Seguridad de la información

Lectura

¡Bienvenido al curso Fundamentos de Seguridad de la Información! En esta primera unidad, explorarás los fundamentos de la seguridad de la información, en base a la triada de la seguridad de la información. También aprenderás sobre los requisitos para la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI), acorde con la Norma ISO 27001, así como sobre controles CSI. Se espera que logres la base teórica para aplicar los elementos que conforman la triada de la seguridad de la información, con el fin de dar cumplimiento a las normas y procedimientos establecidos en el marco de los Framework de seguridad.

¡Adelante!

Fundamentos de la Seguridad de la Información

La triada de la seguridad de la información

En la era digital actual, la información se ha convertido en un activo invaluable para individuos, organizaciones y sociedades. Su protección es crucial para garantizar la continuidad de las operaciones, la privacidad de los datos y la confianza en los sistemas informáticos**.** Los fundamentos de la seguridad de la información se basan en la triada de la seguridad, cuyos principios —confidencialidad, integridad y disponibilidad-— establecen los objetivos básicos para la protección de la información. Por ello, es importante analizar dichos principios.

La triada de la seguridad de la información es un concepto fundamental en el ámbito de la seguridad informática que se compone de tres elementos principales: **confidencialidad, integridad y disponibilidad.** Estos elementos trabajan en conjunto para garantizar la protección adecuada de la información sensible y los sistemas de una organización.

Estos son los componentes de la triada de la información:

a) **Confidencialidad:** Este principio se refiere a la protección de la información contra accesos no autorizados. En otras palabras, asegura que la información sensible solo esté disponible para aquellos usuarios o sistemas que tengan los permisos adecuados de acceso. Para garantizar la confidencialidad, se utilizan técnicas como la **encriptación, la autenticación y la gestión de acceso.**

   Ejemplo: Una empresa financiera utiliza el cifrado para proteger los datos de sus clientes. Cuando un cliente ingresa su información personal y detalles bancarios en el sitio web de la empresa, estos datos son cifrados y solo pueden ser descifrados por el servidor seguro de la empresa. Además, se implementan controles de acceso estrictos, como la autenticación de dos factores (2FA), para asegurar que solo los empleados autorizados puedan acceder a la información confidencial de los clientes.

b) **Integridad:** Este principio se refiere a la garantía de que la información no ha sido alterada o modificada sin autorización. Esto implica asegurar que los datos sean

precisos, completos y fiables. Para lograr la integridad de la información, se utilizan técnicas como firmas digitales, *checksums* y registros de auditoría; estas permiten detectar y prevenir cualquier alteración no autorizada de los datos.

Ejemplo: Una compañía de software emplea **firmas digitales** para garantizar que sus actualizaciones de software no sean alteradas. Cuando los desarrolladores lanzan una nueva versión de su software, adjuntan una firma digital única. Los usuarios que descargan e instalan la actualización pueden verificar la firma digital para asegurarse de que la actualización proviene de una fuente confiable y no ha sido modificada. Además, la empresa usa **sumas de verificación (checksums)** para validar que los archivos no han sido corrompidos durante la transferencia.

c) **Disponibilidad:** La disponibilidad se refiere a la garantía de que los sistemas y la información están disponibles y accesibles cuando se necesitan. Esto implica proteger los sistemas contra interrupciones, fallos o ataques que puedan afectar su funcionamiento normal. Para garantizar la disponibilidad, se utilizan técnicas como la **redundancia, la copia de seguridad y la planificación de la continuidad del negocio**.

Ejemplo: Un hospital implementa un sistema de redundancia para sus servidores de datos médicos. Esto incluye **servidores de respaldo y almacenamiento en la nube** para garantizar que los registros médicos electrónicos estén siempre accesibles, incluso en caso de fallo del servidor principal. Además, el hospital tiene un plan de recuperación ante desastres que incluye procedimientos para **restaurar rápidamente los sistemas y datos críticos** en caso de interrupciones causadas por desastres naturales o ciberataques. Regularmente, realizan pruebas de estos planes para asegurarse de que estos pueden ser ejecutados eficazmente cuando sea necesario.

En resumen, la triada de la seguridad de la información establece los principios fundamentales que deben ser considerados para proteger la información de una organización de manera efectiva, asegurando su confidencialidad, integridad y disponibilidad.

Los beneficios de aplicar la seguridad de la información son numerosos. Estos son algunos:

- Protege la información sensible de la empresa y de los clientes, lo que puede evitar pérdidas financieras y daños a la reputación.
- Mejora la confianza de los clientes y socios comerciales, quienes valoran la seguridad de sus datos personales y transaccionales.
- Contribuye a la continuidad del negocio, pues previene interrupciones operativas causadas por ciberataques o fallos en los sistemas.
- Ayuda a las organizaciones a cumplir con las normativas y estándares internacionales, evitando sanciones legales y mejorando su posición competitiva en el mercado.

Diferencias entre seguridad de la información y seguridad informática

A menudo, la diferencia entre seguridad de la información y seguridad informática se vuelve borrosa porque ambas disciplinas están estrechamente relacionadas y comparten objetivos similares. Sin embargo, existen **distinciones importantes entre ellas** en términos de enfoque y alcance. Veamos cuales son.

	Seguridad de la información	Seguridad Informática
Definición	Conjunto de medidas que se centra en la protección de la información en todas sus formas (digital, física, en tránsito, en reposo, etc.) y aborda aspectos como la confidencialidad, integridad y disponibilidad.	Conjunto de medidas que se centra, específicamente, en la protección de los sistemas informáticos, incluyendo hardware, software, redes y datos almacenados en esos sistemas.

Objetivo	Garantizar que la información de una organización esté protegida contra amenazas y riesgos, asegurando su confidencialidad, integridad y disponibilidad.	Proteger los sistemas informáticos contra amenazas como virus, malware, intrusiones, fallos de hardware/software, entre otros, asegurando su disponibilidad, integridad y confidencialidad.
Frameworks y estándares relacionados	• ISO 27001 (Gestión de la Seguridad de la Información) • NIST SP 800-53 (Seguridad y Privacidad en Sistemas de Información) • ISACA COBIT (Marco de Gobierno y Gestión de TI)	• NIST SP 800-171 (Requisitos de Seguridad para Información Controlada No Clasificada) • CIS Controls (Controles de Seguridad Críticos) • PCI DSS (Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago)

En resumen, **mientras que la seguridad de la información se enfoca en proteger la información** en su totalidad y aborda aspectos como políticas, procedimientos y controles para gestionar los riesgos de seguridad de la información, **la seguridad informática se centra más específicamente en la protección de los sistemas informáticos** contra amenazas y riesgos.

Sin embargo, ambas disciplinas son complementarias y trabajan juntas para garantizar la seguridad global de una organización.

Implementación de un Sistema de Gestión de la Seguridad de la Información

La implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI), conforme a la norma ISO 27001, es fundamental para cualquier organización que busque proteger sus datos y garantizar la seguridad de la información.

Norma ISO 27001

La ISO 27001 proporciona un marco sistemático para gestionar la seguridad de la información, abordando aspectos como la confidencialidad, integridad y disponibilidad de los datos. Para cumplir con esta norma, las organizaciones deben seguir una serie de requisitos que incluyen la evaluación y gestión de riesgos, la implementación de controles de seguridad, y la creación de políticas y procedimientos claros.

La norma ISO 27001 establece los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) dentro de una organización.

Estos son los principales requisitos que se deben cumplir para implementar un SGSI según la ISO 27001:

- **Comprensión del contexto de la organización:** La organización debe comprender su contexto externo e interno, así como los requisitos y expectativas de las partes interesadas relevantes.
- **Liderazgo y compromiso de la dirección:** La alta dirección debe demostrar liderazgo y compromiso con respecto a la seguridad de la información, asignando responsabilidades y recursos apropiados para el SGSI.

- **Política de seguridad de la información:** Se debe establecer y mantener una política de seguridad de la información documentada que proporcione un marco general para los objetivos y compromisos de seguridad de la información de la organización.
- **Gestión de riesgos:** La organización debe realizar una evaluación de riesgos para identificar y valorar los riesgos de seguridad de la información, y luego seleccionar e implementar controles de seguridad adecuados para mitigar estos riesgos.
- **Soporte organizacional:** Se deben proporcionar los recursos humanos, técnicos y financieros necesarios para implementar y mantener el SGSI, así como para proporcionar concienciación y formación en seguridad de la información.
- **Operación:** La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información y lograr los objetivos del SGSI.
- **Evaluación del desempeño:** Se deben establecer procesos para monitorear, medir, analizar y evaluar el desempeño del SGSI, incluida la realización de auditorías internas periódicas y la revisión por la dirección.
- **Mejora continua:** La organización debe identificar oportunidades de mejora y tomar acciones para mejorar continuamente la eficacia del SGSI, incluida la respuesta a incidentes de seguridad de la información y la revisión de la política y los objetivos de seguridad de la información**.**

Cumplir con estos requisitos permite a una organización establecer un SGSI sólido y efectivo que proteja la información sensible y garantice la confidencialidad, integridad y disponibilidad de la misma.

CIS Controls

Los CIS Controls (Controles de Seguridad Críticos) son un conjunto de mejores prácticas desarrolladas por el Center for Internet Security (CIS) para ayudar a las organizaciones a mejorar su postura de seguridad cibernética y proteger sus activos de información.

Categorización de los CIS Controls

Los CIS Controls se dividen en tres categorías principales: controles básicos, controles fundacionales y controles organizacionales. Cada categoría está diseñada para abordar diferentes aspectos de la seguridad y mejorar gradualmente la postura de seguridad global de la organización.

a) Controles básicos

Los controles básicos son los primeros que todas las organizaciones deben implementar para establecer una base sólida de seguridad. Estos controles se centran en aspectos esenciales que cualquier organización, independientemente de su tamaño o industria, debe abordar para protegerse contra amenazas comunes. Incluyen:

- **Inventario y control de activos de hardware:** Mantener un inventario actualizado y preciso de todos los dispositivos de hardware dentro de la red de la organización.
- **Inventario y control de activos de software:** Gestionar y rastrear todas las aplicaciones y programas instalados en los dispositivos de la organización.
- **Gestión continua de vulnerabilidades:** Implementar procesos para identificar, evaluar y remediar vulnerabilidades en sistemas y aplicaciones.

- **Uso controlado de privilegios administrativos:** Asegurar que los privilegios administrativos se gestionen y controlen adecuadamente para minimizar el riesgo de abuso.

b) Controles fundacionales

Los controles fundacionales construyen sobre la base establecida por los controles básicos y abordan áreas más específicas y técnicas de la seguridad cibernética. Estos controles son fundamentales para la protección de la infraestructura de TI y la gestión de la seguridad operativa. Incluyen:

- **Configuración segura de dispositivos de hardware y software:** Establecer y mantener configuraciones seguras para todos los dispositivos y software dentro de la organización.

- **Mantenimiento, monitoreo y análisis de registros de auditoría:** Recopilar, gestionar y analizar registros de auditoría para detectar y responder a incidentes de seguridad.

- **Protección de datos:** Implementar medidas para proteger los datos en reposo y en tránsito, incluyendo el cifrado y la gestión de claves.

- **Defensa contra malware:** Utilizar software antivirus y otras herramientas para detectar y prevenir infecciones de malware.

c) Controles organizacionales

Los controles organizacionales se centran en las políticas, procedimientos y la gestión de la seguridad dentro de la organización. Estos controles aseguran que la seguridad cibernética esté integrada en la cultura organizacional y que todos los empleados comprendan su papel en la protección de la información. Incluyen:

- **Desarrollo y mantenimiento de políticas de seguridad:** Crear y mantener políticas claras y comprensibles que guíen las acciones de seguridad en la organización.

- **Gestión de la seguridad de proveedores:** Evaluar y gestionar los riesgos asociados con los proveedores y socios externos.
- **Formación y concienciación de los usuarios:** Implementar programas de formación y concienciación para educar a los empleados sobre las prácticas de seguridad y las amenazas cibernéticas.
- **Planificación y ejecución de respuestas a incidentes:** Desarrollar y mantener planes de respuesta a incidentes para gestionar y mitigar los impactos de los incidentes de seguridad.

La categorización de los CIS Controls permite a las organizaciones implementar un enfoque escalonado y estratégico hacia la seguridad cibernética.

Veamos algunos controles relevantes de acuerdo con una problemática específica:
Problemática: Amenazas persistentes avanzadas (APT) que buscan infiltrarse en la red y robar datos sensibles.

Controles de seguridad seleccionados:

- **Control CIS 1: Control de Inventario de Activos de Hardware y Software**

  Este control implica mantener un inventario de todos los dispositivos de hardware y software en la red, lo que ayuda a identificar y gestionar activos de manera más efectiva. Esto puede ayudar a detectar dispositivos no autorizados que podrían ser utilizados por un atacante.

- **Control CIS 3: Control de Actualizaciones de Software y Configuración Segura**

  Mantener el software actualizado y configurado de manera segura es fundamental para mitigar las vulnerabilidades que podrían ser explotadas por los atacantes. Este control implica aplicar parches de seguridad y configurar el software de acuerdo con las mejores prácticas de seguridad.

- **Control CIS 5: Control de Acceso y Control de Cuentas de Usuario**

Limitar el acceso a sistemas y datos sensibles es crucial para prevenir intrusiones no autorizadas. Este control implica implementar políticas de control de acceso, autenticación de múltiples factores y monitoreo de actividad de usuario para detectar comportamientos anómalos.

- **Control CIS 9: Control de Restricción de Dispositivos Portátiles y Movilidad**

Los dispositivos portátiles y móviles pueden representar una amenaza para la seguridad si no se gestionan adecuadamente. Este control implica establecer políticas y controles para restringir y proteger el uso de dispositivos móviles dentro de la red corporativa.

- **Control CIS 18: Control de Respuesta y Recuperación Ante Incidentes de Seguridad**

Es importante tener un plan de respuesta ante incidentes para poder detectar, contener y recuperarse de una intrusión exitosa. Este control implica establecer procesos y procedimientos para la gestión eficaz de incidentes de seguridad, incluida la notificación de incidentes y la restauración de sistemas afectados.

Estos controles proporcionan una base sólida para abordar la problemática de las amenazas persistentes avanzadas, ayudando a **mitigar los riesgos y proteger los activos de información** de la organización.

En síntesis, la triada de la seguridad de la información, compuesta por la confidencialidad, integridad y disponibilidad, es esencial para la protección y el manejo adecuado de los datos en cualquier organización. Estos tres principios trabajan en conjunto para asegurar que la información esté protegida contra accesos no autorizados, se mantenga precisa y sin alteraciones indebidas, y esté disponible para los usuarios cuando la necesiten. Comprender y aplicar adecuadamente la triada de la seguridad de la información es crucial para el éxito y la sostenibilidad de cualquier empresa en el entorno digital actual.

Por otro lado, la ISO 27001 establece los requisitos fundamentales para gestionar el Sistema de Gestión de la Seguridad de la Información (SGSI), mientras que los CIS Controls ofrecen directrices específicas y prácticas para abordar las amenazas cibernéticas más críticas. Al integrar estos dos enfoques, las organizaciones no solo fortalecen su postura de seguridad, sino que también aseguran la continuidad del negocio, cumplen con las normativas legales y ganan la confianza de sus clientes y socios.

Referencias bibliográficas

Instituto Nacional de Ciberseguridad (INCIBE). (n.d.). *Fundamentos de la seguridad de la información*. https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

Instituto Nacional de Estándares y Tecnología (NIST). (2021). *Guía de fundamentos para la seguridad de la información*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Organización de los Estados Americanos (OEA). (n.d.). *Guía de fundamentos de la seguridad de la información*. https://www.oas.org/ext/es/seguridad/prog-ciber