**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Técnico en sistemas teleinformáticos. |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220501121 - Operar herramientas informáticas y digitales de acuerdo con protocolos y manuales técnicos. | RESULTADOS DE APRENDIZAJE | 20501121-03. Tratar la información según criterios de ciberseguridad.  220501121-04. Documentar la gestión de la información acuerdo a protocolos establecidos. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | CF02 |
| NOMBRE DEL COMPONENTE FORMATIVO | 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. |
| PALABRAS CLAVE | Amenaza, controles, riesgo, seguridad, vulnerabilidad. |

|  |  |
| --- | --- |
| ÁREA OCUPACIONAL | 2 - CIENCIAS NATURALES, APLICADAS Y RELACIONADAS. |
| IDIOMA | Español. |

1. **TABLA DE CONTENIDOS:**

**Introducción**

**1. Seguridad informática en la organización**

1.1 Privilegios de acceso y seguridad de la información

1.2 Monitoreo del almacenamiento de la información

1.3 Procesos de mejora para el tratamiento de la información

1.4 Gestión de las copias de seguridad

**2. Gestión de la información**

2.1 Actualización de bases de datos de activos de la información

2.2 Realización de informes técnicos de gestión de información

**Síntesis**

1. **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:

|  |
| --- |
| **CF02\_video\_Introducción** |

1. **DESARROLLO DE CONTENIDOS:**

**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.

|  |  |
| --- | --- |
| Tableta de toque de mano con foto gratis | 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 *softwares* 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:

|  |
| --- |
| **CF02\_\_1\_1\_gráfico\_preguntas base** |

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:

|  |
| --- |
| **CF02\_\_1\_1\_infografía\_con\_audio\_control de acceso** |

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:

|  |
| --- |
| **CF02\_\_1\_1\_infografía\_interactiva\_componentes** |

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.

|  |  |
| --- | --- |
| Free photo composition with person working in human resources | 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:

|  |
| --- |
| **CF02\_\_1\_1\_video\_factores de control** |

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:

|  |
| --- |
| **CF02\_\_1\_1\_infografía\_interactiva\_modelos de control** |
| 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 todo 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).

|  |  |
| --- | --- |
| Free photo standard quality control concept m | 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:

|  |
| --- |
| **CF02\_\_1\_2\_pestañas\_tipos de almacenamiento** |

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:

|  |
| --- |
| **CF02\_\_1\_2\_slider\_con numerales\_funcionalidades** |

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:

|  |
| --- |
| **CF02\_\_1\_2\_gráfico\_tareas de herramientas** |

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.

|  |  |
| --- | --- |
| Free photo man with his hand in digital sphere | **¿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:

|  |
| --- |
| **CF02\_\_1\_3\_pasos\_verticales\_etapas** |

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.

|  |  |
| --- | --- |
| Free photo man with a tablet and clouds background icons | 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.

|  |  |
| --- | --- |
| Photo portrait of a happy young male technician holding computer chip | 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:

|  |
| --- |
| **CF02\_\_1\_3\_acordeón\_métodos de procesamiento** |

|  |
| --- |
| 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:

|  |
| --- |
| **CF02\_1\_3\_pestañas\_Intel** |

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:

|  |
| --- |
| **CF02\_1\_4\_pestañas verticales\_gestión de copias** |

|  |
| --- |
| 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.

|  |  |
| --- | --- |
| Free photo index finger pressing a shiny button | 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:

|  |
| --- |
| **CF02\_1\_4\_infografía interactiva\_causas** |

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

|  |
| --- |
| **CF02\_1\_4\_slide\_métodos** |

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.

|  |
| --- |
| **CF02\_1\_4\_gráfico\_consideraciones** |

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:

|  |
| --- |
| **CF02\_1\_4\_Acordeón\_notas adicionales** |

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

|  |
| --- |
| **CF02\_1\_4\_tarjetas\_fallas** |

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:

|  |
| --- |
| **CF02\_1\_4\_infografía interactiva\_aspectos de las copias** |

**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. | Photo cyber security and digital data protection concept |

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.

|  |  |
| --- | --- |
| Photo cybersecurity and privacy concepts to protect data lock icon and internet network security technology businessman protecting personal data on smart phone with virtual screen interfaces | 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.

|  |
| --- |
| **CF02\_2\_slide\_importancia de la gestión** |

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:

|  |
| --- |
| **CF02\_2\_infografía interactiva\_medidas de seguridad** |

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:

|  |
| --- |
| **CF02\_2\_pestañas\_definición de la gestión** |

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:

|  |
| --- |
| **CF02\_2\_acordeón\_situaciones** |

**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:

|  |
| --- |
| **CF02\_2\_1\_infográfia\_activos** |

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 1**

*Clasificación de activos*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Medios de papel | Medios de memoria externa | Audio | Imagen | Saber hacer | Aplicaciones empresariales, atención al cliente. | Equipo de red/Equipo de información |
| Información en papel | Información electrónica (incluyendo audio y video) | Conocimiento | Software | Hardware |
| Activos Tangibles | | Activos Intangibles | | |
| Información | | | | | Sistema de Información | |
| Activos de Información | | | | | | |

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

|  |
| --- |
| **CF02\_2\_1\_infografía\_clasificación de activos** |

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.

|  |  |
| --- | --- |
| Free photo e-mail popup warning window concept | 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:

**Figura 2**

*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 |
| 3 En caso de fuga, el impacto en el negocio en cuestión es grande | Secretaria extranjera |
| 2 La fuga tendría poco impacto en el negocio en cuestión | Secreto |
| 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. | － |
| 3 Si se manipula, el impacto en el negocio en cuestión es grande | － |
| 2 La falsificación tendría poco impacto en el negocio en cuestión | － |
| 1 Si es falsificado, no tiene impacto en el negocio en cuestión | － |
| Disponibilidad (los beneficiarios de acceso pueden acceder a los activos de información cuando sea necesario) | 4 La suspensión del uso tendrá un gran impacto en los socios comerciales y clientes. O tiene un impacto serio en la gestión. | － |
| 3 En el caso de suspensión de uso, el impacto en el negocio en cuestión es grande | － |
| 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:

|  |
| --- |
| **CF02\_2\_1\_pestañas\_categorías de violación de datos** |

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:

|  |
| --- |
| **CF02\_2\_1\_acordeón\_acciones de respaldo** |

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.

**Figura 3**

*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 la 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.

|  |  |
| --- | --- |
| Photo female psychologist listening to problems of african american woman | 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:

|  |
| --- |
| **CF02\_2\_2\_tarjetas\_aspectos de contexto** |

|  |
| --- |
| 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.

|  |  |
| --- | --- |
| Free photo people using digital device while in a meeting | 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:

|  |
| --- |
| **CF02\_2\_2\_pestañas verticales\_encabezados** |

|  |
| --- |
| 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.

|  |  |
| --- | --- |
| Free photo business meeting at night | 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:

|  |
| --- |
| **CF02\_2\_2\_acordeón\_preocupaciones** |

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.

**C. 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:

|  |
| --- |
| **CF02\_gráfico\_síntesis** |

1. **ACTIVIDADES DIDÁCTICAS**

|  |  |
| --- | --- |
| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| Nombre de la Actividad | Ciberseguridad en las organizaciones |
| Objetivo de la actividad | Apropiar los conceptos más importantes asociados a los sistemas informáticos, de acuerdo a los procesos de ciberseguridad en las organizaciones. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | CF02\_Actividad didáctica\_01 |

1. **MATERIAL COMPLEMENTARIO:**

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | Referencia APA del Material | Tipo de material  (Video, capítulo de libro, artículo, otro) | Enlace del Recurso o  Archivo del documento o material |
| 1. Seguridad informática en la organización | Arroyo Guardeño, D., Martínez, Gayoso, V. & Encinas Hernández, L. (2020). *Ciberseguridad*. Madrid: CSIC : Los Libros de la Catarata | Libro | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_elibroELB172144> |
| 1. Seguridad informática en la organización | Cardador Cabello, A. L. (2018). *Ciberseguridad para Usuarios IFCT135PO*. IC Editorial. | Libro | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_aleph000106036> |
| 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 | Articulo | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_dialnet_primary_oai_dialnet_unirioja_es_ART0000922259> |
| 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. (2ª ed.) Barcelona: Ediciones ENI. | Libro | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_biblioteca_eniEPT3MAL> |
| 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/permalink/f/1j5choe/sena_biblioteca_eniEPT3AZWIN> |
| 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/permalink/f/1i756fj/TN_cdi_dialnet_primary_oai_dialnet_unirioja_es_ART0001502522> |
| 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/permalink/f/1j5choe/sena_ebooks00029> |
| 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/permalink/f/1j5choe/sena_biblioteca_eniDPT2PILSI> |

1. **GLOSARIO:**

|  |  |
| --- | --- |
| TÉRMINO | SIGNIFICADO |
| 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. |

1. **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/>

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| Autor (es) | Ronald Alexander Vacca Ascanio | Experto temático | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios | Diciembre 2022 |
| Miroslava González Hernández | Diseñadora y evaluadora Instruccional | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios | Diciembre 2022 |
| Andrés Felipe Velandia Espitia | Asesor Metodológico | Regional Distrito Capital – Centro de Diseño y Metrología | Diciembre 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo Desarrollo Curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura | Diciembre 2022 |

1. **CONTROL DE CAMBIOS**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** | **Razón del Cambio** |
| **Autor (es)** | Gloria Lida Alzate Suarez | Adecuador Instruccional | Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información. | Julio de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |
| Alix Cecilia Chinchilla Rueda | Asesor Metodológico | Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información. | Julio de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |
| Liliana Victoria Morales Guadrón | Responsable Línea de Producción Distrito Capital. | Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información. | Julio de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |

**Nota:**Para la propuesta instruccional se deben tener en cuenta las métricas desarrolladas en el equipo:

<https://drive.google.com/drive/u/1/folders/1UiJvaklSCICR4BaQ7ga_q04JFa53h_u_>