Ciberseguridad vs Seguridad de la Información

Ciberseguridad

La Ciberseguridad se enfoca específicamente en la **protección de sistemas, redes y programas informáticos contra amenazas digitales**. Su alcance abarca la **prevención, detección y respuesta a ataques cibernéticos** que buscan comprometer la confidencialidad, integridad y disponibilidad de los recursos digitales. Esto incluye la protección contra *malware*, *phishing*, ataques de denegación de servicio (DDoS), y otras tácticas empleadas por actores malintencionados.

Las estrategias de Ciberseguridad a menudo involucran la **implementación de tecnologías avanzadas**, como *firewalls*, sistemas de prevención de intrusiones, cifrado, análisis forense digital y la gestión proactiva de vulnerabilidades. Además, implica la formación y concienciación de los usuarios para fortalecer la **primera línea de defensa** contra amenazas cibernéticas.

Seguridad de la información

Tiene un **enfoque más amplio e integral**. Se ocupa de **salvaguardar la información en todas sus formas**, ya sea impresa, electrónica o verbal, y no se limita únicamente a la esfera digital. La seguridad de la información incorpora **principios como *confidencialidad, integridad, disponibilidad, autenticidad* y *no repudiación*** para garantizar un manejo seguro y ético de la información.

La seguridad de la información **abarca aspectos más allá de las amenazas digitales**, como la gestión de documentos físicos, la formulación de políticas de acceso, la educación de los empleados sobre prácticas seguras y la implementación de controles físicos. Incluye la identificación y protección de activos de información críticos, así como la gestión de riesgos en el contexto de toda la organización.

Introducción a la ciberseguridad

La Ciberseguridad engloba prácticas, estrategias y tecnologías diseñadas para salvaguardar la integridad, confidencialidad y disponibilidad de sistemas, redes y datos en el entorno digital.

Esto implica la implementación de medidas preventivas y correctivas para contrarrestar las amenazas cibernéticas en constante evolución.

La ciberseguridad es como el guardián de nuestro mundo digital. En un momento en el que todo, desde nuestras conversaciones hasta nuestras compras, ocurre en línea, proteger esa información se vuelve fundamental.

Imagina que alguien puede acceder a tus fotos, mensajes o incluso a tu cuenta bancaria sin permiso. Eso podría causar grandes problemas, ¿verdad? La Ciberseguridad evita que eso suceda. Protege nuestra información personal y financiera de personas que intentan robarla o usarla de manera incorrecta.

Pero no se trata solo de nosotros. También afecta a las empresas y al país en general. Si las empresas no están seguras, podrían perder mucho dinero, y si un país es atacado digitalmente, podría tener problemas graves.

Entonces, la Ciberseguridad no es solo una cosa técnica. Es como un superhéroe que nos protege a todos en el mundo digital, asegurándose de que podamos disfrutar de la tecnología sin preocuparnos de que alguien quiera hacer daño. Esencialmente, es la defensa que nos permite usar Internet y la tecnología de manera segura.

Principios fundamentales: tríada CIA

En la Ciberseguridad, hay reglas importantes que actúan como los superpoderes que mantienen a salvo nuestra información. Son como los cimientos de un edificio fuerte.

Confidencialidad	Integridad	Disponibilidad
Este principio trata de **mantener secretos**. Imagina que tus secretos digitales, como contraseñas o mensajes, son como tesoros. La confidencialidad **asegura que solo tú y las personas autorizadas puedan acceder a esos tesoros**, protegiéndolos de miradas indiscretas.	La integridad es como el **guardián de la verdad, asegura que la información no sea alterada o cambiada sin permiso**. Si envías un mensaje, la integridad se asegura de que llegue tal como lo enviaste, sin cambios no deseados.	Piensa en la disponibilidad como tener acceso a tus cosas cuando las necesitas. **Garantiza que la información esté disponible y accesible cuando la requieres**, evitando que alguien la bloquee o te impida llegar a ella.

Importancia de la Tríada

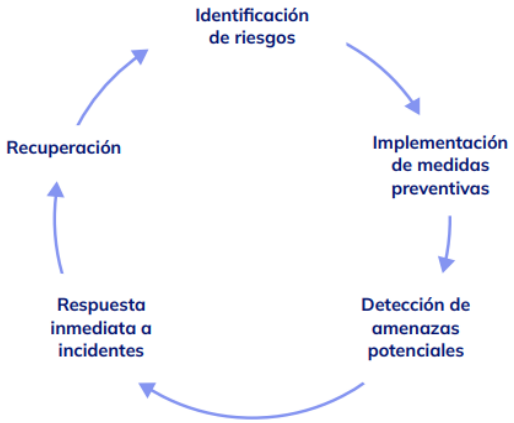
- Protege los activos de información: la información es un activo valioso para cualquier organización, y la Tríada CIA ayuda a protegerla de amenazas como el robo, la corrupción y la pérdida.
- Mantiene la confianza: los usuarios necesitan confiar en que la información que utilizan es precisa y confiable. La Tríada CIA ayuda a construir esta confianza.
- Cumple con las regulaciones: muchas organizaciones están sujetas a regulaciones que exigen la protección de la información. La Tríada CIA ayuda a las organizaciones a cumplir con estas regulaciones.

Ejemplo de cómo se aplica la tríada CIA

- Uso de contraseñas: las contraseñas ayudan a garantizar la confidencialidad de la información al restringir el acceso a los sistemas y datos.
- Respaldos de datos: los respaldos de datos ayudan a garantizar la integridad de la información al proporcionar una copia en caso de que la información original se corrompa o se pierda.

- Planes de recuperación de desastres: los planes de recuperación de desastres ayudan a garantizar la disponibilidad de la información al proporcionar un plan para restaurar los sistemas y datos en caso de un desastre.

Ciclo de vida de la ciberseguridad



La ciberseguridad tiene un plan de acción como un superhéroe tiene un plan para resolver el dia.
Este plan se llama el ciclo de vida de la ciberseguridad:

Herramientas y tecnologías

En el ámbito de la Ciberseguridad, se emplean diversas herramientas y tecnologías para fortalecer las defensas contra amenazas digitales. Estos recursos varían en complejidad y propósito, abarcan desde medidas básicas hasta soluciones altamente especializadas. Veamos el detalle de cada uno, a continuación.

- *Firewalls.*
- Antivirus.
- Sistemas de Prevención de Intrusiones (IPS).
- Análisis forense digital.
- Sistemas de Detección de Amenazas (TDS).
- Cifrado de datos.
- Autenticación Multifactor (MFA).
- Gestión de vulnerabilidades.

- *Firewalls*: Actúan como una barrera protectora entre una red privada y el tráfico no autorizado de Internet. Monitorean y controlan el tráfico basándose en un conjunto de reglas predefinidas.

- *Antivirus*: Identifican y eliminan software malicioso, como virus y malware, que pueda comprometer la integridad de sistemas y datos.
- *Sistemas de Prevención de Intrusiones (IPS)*:Detectan y previenen intrusiones en tiempo real, analizando patrones de tráfico y bloqueando actividades maliciosas.
- *Análisis forense digital*: Se utiliza para investigar y analizar incidentes de seguridad. Permite rastrear el origen y el impacto de un incidente, esto facilita la respuesta y la mejora continua de las medidas de seguridad.
- *Sistemas de Detección de Amenazas (TDS)*: Monitorean continuamente la red en busca de patrones anómalos que puedan indicar actividad maliciosa. Ayudan a identificar amenazas antes de que causen daño significativo.
- *Cifrado de datos*: Garantiza la confidencialidad de la información mediante la codificación de datos, de modo que sólo aquellos con las claves adecuadas puedan acceder a ellos.
- *Autenticación Multifactor (MFA)*: Refuerza la seguridad del acceso al requerir múltiples formas de verificación antes de permitir la entrada, como contraseñas y códigos generados.
- *Gestión de vulnerabilidades*: Identifica, evalúa y mitiga vulnerabilidades en sistemas y aplicaciones, para prevenir posibles explotaciones por parte de atacantes.

Áreas de Seguridad Informática

El esquema muestra algunos de los principios de la Seguridad informática, desde la gestión de riesgos hasta el desarrollo de software. Cada componente es clave y fortalece la seguridad en entornos digitales.