En la actualidad es común encontrar noticias o artículos referentes a la seguridad cibernética, aunque también se puede ver o escuchar el término seguridad informática. Aunque ambos términos parecen similares, no significan lo mismo.

Seguridad informática

La seguridad informática es un conjunto de prácticas, políticas, procedimientos y tecnologías diseñadas para proteger los sistemas informáticos, la información, los programas y los datos contra accesos no autorizados, daños, robo, interrupciones y cualquier otra amenaza que pueda comprometer la confidencialidad, integridad y disponibilidad de la información. El objetivo principal de la seguridad informática es garantizar que los recursos informáticos se utilicen de manera segura y que la información sensible esté protegida contra pérdidas o accesos no autorizados.

Algunos de los elementos clave de la seguridad informática incluyen:

1. Gestión de Accesos: Controlar quién tiene acceso a qué recursos y garantizar que solo las personas autorizadas puedan acceder a información sensible.
2. Cifrado de Datos: Proteger la información mediante la codificación de los datos para que solo las personas autorizadas puedan entenderlos, incluso si los datos se interceptan.
3. Protección contra Malware: Implementar medidas para prevenir, detectar y eliminar software malicioso como virus, gusanos, troyanos, ransomware, entre otros.
4. Firewalls: Utilizar firewalls para controlar el tráfico de red y prevenir accesos no autorizados.
5. Actualizaciones y Parches: Mantener actualizado el software y aplicar parches de seguridad para corregir vulnerabilidades conocidas.
6. Políticas de Seguridad: Establecer políticas y procedimientos claros sobre el uso seguro de los sistemas informáticos, incluyendo la gestión de contraseñas, la navegación web y el uso de dispositivos extraíbles.
7. Monitoreo y Detección de Intrusiones: Implementar sistemas de monitoreo para detectar actividades sospechosas y responder rápidamente a posibles intrusiones.

8. Educación y Concientización: Capacitar a los usuarios sobre las mejores prácticas de seguridad informática y concientizarlos sobre los riesgos asociados con el manejo de la información.

La seguridad informática es esencial en el mundo actual, donde la dependencia de la tecnología y la conectividad a Internet es generalizada. Las amenazas a la seguridad informática pueden provenir de diversas fuentes, incluyendo hackers, ciberdelincuentes, empleados malintencionados o simplemente errores humanos. Por lo tanto, las organizaciones y los individuos deben tomar medidas proactivas para proteger sus sistemas y datos.

Seguridad cibernética

La seguridad cibernética, también conocida como ciberseguridad, se refiere a las prácticas, procesos y tecnologías diseñadas para proteger sistemas informáticos, redes y datos contra amenazas cibernéticas. La seguridad cibernética se centra específicamente en el entorno digital, abordando riesgos y ataques que tienen lugar en el ciberespacio.

Algunos de los aspectos clave de la seguridad cibernética incluyen:

1. Protección contra Amenazas Cibernéticas: Incluye la prevención, detección y respuesta a una amplia variedad de amenazas en línea, como ataques de malware, phishing, ataques de denegación de servicio (DDoS), intrusiones, entre otros.
2. Seguridad de Red: Implementa medidas para proteger la integridad y la confidencialidad de las comunicaciones en redes, incluyendo la configuración de firewalls, detección de intrusiones y cifrado de datos.
3. Gestión de Identidad y Acceso: Se ocupa de asegurar que solo las personas autorizadas tengan acceso a sistemas y datos, utilizando métodos como la autenticación multifactor y la gestión de accesos.
4. Cifrado de Datos: Aplica técnicas de cifrado para proteger la confidencialidad de la información, tanto en reposo como en tránsito.
5. Gestión de Vulnerabilidades: Identifica y aborda las vulnerabilidades en sistemas y

aplicaciones para prevenir posibles puntos de entrada para los ciberatacantes.
6. Concientización y Capacitación: Educa a los usuarios y profesionales en temas de seguridad cibernética para que estén conscientes de las amenazas y adopten prácticas seguras.
7. Respuesta a Incidentes: Desarrolla planes y procedimientos para responder eficientemente a incidentes de seguridad, minimizando el impacto y restaurando la normalidad lo antes posible.
8. Auditoría y Monitoreo Continuo: Realiza auditorías regulares y monitoreo constante de los sistemas para detectar y mitigar posibles amenazas en tiempo real.

La seguridad cibernética es esencial en un mundo cada vez más conectado, donde las amenazas cibernéticas pueden provenir de actores maliciosos con diversas intenciones, desde el robo de información hasta el sabotaje de infraestructuras críticas. Las organizaciones y los individuos deben implementar medidas de seguridad cibernética para protegerse contra estas amenazas y garantizar la integridad, confidencialidad y disponibilidad de la información digital.

Por lo tanto, conociendo ambos conceptos, resulta más sencillo diferenciarlos entre sí, pero por si aún tienes dudas, aquí hay algunas diferencias entre la seguridad informática y la ciberseguridad.

Diferencias entre seguridad cibernética y seguridad informática

La seguridad informática y la seguridad cibernética son términos que a menudo se utilizan de manera intercambiable, pero pueden tener enfoques ligeramente diferentes. Aunque no hay una distinción universalmente aceptada, se pueden hacer algunas generalizaciones sobre las diferencias:

1. Alcance:

- Seguridad Informática: Tradicionalmente, este término ha abordado la protección de la información en general, incluyendo la seguridad de los datos, la gestión de accesos, la protección contra malware y otras amenazas. Puede referirse a la seguridad en sistemas locales y redes.
- Seguridad Cibernética: Se centra específicamente en la seguridad de los sistemas conectados a Internet y en la protección contra amenazas cibernéticas. A menudo se utiliza para describir un enfoque más amplio que incluye la seguridad informática pero también se enfoca en la protección contra ataques cibernéticos, hacking, y otras amenazas en línea.

1. Enfoque:

- Seguridad Informática: Puede incluir aspectos más amplios de la gestión de la información y la protección de los sistemas de información, independientemente de si están conectados a Internet o no.
- Seguridad Cibernética: Tiende a concentrarse específicamente en la seguridad en el espacio cibernético, donde las amenazas suelen ser más dinámicas y pueden provenir de fuentes externas a la organización.

1. Evolución del término:

- Seguridad Informática: Ha sido utilizado desde antes de la proliferación de Internet y se ha centrado en la seguridad de los sistemas de información en general.
- Seguridad Cibernética: Surgió en respuesta a la creciente importancia de la seguridad en línea y se ha convertido en un término más específico y enfocado en la seguridad en el ciberespacio.

En la práctica, los términos a menudo se utilizan de manera intercambiable y la distinción puede variar según el contexto y la interpretación de las organizaciones y profesionales de seguridad. Ambos campos comparten el objetivo común de proteger la información y los sistemas, ya sea en el ámbito físico o en el ciberespacio.