Seguridad en la red usuario Externo

Con los avances en Internet y los desarrollos de la informática y las telecomunicaciones, la Seguridad Informática, se ha convertido en figura necesaria para la protección, mantenimiento, control de acceso, confidencialidad, integridad y disponibilidad de la información, tanto para su seguridad como para la seguridad en el soporte de las operaciones de las organizaciones. Las Políticas de Seguridad Informática son las directrices de índole técnica y de organización que se llevan adelante respecto de un determinado sistema de computación a fin de proteger y resguardar su funcionamiento y la información en él contenida. El principio y final de toda red es el usuario, esto hace que las políticas de seguridad deban, principalmente, enfocarse a los usuarios, indican a las personas cómo actuar frente a los recursos informáticos de la Entidad.

¿En qué consiste la seguridad en Internet?

La seguridad en Internet comprende el conjunto de medidas destinadas a proteger la infraestructura tecnológica y la información que circula por la red, la cual suele ser el principal objetivo de actores maliciosos.

La seguridad informática, por su parte, desarrolla procedimientos, normas y mecanismos que permiten identificar y mitigar vulnerabilidades tanto en los datos como en los equipos —por ejemplo, computadores o servidores—.

El uso de soluciones antivirus confiables continúa siendo uno de los mecanismos más eficaces para prevenir incidentes.

- Principales riesgos en Internet
- Sustracción de información
- Alteración o pérdida de datos
- Ataques a sistemas o equipos
- Suplantación de identidad
- Comercialización indebida de datos personales
- Fraudes y robo de dinero

Como usuarios, es posible reducir la exposición a estos riesgos adoptando prácticas preventivas: mantener actualizados los antivirus en los dispositivos conectados a Internet, evitar operaciones financieras desde redes públicas o computadores compartidos, y revisar cuidadosamente los archivos adjuntos asociados a correos de origen desconocido antes de abrirlos o descargarlos.

Recomendaciones para fortalecer la seguridad en Windows

Para incrementar la protección en equipos con Windows, es esencial conservar el sistema operativo y los programas actualizados, contar con un antivirus confiable y tener el firewall configurado de manera adecuada. A esto se suman medidas básicas como emplear contraseñas robustas y evitar abrir enlaces o archivos adjuntos sospechosos.

Recomendaciones puntuales:

- Mantener vigente el sistema operativo y las aplicaciones, pues las actualizaciones incluyen parches que corrigen fallos de seguridad.
- Usar un antivirus reconocido, con protección en tiempo real y actualizaciones frecuentes.
- Configurar el firewall para bloquear accesos no autorizados.
- Implementar contraseñas extensas, únicas y difíciles de predecir.
- Evitar abrir adjuntos o enlaces dudosos.
- Deshabilitar el acceso remoto si no es necesario.
- Minimizar efectos visuales que puedan afectar rendimiento y seguridad.
- Descargar únicamente software proveniente de fuentes verificadas.
- Realizar análisis periódicos de malware.
- Consultar las recomendaciones de “Protección de Windows”.

Recomendaciones para mejorar la seguridad en Mac

En los equipos macOS, la seguridad se refuerza mediante contraseñas sólidas, autenticación biométrica, actualizaciones constantes y el uso adecuado de las configuraciones de privacidad. El cifrado con FileVault, los respaldos regulares y la gestión responsable de accesos y permisos también son claves para reducir riesgos.

Guía detallada:

- Establecer contraseñas complejas y distintas para cada cuenta; un gestor de contraseñas puede ser útil.
- Activar Face ID o Touch ID para una autenticación más segura.
- Mantener el sistema y las aplicaciones al día.
- Configurar el firewall y emplear navegación privada cuando sea necesario.
- Proteger la información con FileVault.
- Realizar copias de seguridad frecuentes con Time Machine.
- Ser precavido frente a enlaces o adjuntos no verificados; utilizar antivirus si se considera pertinente.
- Administrar permisos de acceso a cámara, micrófono y localización.

- Activar la función “Buscar mi Mac”.
- Aplicar buenas prácticas en el uso del correo electrónico.
- Controlar el uso del dispositivo por parte de menores con las opciones de tiempo en pantalla.
- Evitar inicios de sesión automáticos.
- Limitar la instalación de aplicaciones a la App Store o a desarrolladores autorizados.
- Confirmar la legitimidad de las fuentes antes de instalar actualizaciones.
- Adoptar medidas de seguridad para servicios en la nube, incluidas contraseñas fuertes y controles adicionales de acceso.