté realizando correctamente sólo porque se haya implantado una herramienta. En particular, cuando la gestión de la información no va bien, hay muchos casos en los que solo se han introducido herramientas. Por lo tanto, para utilizar correctamente las herramientas y garantizar una gestión completa de la información dentro de la empresa, es necesario comprender las precauciones y los puntos de minuciosidad que se han introducido hasta ahora y construir un sistema de gestión de la información.

C. **Compendio de herramientas**

La elección de herramientas de TI para la gestión de información es crucial, considerando factores como la accesibilidad, seguridad y facilidad de uso. La gestión de información no debe ser responsabilidad de unos pocos empleados, sino accesible para todos. Además, al utilizar servicios en la

nube, se deben evaluar cuidadosamente las medidas de seguridad y la administración de datos. Introducir una herramienta como “Stock” facilita el intercambio de información y cumple con altos estándares de seguridad.

D. Elija herramientas que aseguren la accesibilidad

Las herramientas de gestión de la información pueden reformularse como herramientas de comunicación entre quienes tienen información y quienes la buscan. Por lo tanto, al considerar la introducción de herramientas, es esencial tener en cuenta la accesibilidad para sus propios miembros. ¿Qué tipo de “lead” y qué tipo de capacidad de búsqueda se debe preparar para que los miembros de la empresa puedan acceder a la información que desean? Si introduce una herramienta de gestión de información sin esta perspectiva, no conducirá a la operación deseada. Las herramientas de gestión de la información incluyen herramientas de comunicación de preguntas y respuestas, como los sistemas de preguntas frecuentes.

2.1. Actualización de bases de datos de activos de la información

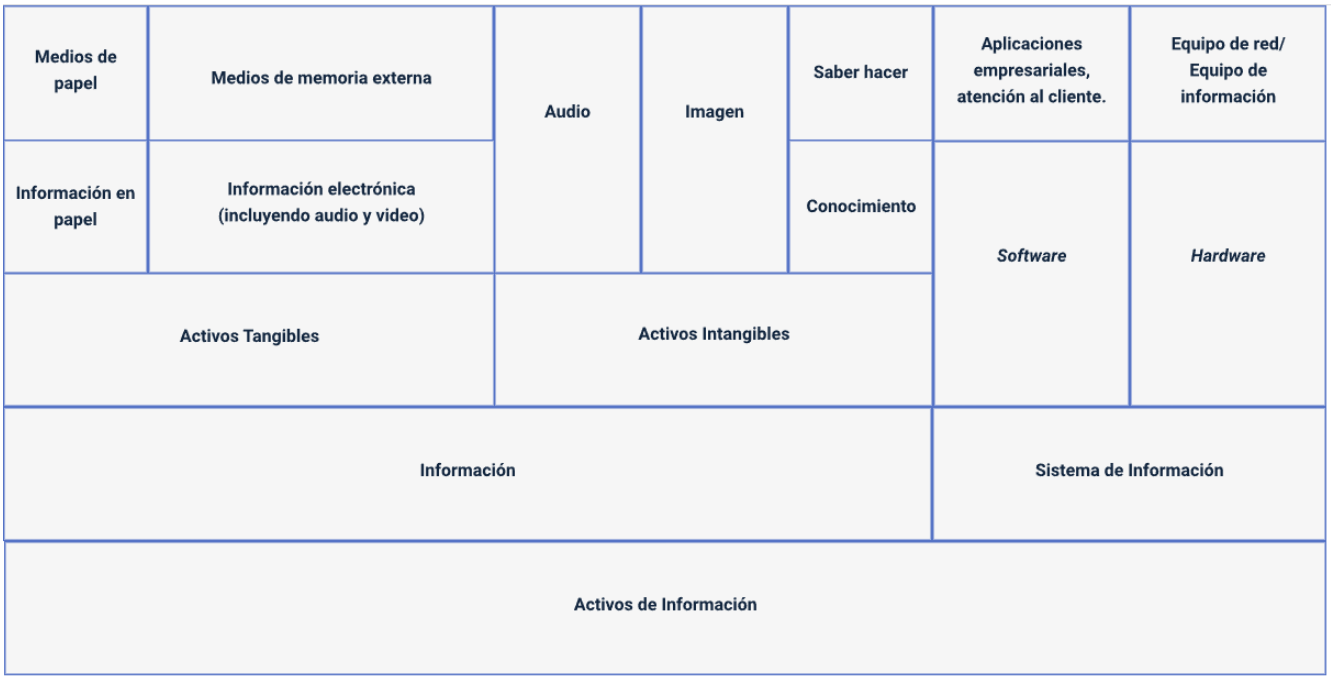
La información recopilada por empresas y organizaciones incluye datos valiosos como activos de información, como lo son la información del cliente (incluida la información personal) e información de tecnología del producto, así como ubicación, número de teléfono, información básica publicada en el sitio web oficial de la empresa, entre otros. La información que tiene valor de activo para una empresa/organización debe ser sujeta a procesos de protección de seguridad.

A continuación, se detallan los activos de información base en poder de empresas/organizaciones:

1. Información técnica del producto, como planes de producción, dibujos de diseño del producto, especificaciones, listas de piezas y procedimientos de trabajo.
2. Planes de gestión y de negocio, información de nuevos productos, información estratégica como seguridad de la información, documentos de contratos entre empresas, etc.
3. Información financiera para comprender la situación comercial de la empresa/organización.
4. Información del cliente (incluida la información personal): nombre del cliente, dirección, número de teléfono, información de la tarjeta de crédito, historial de pedidos, proveedor/destino de ventas, etc.
5. Información del personal (incluida la información personal): número de teléfono móvil personal del empleado, dirección de correo electrónico, domicilio, información de la solicitud en el momento del empleo, salario, aumento de salario, información de asistencia, mi número, etc.
6. “Activos físicos” como equipos, instalaciones y vehículos.
7. Sistema de información, “software”, red interna (servidor/PC, equipo de comunicación, etc.), base de datos, “know-how” en tecnología informática, etc.
8. Activos intangibles como marcas de productos e imagen corporativa.

Además, existen varios tipos de activos de información y el método de clasificación difiere según la empresa, pero en general, se pueden clasificar ampliamente en ‘información’, ‘sistemas de información’ y 'activos tangibles'.

Figura 5. Clasificación de activos



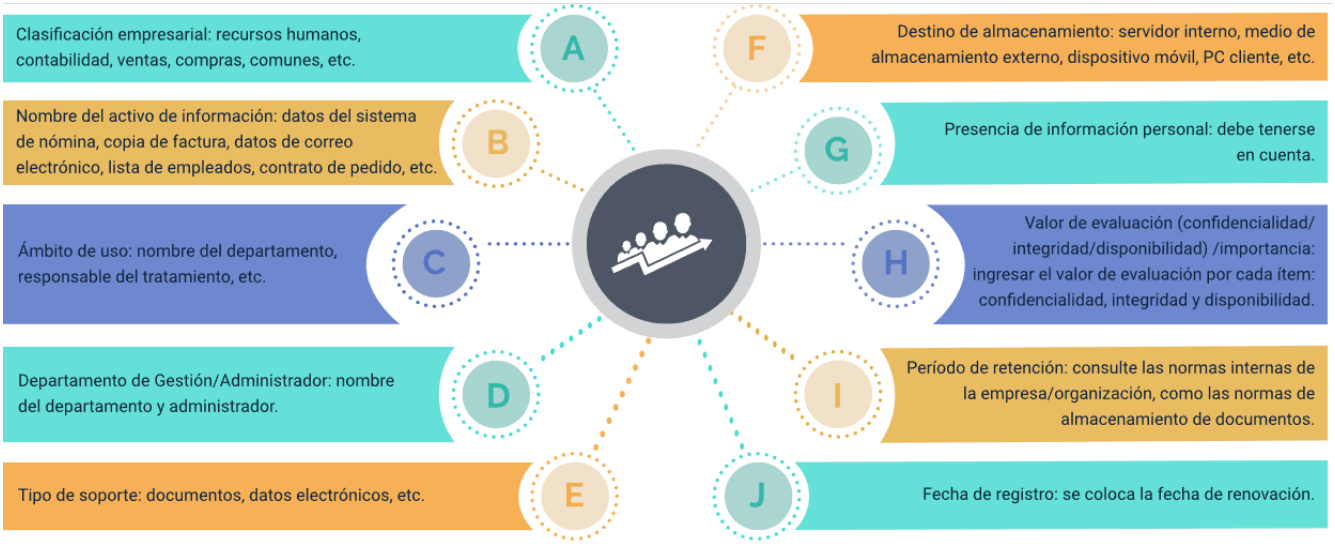
A partir de lo anterior, se hace necesario identificar los activos de información que pueden requerir algún tipo de respuesta entre los activos de información organizacionales. La información extraída está sujeta a evaluación de riesgos (análisis /evaluación de riesgos) y luego se convierte en un activo de información que examina la presencia o ausencia de contramedidas desde las perspectivas de confidencialidad, integridad y disponibilidad. Posteriormente, luego de su identificación, hay que confirmar en qué forma se almacenan los activos de información en la empresa u organización, dónde se utilizan, quién los utiliza y cómo se gestionan.

Una forma de identificar los activos de información es visualizar el flujo de negocios antes de hacerlo. Al verificar la lista de activos de información enumerados anteriormente de acuerdo con el trabajo real, se reducirá la posibilidad de identificar activos de información importantes.

Sin embargo, esto no significa que todos los activos de información deban ser identificados. Dado que los activos de información en poder de la organización cambian a diario, por tanto se recogen los activos de información que deben protegerse en la actualidad. Se recomienda verificar el flujo comercial antes de continuar. Ahora, si es difícil ordenar los activos de información, se debe pensar en el impacto en la organización si los activos de información se filtran, falsifican o pierden. Si tiene un impacto negativo en su organización, hay que agregarlo a la lista. Posteriormente, se clasifica la información desde el punto de vista vulnerabilidad de su naturaleza.

Algunos ejemplos de elementos de gestión, en el libro de mayor gestión de activos de información, son:

Figura 6. Ejemplos de elementos de gestión



A. Clasificación empresarial: recursos humanos, contabilidad, ventas, compras, comunes, etc.
B. Nombre del activo de información: datos del sistema de nómina, copia de factura, datos de correo electrónico, lista de empleados, contrato de pedido, etc.
C. Ámbito de uso: nombre del departamento, responsable del tratamiento, etc.
D. Departamento de Gestión/Administrador: nombre del departamento y administrador.
E. Tipo de soporte: documentos, datos electrónicos, etc.
F. Destino de almacenamiento: servidor interno, medio de almacenamiento externo, dispositivo móvil, PC cliente, etc.
G. Presencia de información personal: debe tenerse en cuenta.
H. Valor de evaluación (confidencialidad/integridad/disponibilidad) /importancia: ingresar el valor de evaluación por cada ítem: confidencialidad, integridad y disponibilidad.
I. Período de retención: consulte las normas internas de la empresa/organización, como las normas de almacenamiento de documentos.
J. Fecha de registro: se coloca la fecha de renovación.

Luego de clasificarlos, se categorizan por su valor: alto valor o bajo valor. Un ejemplo de alto valor son aquellos activos que pueden llegar a ser una pérdida significativa empresarial al no involucrarles en un plan de gestión. Por otro lado, los

informes trimestrales y la información publicada en páginas web, por ejemplo, son activos de bajo valor.

Después, la información categorizada como información valiosa se etiqueta aún más y se crean criterios de evaluación para esta. Por ejemplo, hay información con valor económico, información que seguramente causará pérdida en caso de fuga de información, información que puede reducir la credibilidad social e información personal. Se divide, entonces, la información en categorías y se clasifican según su importancia, estableciendo indicadores como la confidencialidad y el secreto. Al clasificar, se puede configurar medidas de seguridad que coincidan con cada requerimiento. Además, al usar información, será posible usarla de manera efectiva de acuerdo con el rango.

Es necesario identificar vulnerabilidades y amenazas para cada activo de información clasificado. Por ejemplo, se puede decir que un estado en el que "cualquiera puede acceder a información altamente confidencial" es un estado de alto riesgo porque no se han implementado medidas de seguridad de la información.

Los activos de información a proteger, entonces, se clasifican por categoría y se valoran (califican). Para las normas de clasificación y valoración, se es necesario consultar las normas unificadas de las agencias gubernamentales y las pautas establecidas por cada ministerio y agencia. A continuación, se muestra un ejemplo de evaluación del valor de los activos de información clasificada y calificada desde la perspectiva de la confidencialidad, integridad y disponibilidad (tres elementos). Si los tres elementos de los activos de información no se pueden asegurar, el grado de impacto en el negocio se evaluará paso a paso utilizando el ejemplo de evaluación del valor de los activos de información, en el que se adopta una evaluación de cuatro

niveles, y cuanto mayor sea el valor de la evaluación de importancia, mayor será el valor del activo de información:

Tabla 1. Ejemplo de evaluación del valor de un activo de información

Clasificación de importancia	Criterios de juicio	Arrasamiento
Confidencialidad (accesible solo para aquellos que otorgan acceso)	4 Si se filtra, el impacto en los socios comerciales y los clientes es grande. O tiene un impacto serio en la gestión.	Ultra secreto
Confidencialidad (accesible solo para aquellos que otorgan acceso)	3 En caso de fuga, el impacto en el negocio en cuestión es grande.	Secretaría extranjera
Confidencialidad (accesible solo para aquellos que otorgan acceso)	2 La fuga tendría poco impacto en el negocio en cuestión.	Secreto
Confidencialidad (accesible solo para aquellos que otorgan acceso)	1 Si se filtra, no hay impacto en el negocio en cuestión.	Divulgación general
Integridad (la información y los sistemas de información son precisos y completos)	4 Si se manipula, tendrá un gran impacto en los socios comerciales y clientes. O tiene un impacto serio en la gestión.	—
Integridad (la información y los sistemas de información son precisos y completos)	3 Si se manipula, el impacto en el negocio en cuestión es grande.	—
Integridad (la información y los sistemas de información son precisos y completos)	2 La falsificación tendría poco impacto en el negocio en cuestión.	—
Integridad (la información y los sistemas de información son precisos y completos)	1 Si es falsificado, no tiene impacto en el negocio en cuestión.	—
Disponibilidad (los beneficiarios de acceso pueden acceder a los	4 La suspensión del uso tendrá un gran impacto en los socios	—

activos de información cuando sea necesario)	comerciales y clientes. O tiene un impacto serio en la gestión.	
Disponibilidad (los beneficiarios de acceso pueden acceder a los activos de información cuando sea necesario)	3 En el caso de suspensión de uso, el impacto en el negocio en cuestión es grande.	—
Disponibilidad (los beneficiarios de acceso pueden acceder a los activos de información cuando sea necesario)	2 En el caso de suspensión de uso, casi no hay impacto en el negocio afectado.	—

La mayoría de los incidentes de violación de datos se dividen en tres categorías:

I. Error humano interno

Por ejemplo, dejar el HDD o USB utilizado para trabajar en otro espacio fuera de la oficina. En este caso, es posible que se puedan tomar medidas como establecer reglas internas para contactar con otras empresas o utilizar un servicio confiable en la nube.

II. Ataque externo

Incluyen el acceso no autorizado y los ataques cibernéticos. Se puede decir que es posible gestionar inmediatamente puntos como si el ID y la contraseña que está utilizando no son simples, si no se reutilizan y si el "software" está actualizado a la última versión. Por otra parte, también hay ataques por delitos internos. Existen casos en los que una persona dentro de una organización filtra información intencionalmente, en cuyo caso será necesario verificar el sistema de gestión de toda la empresa, como el control de acceso a la información confidencial.

III. Activo de la información

Los activos de información manejados por empresas y organizaciones incluyen activos de información con bajo valor de activo y activos de información valiosos como información de clientes (incluyendo información personal) e información de tecnología de productos. Para este caso se debe:

- ✓ Identificar todos los activos de información en su posesión.
- ✓ Identificar los activos de información que deben protegerse.
- ✓ Realizar la evaluación del valor de los activos de información (clasificación y calificación) para los activos de información identificados.
- ✓ Luego, los procesos posteriores (ciclo PDCA) pueden operarse de manera eficiente.

Para mantener la disponibilidad de los activos de información dentro de una empresa u organización, es necesario contar con copias de seguridad adecuadas de la información que se posee. Se requiere que el personal de administración de la información tenga operaciones de respaldo que puedan recuperarse rápidamente de fallas de la computadora o de la red, errores de operación del sistema, etc., con el menor impacto posible en el negocio.

En una empresa u organización, hay dos cosas principales que el personal de gestión de la información debe hacer para respaldar la información. La primera es una copia de seguridad de datos compartidos y la otra es una copia de seguridad de datos individuales.

Sumado a esto, también es una buena idea describir claramente el método y la frecuencia de las copias de seguridad como reglas internas en la política de seguridad de la información. A continuación, se describen estos aspectos:

A. Copia de seguridad del servidor

El personal de gestión de la información es responsable de realizar copias de seguridad de los datos compartidos almacenados en servidores de bases de datos y servidores de archivos. Normalmente, los datos en el servidor se respaldan en medios de cinta como DAT, DLT y AIT. Para ejecutar una copia de seguridad, utilice la utilidad de copia de seguridad proporcionada con el sistema operativo o una herramienta de copia de seguridad dedicada. Las copias de seguridad del servidor se realizan tarde en la noche o temprano en la mañana cuando los usuarios no están operando, utilizando las funciones de programación del sistema operativo y las herramientas de copia de seguridad.

B. Instrucciones de copia de seguridad

Los datos que los empleados y el personal almacenan también son activos de información importantes. Por lo tanto, se debe indicar a los usuarios de su organización que realicen una copia de seguridad de la información almacenada. Al hacerlo, se deben comprender correctamente el destino de almacenamiento de la copia de seguridad (medios, servidor de copia de seguridad, etc.), las herramientas y los métodos de copia de seguridad utilizados, la frecuencia de las copias de seguridad, etc., y proporcionar consejos y métodos. Se tiene que ser específico.

Tenga en cuenta que si los usuarios utilizan medios de almacenamiento externo para la copia de seguridad, se aumenta la posibilidad de fuga de información confidencial o personal debido a la eliminación de datos. Si se recomiendan medios de almacenamiento externo para la copia de seguridad, también es importante implementar minuciosamente reglas para la gestión de la información, como prohibir la eliminación innecesaria de datos y estipular ubicaciones de almacenamiento, en una política de seguridad de la información.

C. Administrar activos

Para proteger los activos de información, es fundamental garantizar la confidencialidad, integridad y disponibilidad:

- ✓ **Confidencialidad:** restringir el acceso no autorizado a la información.
- ✓ **Integridad:** prevenir manipulación o destrucción por personas no autorizadas.
- ✓ **Disponibilidad:** asegurar que los servicios de información estén siempre disponibles.

La gestión y mantenimiento de los activos de información son acciones clave para la seguridad. Es importante considerar las características de los activos y equilibrar confidencialidad, integridad y disponibilidad.

D. Clasificaciones para los activos de información

Los activos se clasifican según la importancia de la información y se determinan los métodos de gestión. Por ejemplo, mientras que la información personal y la información técnica se gestionan estrictamente, la información publicada en la Web no requiere el mismo grado de gestión estricta que la información personal y la información técnica. La

clasificación de los activos de información funciona como una etiqueta para determinar el grado y método de gestión de la información con el mismo valor e importancia.

E. Identificar activos de información

Tener personal comercial que identifique los activos de información tiene la ventaja de que, a diferencia de la identificación centralizada, se pueden evitar las omisiones porque se usa en las operaciones normales y es eficiente. Por ejemplo, para la base de datos maestra de clientes (base de datos), averigüe cuál de los siguientes es el lugar de uso, cuál es la forma de almacenamiento, dónde está el lugar de almacenamiento y cuál es el grado de importancia. Luego, se resume cada departamento en un archivo de Excel y se envía a la persona a cargo de la seguridad de la información para que pueda comprender los activos de información en general.

La gestión de activos de información comienza con la decisión de quién debe gestionar qué y en qué medida. Se muestra un ejemplo de los elementos enumerados en el libro mayor que pueden captar de forma centralizada la gestión de activos de información de toda la empresa. El libro mayor debe ser suficiente para proporcionar una descripción general del esquema de controles físicos/humanos u organizacionales/técnicos.

Tabla 2. Ejemplo de lo elementos en un libro mayor

Nombre del recurso de información	Datos del sistema de nómina, copia de factura, datos de correo electrónico, lista de empleados, contrato de pedido, etc.
Rango de uso	Nombre del departamento, responsable del tratamiento, etc.

Departamento de Gestión / Gerente	Nombre y gerente del departamento.
Autoridad de acceso	Gerente o superior, todas las personas a cargo, solo grupo empresarial, etc.
Tipo de medio	Documentos, datos electrónicos, etc.
Destino	Servidores internos, medios de almacenamiento externo, dispositivos móviles, PC cliente, etc.
Presencia o ausencia de información personal	Presencia o ausencia.
Presencia o ausencia de información de mi Número	Presencia o ausencia.
Valor de la evaluación (confidencialidad/integridad/disponibilidad)/importancia	Valor de evaluación: Ingrese cada valor de evaluación para confidencialidad, integridad y disponibilidad Importancia: Ingrese el valor más alto entre confidencialidad, integridad y disponibilidad.
Periodo de retención	De acuerdo con las normas internas de la empresa/organización, como las normas de almacenamiento de documentos.
Fecha de registro (fecha de renovación)	AAMMDD

2.2. Realización de informes técnicos de gestión de información

Toda organización necesita informes de ciberseguridad precisos y convincentes; siendo estos vitales para la comunicación interna sobre la gestión del desempeño del riesgo cibernético, pues esto puede significar la diferencia entre sistemas seguros e incidentes masivos. A medida que disminuyen los presupuestos y los equipos continúan adaptándose a un nuevo entorno operativo, es más importante que nunca contar con una estrategia sólida para evaluar, monitorear e informar sobre la gestión del desempeño del riesgo cibernético a lo largo del tiempo.

Los informes de ciberseguridad, lejos de ser un trámite, son el mecanismo de control de esta comunicación. Al adoptar un enfoque basado en el riesgo para los informes de seguridad cibernética, puede evaluar la gestión del desempeño del mismo en función de la exposición real a las amenazas cibernéticas, proporcionar un contexto procesable, resaltar el valor de sus esfuerzos de seguridad cibernética y asegurarse de que está aprovechando al máximo sus recursos limitados.

Los informes de seguridad cibernética basados en el riesgo, a diferencia de los informes integrales, basados en el cumplimiento o basados en incidentes, son el enfoque más adecuado para reducir la exposición de su organización a las amenazas cibernéticas. Seguir un enfoque basado en el riesgo para los informes de seguridad cibernética puede ayudar a las personas y equipos en todos los niveles a enfocarse en los problemas más importantes sin ser víctimas de la fatiga de alertas y las advertencias ignoradas.

Hay ciertos factores que pueden ayudar a determinar si cualquier reporte de ciberseguridad es efectivo:

- ✓ ¿El informe transmite información procesable en contexto?
- ✓ ¿Es el informe lo suficientemente conciso para que los hallazgos clave no queden enterrados?
- ✓ ¿El lenguaje es lo suficientemente claro para que lo entienda una audiencia no técnica?
- ✓ ¿El informe relaciona los hallazgos con el riesgo cibernético?

La última pregunta es la más importante porque forma la base de un enfoque basado en el riesgo para la gestión del desempeño de la seguridad cibernética.

Las métricas presentadas en el vacío rara vez son procesables. ¿Qué significa, por ejemplo, que sus cortafuegos hayan detenido 1.500 intrusiones este mes? ¿Es eso mucho o poco?

Un informe de ciberseguridad basado en el riesgo ofrece hallazgos en contexto, lo que ayuda al destinatario a comprender qué papel juega un número en el panorama general de riesgos de la organización. Ese contexto puede incluir:

A. **Desempeño pasado**

   ¿Cómo fueron estos mismos números el mes pasado o el último trimestre? ¿Estás mejorando o empeorando con el tiempo?

B. **Concentración de riesgos**

   ¿Cómo se están desempeñando las diferentes unidades de negocios y subsidiarias en su organización?

C. **Puntos de referencia de la industria**

   ¿Cómo se compara su desempeño con el de sus pares y competidores?

D. **Cuantificación financiera**

   ¿Qué está en juego financieramente con su postura de riesgo actual?

E. **Marcos de seguridad cibernética**

   ¿Cómo se alinean sus hallazgos con los marcos de seguridad cibernética para su industria?

Con el contexto apropiado, los profesionales, gerentes, ejecutivos y miembros de la Junta pueden tomar decisiones más seguras sobre la gestión del desempeño del riesgo cibernético. Armados con esta información, pueden asignar los recursos apropiados a los proyectos que tienen más probabilidades de reducir el riesgo en toda la organización.

Sumado a esto, los elementos centrales de la información basada en el riesgo son:

- ✓ Cómo presentar las métricas en contexto para lograr el máximo impacto.
- ✓ Enfoques específicos para miembros de la Junta, ejecutivos, gerentes y profesionales.
- ✓ Una guía práctica para la elaboración de informes de ciberseguridad basados en el riesgo.
- ✓ Ver sus informes e investigaciones.
- ✓ Primer nombre.
- ✓ Apellido.
- ✓ Correo electrónico de la empresa.
- ✓ Introduzca la dirección de correo electrónico.
- ✓ Teléfono.
- ✓ Nombre de empresa.
- ✓ Puesto de trabajo.
- ✓ Nivel de trabajo.

Ahora bien, siendo realistas, los expertos en tecnología de la información no suelen ser escritores entusiastas. Entonces, cuando se trata de crear un informe ejecutivo, el personal de seguridad cibernética no se presiona entre sí para completar esta emocionante tarea de redacción. En cambio, sigue retrasándose, día a día, hasta la noche anterior a su presentación. Muchos se atascan en la sección del resumen ejecutivo, obsesionados con su perfección. Esto es comprensible, ya que el resumen ejecutivo es probablemente el componente más importante del informe. Todos los

interesados juzgan el valor de un informe por su resumen ejecutivo y algunos no leen nada más que el resumen.

El resumen ejecutivo de su informe de ciberseguridad es solo eso: ¡Un resumen! No se llena de explicaciones técnicas; para eso está el cuerpo del informe (e incluso entonces, debe mantener sus divagaciones técnicas restringidas). Su informe ejecutivo debe adaptarse a las expectativas del equipo de liderazgo, y la mayoría de ellos no quieren jerga técnica. El resumen ejecutivo debe resumir sucintamente los esfuerzos de su programa de seguridad y abordar todas las preocupaciones de seguridad de alto nivel del equipo de liderazgo.

Un resumen ejecutivo debe estar compuesto por los siguientes encabezados:

- ✓ Resultados clave.
- ✓ Resumen de monitoreo de riesgos de seguridad.
- ✓ Resumen del incidente cibernético.
- ✓ Resumen de ciberamenazas.
- ✓ Recomendaciones de remediación.

Este conjunto de encabezados es característico de un método clásico de estructuración de un resumen ejecutivo para un informe de seguridad. Si bien esta estructura clásica aún es aceptable, si realmente desea impresionar al equipo de liderazgo, considere usar un estilo de informes de seguridad cibernética más moderno en su próximo ciclo de informes. Más detalles a continuación:

A. Resultados clave

La sección de hallazgos clave es un resumen de alto nivel de los principales riesgos de seguridad encontrados en el período de informe actual. También

debe resumir los esfuerzos de remediación que abordaron estos riesgos y su eficacia. Algunos ejemplos de incidentes de seguridad dignos de incluir en esta sección son:

- ✓ Ataques de "phishing": especialmente las campañas que involucran a piratas informáticos que se hacen pasar por ejecutivos de C-suite.
- ✓ Vulnerabilidades críticas: incluidas las vulnerabilidades de día cero, como Log4Shell y Spring4Shell.
- ✓ Inyecciones de "malware": incluidos los ataques fallidos de "ransomware" y otros intentos de ciberataques.
- ✓ Abuso de control de acceso: como intentos de escalada de privilegios.
- ✓ Violaciones de datos: los vectores de ataque específicos que facilitaron cada intento de violación de seguridad.
- ✓ Amenazas a la seguridad física: incluidos los discos duros perdidos.
- ✓ Vulnerabilidades críticas del proveedor de servicios: configuraciones incorrectas de "software" y fugas de datos en el ecosistema de terceros, ya sea que estén relacionadas con prácticas de seguridad deficientes o controles de seguridad insuficientes.
- ✓ Algunos detalles de mitigación de amenazas dignos de mencionar:
  - Protocolos del Plan de Respuesta a Incidentes que se activaron para cada riesgo cibernético enumerado.
  - Metodologías utilizadas para medir el impacto del riesgo.
  - El ciclo de vida de cada evento de seguridad.
  - El impacto en los sistemas informáticos y los sistemas de información.

- Resumen de monitoreo de riesgos de seguridad.

Resuma la gama de riesgos de seguridad y amenazas cibernéticas monitoreados en el ciclo de informes actual. Es igual de importante mencionar qué regiones del ecosistema de TI no se monitorearon y por qué. Además, se describe la metodología de monitoreo de riesgos utilizada, es decir, monitoreo de superficie de ataque en tiempo real.

B. Resumen del incidente cibernético

La sección de incidentes relacionados con la seguridad es una descripción más detallada de los principales esfuerzos de remediación mencionados en los hallazgos clave. Concéntrese en los incidentes de seguridad más críticos, aquellos que potencialmente perjudican más su postura de seguridad. Dichos eventos en el panorama de amenazas de terceros son más fáciles de rastrear e identificar si está implementando una estrategia de nivelación de proveedores. Demuestre un compromiso con la mejora continúa, comparando sus esfuerzos de gestión de riesgos con las políticas de seguridad y métricas clave como el tiempo medio de contención (MTTC), el tiempo medio de resolución (MTTR), etc.

Además, se mencionan los controles de seguridad específicos que previnieron incidentes cibernéticos, como la autenticación de múltiples factores o los controles específicos del marco de seguridad cibernética.

Debido a que esta sección del informe ofrece una explicación más profunda de los incidentes cibernéticos encontrados, existe el riesgo de ser demasiado técnico con su redacción. Pero no se obsesione con mantener una línea de base establecida de simplicidad. Tiene un representante

técnico en el equipo ejecutivo que puede ofrecer más aclaraciones si es necesario: el CISO.

C. **Resumen de ciberamenazas**

La sección anterior se centró en los incidentes cibernéticos que afectan su postura de seguridad, incluidos los iniciados por los ciberdelincuentes. Esta sección debe centrarse en las amenazas emergentes en su ecosistema, internamente y en toda la red de terceros. Describir los mecanismos utilizados para descubrir estas amenazas, es decir, evaluaciones de riesgo. Las amenazas cibernéticas también incluyen el incumplimiento de regulaciones de seguridad críticas como PCI DSS y HIPAA, especialmente para industrias altamente reguladas como la atención médica.

D. **Recomendaciones de remediación**

Esta sección final debe resumir los procesos de remediación necesarios para abordar los riesgos emergentes mencionados en la sección anterior. Si estas iniciativas de remediación requieren una inversión adicional, incluya sus costos aproximados. Justifique el ROI de sus solicitudes de inversión asignándolas a los costos de daños potenciales de los riesgos cibernéticos que abordarán.

Los elementos gráficos y los cuadros representan los KPI de ciberseguridad que más importan a los ejecutivos, con gráficos y elementos visuales que hacen que sus esfuerzos de seguridad sean más fáciles de comprender y apreciar.

El "software" de calificación de seguridad es el método más popular para monitorear los riesgos de seguridad emergentes y las desviaciones de la postura de

seguridad. Si su equipo de seguridad de la información utiliza una herramienta de este tipo, asegúrese de resumir los vectores de ataque de seguridad de datos específicos que influyen en el cálculo de su calificación de seguridad.

Los informes ejecutivos en ciberseguridad son importantes porque mantienen informados a los líderes empresariales y a las partes interesadas sobre el progreso de las iniciativas de ciberseguridad, lo que les permite realizar un seguimiento de la alineación de la ciberseguridad con los objetivos generales de la empresa.

Un sistema eficiente de informes ejecutivos fortalece la cadena de mando entre el personal de liderazgo responsable de supervisar las políticas y estrategias de seguridad de la empresa, como el director de seguridad de la información (CISO) o el director de información (CIO), y los equipos de ciberseguridad que implementan estas iniciativas.

Las partes interesadas y los ejecutivos que toman decisiones, que en el pasado preferían evitar los detalles técnicos de las iniciativas de ciberseguridad, ahora están más informados sobre los riesgos asociados con las violaciones de datos y las malas posturas de ciberseguridad. Los ejecutivos exigen cada vez informes más transparentes para ayudar en las decisiones comerciales y realizar un seguimiento de las mejoras en la respuesta a incidentes.

Un informe valioso de ciberseguridad es aquel que realmente brinda a los ejecutivos información útil. Por lo tanto, el proceso de creación de un informe de ciberseguridad efectivo debe comenzar con una comprensión clara de los requisitos de información clave de los equipos ejecutivos. Para comprender la mentalidad de un ejecutivo, estas son las principales preocupaciones y atributos de un equipo de

liderazgo típico compuesto por miembros de la junta, partes interesadas y ejecutivos de C-Suite:

A. **El equipo de liderazgo no quiere ver a la empresa en un titular de noticias**

   Tras el ataque a “SolarWinds”, los ejecutivos están preocupados por los riesgos de seguridad informática y las violaciones de datos. Quieren respuestas claras sobre el riesgo de filtración de datos, las vulnerabilidades, el plan de respuesta a incidentes, los incidentes recientes, las estrategias de mitigación de riesgos, la defensa contra “ransomware” y la comparación de los esfuerzos de seguridad con los estándares de la industria. El informe debe incluir un resumen de las amenazas emergentes y las tendencias de ataque, evitando detalles técnicos innecesarios.

B. **Resultados del análisis de vulnerabilidades**

   Resultados del análisis de vulnerabilidades que muestran desviaciones en la calificación de seguridad durante un período determinado, desviaciones de calificación de seguridad a lo largo del tiempo por parte del reportaje de un ejecutivo generado en la plataforma.

C. **Desglose del riesgo de seguridad por categoría**

   Un desglose del riesgo de seguridad en todas las categorías de amenazas principales dentro del ecosistema de la empresa, categorizado por grado de criticidad y desglose de riesgos por categoría; una característica de un informe ejecutivo generado.

D. Amenaza de infracciones de terceros

Los riesgos de seguridad de terceros han sido la causa principal de filtraciones de datos. Los ejecutivos están cada vez más preocupados por estos riesgos y buscan respuestas sobre la gestión de riesgos de proveedores en informes de seguridad cibernética. Es importante comprender la distribución de los riesgos de terceros según su criticidad y priorizarlos según el apetito de riesgo predefinido. Los riesgos residuales siempre estarán presentes y deben ser abordados adecuadamente.

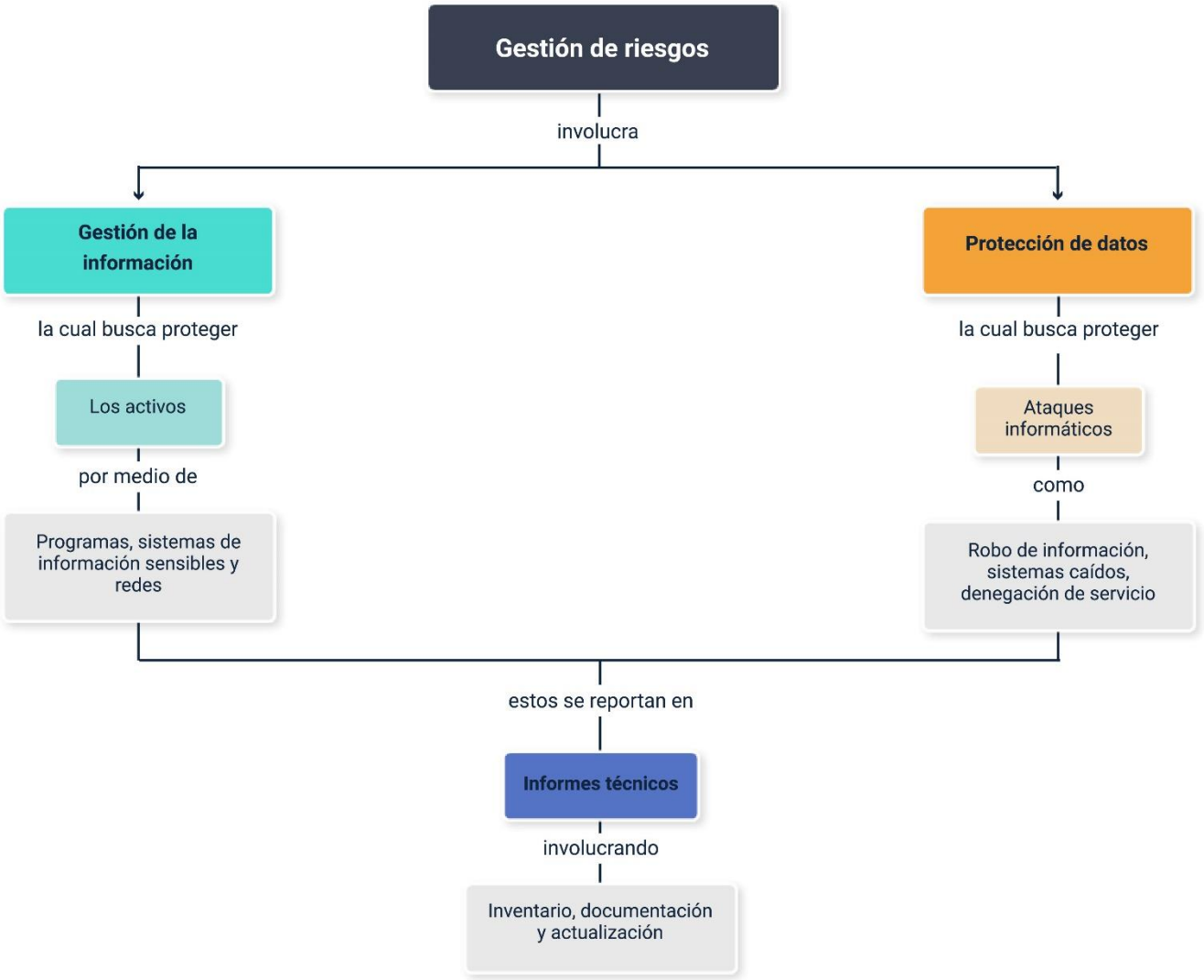
El equipo de liderazgo, entonces, establece las expectativas de seguridad para la empresa y el CISO (Director de seguridad de la Información) tiene la tarea de garantizar que el programa de ciberseguridad cumpla con estas expectativas. El desempeño de un programa de seguridad cibernética se resume de manera más eficiente con una evaluación de las métricas de seguridad clave. Estas métricas deben alinearse con la estrategia de gestión de riesgos empresariales que está implementando el CISO. Esta lista de métricas aún podría ser más exhaustiva de lo que prefiere la junta. Si este es el caso, las siguientes preguntas lo ayudarán a filtrar las métricas de seguridad más significativas:

- ✓ ¿Qué información está tratando de comunicar a la junta?
- ✓ ¿Qué respuestas pretende estimular (inversiones en nuevas tecnologías, etc.)?
- ✓ ¿Qué detalles quiere que la junta entienda mejor?
- ✓ ¿Qué miedos o frustraciones clave pretende abordar?

Finalmente, una vez que haya terminado su lista de métricas, siempre ayuda respaldarlas con gráficos relevantes.

Síntesis

Una vez se ha reconocido la importancia sobre la responsabilidad y acciones que se deben para salvaguardar los activos informáticos ante ataques de ciberseguridad, se sintetiza cada uno de los aspectos desarrollados:



Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
1. Seguridad informática en la organización	Cardador Cabello, A. L. (2018*). Ciberseguridad para Usuarios IFCT135PO*. IC Editorial.	Libro	https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=sena_aleph000106036&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=L
1.3. Procesos de mejora para el tratamiento de la información	Villalobos-Murillo, J. (2008). *Vulnerabilidad de sistemas gestores de bases de datos*. Uniciencia, 22 (1-2), p. 131-134	Artículo	https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=TN_cdi_dialnet_primary_oai_dialnet_unirioja_es_ART0000922259&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=PC
1.3. Procesos de mejora para el tratamiento de la información	Rascagneres, P. (2020). *Seguridad informática y malwares: análisis de amenazas e implementación de contramedidas.* (3ª ed.) Barcelona: Ediciones ENI.	Libro	https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=sena_biblioteca_eniEPT3MAL&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=L
1.4. Gestión de copias de seguridad	Païola, P. (2021). *Microsoft Azure: Gestione su Sistema de Información en la Nube*. Barcelona: Ediciones ENI.	Libro	https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=sena_biblioteca_eniEPT3AZWIN&vid=SENA&search_s

			cope=sena_completo&tab=sena_completo&lang=es_ES&context=L
2. Gestión de la información	Balseca Chávez, F., Colina Vargas, A. & Espinoza Mina, M. A. (2021). *Identificación de amenazas informáticas aplicando arquitecturas de Big Data*. INNOVA Research Journal, 6(3).	Libro	https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=TN_cdi_dialnet_primary_oai_dialnet_unirioja_es_ART0001502522&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=PC
2. Gestión de la información	Piattini Velthius, M. & Ruiz González, F. (2021). *Gobierno y gestión de las tecnologías y los sistemas de información*. Bogotá Ediciones de la U.	Libro	https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=sena_ebooks00029&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=L
2. Gestión de la información	Poggioli, J. & Demasson, J. (2021). *Gestión de un sistema de información: método y buenas prácticas*. Barcelona: Ediciones ENI	Libro	https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=sena_biblioteca_eniDPT2PILSI&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=L

Glosario

Análisis de riesgos: es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

Auditoría de seguridad: es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales en tecnologías de la información (TI) con el objetivo de identificar, enumerar y describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores o aplicaciones.

Aviso legal: es un documento, en una página web, donde se recogen las cuestiones legales que son exigidas por la normativa de aplicación.

"Backup": copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados.

Biometría: es un método de reconocimiento de personas basado en sus características fisiológicas (huellas dactilares, retinas, iris, cara, etc.) o de comportamiento (firma, forma de andar, tecleo, etc.).

"Bug": es un error o fallo en un programa de dispositivo o sistema de "software" que desencadena un resultado indeseado.

Centro de respaldo: un centro de respaldo es un centro de procesamiento de datos (CPD) específicamente diseñado para tomar el control de otro CPD principal en caso de contingencia.

Certificado de autenticidad: el Certificado de autenticidad (COA) es una etiqueta especial de seguridad que acompaña a un software con licencia legal para impedir falsificaciones.

Cortafuegos: sistema de seguridad compuesto o bien de programas ("software") o de dispositivos "hardware" situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios.

Denegación de servicio: se entiende, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar los servicios por prestados por él.

Disponibilidad: se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

Fuga de datos: es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no debería ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros.

Incidente de seguridad: cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

Inyección SQL: es un tipo de ataque que se aprovecha de una vulnerabilidad en la validación de los contenidos introducidos en un formulario web y que puede permitir la obtención de forma ilegítima de los datos almacenados en la base de datos del sitio web, entre ellos las credenciales de acceso.

Referencias bibliográficas

Intel (s.f.). *Intel® QuickAssist Adapter Family for Servers*. https://www.intel.la/content/www/xl/es/products/docs/network-io/ethernet/10-25-40-gigabit-adapters/quickassist-adapter-for-servers.html

Logic technology. (s.f.). *Intel® oneAPI AI Analytics Toolkit*. https://www.logic.nl/ides/intel-oneapi-ai-analytics-toolkit/

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal Gutiérrez	Responsable del equipo	Dirección General
Liliana Victoria Morales Gualdrón	Responsable de línea de producción	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Ronald Alexander Vacca Ascanio	Experto temático	Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios
Miroslava González Hernández	Diseño instruccional	Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios
Andrés Felipe Velandia Espitia	Asesoría metodológica y pedagógica	Regional Distrito Capital - Centro de Diseño y Metrología
Rafael Neftalí Lizcano Reyes	Responsable equipo desarrollo curricular	Regional Santander - Centro Industrial del Diseño y la Manufactura
Gloria Lida Alzate Suarez	Adecuador instruccional	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Alix Cecilia Chinchilla Rueda	Asesoría metodológica y pedagógica	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Jesús Antonio Vecino Valero	Diseñador web	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Adriana Marcela Suarez Eljure	Diseñador web	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información

Nombre	Cargo	Regional y Centro de Formación
Jhon Jairo Urueta Álvarez	Desarrollador fullstack	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Lady Adriana Ariza Luque	Animador y producción audiovisual	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Zuleidy María Ruiz Torres	Validador de recursos Educativos Digitales	Regional Santander - Centro Industrial del Diseño y la Manufactura
Luis Gabriel Urueta Álvarez	Validador de recursos Educativos Digitales	Regional Santander - Centro Industrial del Diseño y la Manufactura
Daniel Ricardo Mutis Gómez	Evaluador para contenidos inclusivos y accesibles	Regional Santander - Centro Industrial del Diseño y la Manufactura
Carolina Coca Salazar	Evaluación de contenidos inclusivos y accesibles	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Lina Marcela Pérez Manchego	Validación de recursos educativos digitales	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Leyson Fabian Castaño Pérez	Validación de recursos educativos digitales y vinculación LMS	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información