Conceptos básicos de ciberseguridad

La ciberseguridad es el conjunto de técnicas y herramientas utilizadas para proteger los sistemas informáticos, las redes y los datos contra amenazas digitales. Es fundamental comprender estos conceptos básicos para mantener a salvo nuestra información y nuestra privacidad en el mundo digital.

PH by Pablo Horcajuelo

Made with Gamma

Amenazas cibernéticas comunes

1 Malware

Software malicioso como virus, troyanos y ransomware que pueden dañar o robar datos.

2 Phishing

Intentos de engaño para obtener información confidencial a través de correos electrónicos o sitios web falsos.

3 Ataques de denegación de servicio

Abrumamiento de sistemas para bloquear el acceso legítimo a recursos en línea.

4 Robo de identidad

Uso no autorizado de datos personales para cometer fraude o acceder a cuentas.

Made with Gamma

Principios de la ciberseguridad

Confidencialidad

Garantizar que la información solo esté disponible para aquellos autorizados a acceder a ella.

Integridad

Asegurar que los datos no sean alterados o modificados de manera no autorizada.

Disponibilidad

Velar por que los sistemas y recursos informáticos estén accesibles cuando se los necesite.

Made with Gamma

Protección de datos y privacidad

1

Cifrado

Convertir la información en un formato ilegible para que solo los autorizados puedan acceder a ella.

2

Backups

Realizar copias de seguridad regulares de los datos importantes para evitar su pérdida.

3

Gestión de permisos

Establecer y controlar quién tiene acceso a qué información y funciones.

Made with Gamma

Seguridad de redes y dispositivos

Firewalls

Filtran y controlan el tráfico de red para detectar y bloquear actividades sospechosas.

Actualizaciones

Mantener los sistemas operativos, aplicaciones y dispositivos actualizados para corregir vulnerabilidades.

Segmentación de red

Dividir la red en segmentos más pequeños y controlados para limitar los daños en caso de un ataque.

Detección de intrusos

Monitorear la actividad de la red y los dispositivos para identificar y responder a amenazas.

Made with Gamma

Gestión de contraseñas y autenticación

Contraseñas seguras

Utilizar contraseñas largas, complejas y únicas para cada cuenta.

Autenticación biométrica

Utilizar características físicas, como huellas digitales o reconocimiento facial, para verificar la identidad.

Autenticación de dos factores

Requerir dos métodos de verificación, como contraseña y código SMS, para acceder a cuentas.

Gestores de contraseñas

Herramientas que almacenan de forma segura múltiples contraseñas y las rellenan automáticamente.

Made with Gamma

Respuesta a incidentes de seguridad

1

Detección

Identificar y reconocer que se ha producido un incidente de seguridad.

2

Contención

Tomar medidas rápidas para limitar el daño y evitar que el incidente se propague.

3

Investigación

Analizar el incidente para determinar el alcance, la causa y el impacto.

4

Recuperación

Restaurar los sistemas y datos afectados y fortalecer la seguridad para prevenir futuros incidentes.

Made with Gamma

Buenas prácticas y recomendaciones

Concientización y capacitación	Educar a los usuarios sobre amenazas y mejores prácticas de seguridad.
Copias de seguridad regulares	Realizar respaldos periódicos de datos críticos para prevenir su pérdida.
Monitoreo y registro de actividad	Vigilar y registrar los eventos de seguridad para detectar y responder a incidentes.
Planificación de contingencia	Tener un plan de acción y de recuperación ante posibles incidentes de seguridad.

Made with Gamma