

Asegurando la Red Doméstica

Los principales objetivos de asegurar la red doméstica:

- 1) Prevenir que usuarios no autorizados se unan a la red.
- 2) Prevenir que otros vean el tráfico de la red.

Pasos para asegurar la red

Contraseña	Cambia la contraseña predeterminada por una fuerte para Wi-Fi única y compleja.
Habilitar cifrado	Usa WPA3 o WPA2 para una Wi-Fi segura.
Actualizar el firmware	Actualiza regularmente el firmware de tu router para parches de seguridad.
Usar hardware más nuevo	Actualiza a un router/módem moderno para mejorar la seguridad y el rendimiento.
Crear una red de invitados	Aísla a los usuarios invitados para evitar el acceso a tu red principal.
Asegurar dispositivos IoT	Usa contraseñas fuertes y únicas, y actualiza el firmware regularmente.
Habilitar cortafuegos (Firewall)	Configura el cortafuegos de tu router para bloquear el tráfico no deseado.

Concienciación sobre ciberseguridad

Todos debemos aprender sobre ciberseguridad para protegernos a nosotros mismos y a nuestras organizaciones. La educación continua sobre amenazas cibernéticas, riesgos y mejores prácticas es esencial.

Todos tenemos la responsabilidad de aprender sobre las amenazas emergentes. Al hacerlo, podemos:

- 1) Prevenir incidentes de manera proactiva
- 2) Identificar vulnerabilidades en los sistemas
- 3) Adaptar la capacitación, los planes y las políticas según sea necesario

Detección y respuesta ante incidentes

En el contexto de la ciberseguridad, un incidente es un evento anómalo que podría afectar las operaciones normales de una organización o agencia.

Firewall (Cortafuegos)

Los cortafuegos (Firewall) son barreras entre redes confiables y redes no confiables.

Reglas del cortafuegos:

- 1) Denegar tráfico de ciertas direcciones de red o regiones geográficas.
- 2) Denegar servicios, puertos y aplicaciones.
- 3) Permitir tráfico de redes confiables.

Copia de seguridad de datos

La copia de seguridad de datos implica crear copias de datos digitales y almacenarlas en un sistema o ubicación diferente.

Estrategias de copia de seguridad de datos

Copia de seguridad incremental	Solo se respaldan los datos nuevos o modificados, lo que ahorra tiempo y espacio en disco. Garantiza que siempre tengas la versión más reciente de tus datos.
Copia de seguridad completa	Copia todos los datos y permite restaurar diferentes versiones según sea necesario en la ubicación de respaldo. Puede consumir almacenamiento rápidamente si no se eliminan las copias antiguas.

Proveedor de la nube para copia de datos

Recomendaciones al utilizar un proveedor de la nube para copias de seguridad:

- 1) Usar una contraseña fuerte – Protege el acceso a la nube con una contraseña única y compleja.
- 2) Limitar el acceso – Restringe el uso compartido de datos solo a usuarios autorizados.
- 3) Cifrar antes de cargar – Si es posible, cifra los datos para una mayor seguridad.
- 4) Monitorear el uso – Realiza un seguimiento de la actividad en la nube para detectar accesos no autorizados.

Anomalías o comportamientos extraños

Tráfico de direcciones de red desconocidas	Intentos fallidos de inicio de sesión múltiples
Uso aumentado del ancho de banda de la red	Correos electrónicos y llamadas telefónicas sospechosas
Áreas seguras desbloqueadas	Archivos eliminados o alterados
Actividades inusuales fuera del horario laboral	Nuevos usuarios y dispositivos en la red

