



30
NOVIEMBRE

DÍA INTERNACIONAL DE LA SEGURIDAD INFORMÁTICA

TECNO CHRONOS UG
EFEMÉRIDES TECNOLÓGICAS



Esta celebración tuvo su origen en 1988, a raíz del primer caso de malware capaz de propagarse en red, conocido como el "Gusano de Morris". Este incidente afectó al 10% de las máquinas conectadas a Internet en aquel entonces, que formaba parte de ARPANET.



La Association for Computing Machinery (ACM) instituyó este día con el objetivo de concienciar a las personas sobre la importancia de la seguridad de la información y la protección de sus datos en el entorno digital.

En la actualidad, gran parte de la información sensible de las empresas se almacena en Internet, especialmente en diversas plataformas en la nube. Los trabajadores desempeñan un papel fundamental en la protección de estos datos, siendo responsables de garantizar su seguridad y evitando compartirlos por medios que puedan comprometer su integridad, por esta razón se debe de concienciar y entrenar al personal.



5 consejos de seguridad digital en Internet

Con el propósito de sumarnos a la celebración, aquí te compartimos 7 consejos básicos que todo usuario de Internet debería cumplir.

1. Gestión de contraseñas: Es fundamental utilizar contraseñas complejas que no estén relacionadas con información personal evidente, como nombres de mascotas o fechas de nacimiento, y evitar palabras comunes. Además, se recomienda emplear diferentes contraseñas para distintas plataformas, limitando su reutilización a unas pocas claves principales.

2. Precaución con el Wi-Fi público: Puede ser útil para actividades simples como consultar información, leer noticias o ver videos, pero debe evitarse para acciones sensibles, como acceder a bancos en línea, redes sociales o correos electrónicos.

3. Mantener el software actualizado: Aunque las actualizaciones pueden parecer tediosas, suelen incluir parches de seguridad que corrigen vulnerabilidades presentes en versiones anteriores y protegen los datos de posibles riesgos.

4. Cuidado con las descargas: Descargar contenido de sitios no confiables o abrir archivos adjuntos de correos desconocidos puede comprometer la seguridad. Es esencial verificar la legitimidad del sitio web o remitente antes de proceder.

5. El teléfono móvil como dispositivo vulnerable: Al igual que un ordenador, el móvil requiere medidas de seguridad, como la instalación de un antivirus y la precaución al instalar y utilizar aplicaciones y acceder a sitios web.

