CIBERSEGURIDAD

PROTEGE TU MUNDO DIGITAL

Tenemos para ti un conjunto de prácticas y procesos diseñados para proteger redes, dispositivos y datos frente a accesos no autorizados, ataques cibernéticos y daños. Con la digitalización de servicios y el uso de dispositivos inteligentes, estar protegidos digitalmente ya no es opcional: es esencial.

PUBLICADO POR SUVALL FOUR

Cada día realizamos múltiples actividades en línea: trabajamos, compramos, compartimos información personal, gestionamos finanzas y nos comunicamos. Esta vida digital, aunque cómoda y eficiente, también nos expone a numerosas amenazas cibernéticas.

¿POR QUÉ ES IMPORTANTE PROTEGERNOS EN EL ENTORNO DIGITAL?

– Protección de la información personal y financiera

Datos como contraseñas, números de tarjetas, historiales médicos o ubicaciones pueden ser robados y utilizados para fraudes, suplantación de identidad o extorsión.

– Prevención de ataques cibernéticos

Desde virus y malware hasta ransomware y phishing, los ataques digitales pueden afectar tanto a usuarios individuales como a empresas, causando desde pérdidas económicas hasta daños reputacionales.

*– **Seguridad para empresas y profesionales***

Las organizaciones almacenan datos sensibles de clientes, empleados y procesos internos. Un ataque cibernético puede paralizar operaciones, generar demandas legales o sanciones por incumplimiento normativo

*– **Uso responsable de la tecnología***

Protegernos digitalmente también implica educarnos como usuarios, sabiendo identificar riesgos, utilizar herramientas seguras y aplicar buenas prácticas en redes sociales, correos electrónicos y dispositivos.

1

UN ANTIVIRUS **ACTUALIZADO**

CIBERSEGURIDAD - POR SUVALL FOUR

TU PRIMERA LÍNEA DE DEFENSA

Tener un antivirus actualizado es esencial para proteger tu equipo frente a virus, malware, spyware y otros ataques informáticos. No basta con instalar uno y olvidarse: las amenazas evolucionan cada día, y solo un antivirus con actualizaciones constantes puede detectar y neutralizar los riesgos más recientes.

- *Un buen antivirus actualizado te ayuda a:*
- *Bloquear sitios web maliciosos.*
- *Detectar archivos sospechosos en tiempo real.*
- *Proteger tus datos personales frente al robo de identidad.*
- *Evitar la instalación de software espía o troyanos.*
- *Garantizar un rendimiento seguro de tu computadora o dispositivo móvil.*

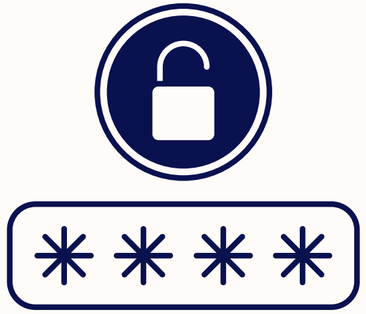
🔁 *Recuerda: mantener tu antivirus actualizado es tan importante como tenerlo instalado. Es una inversión mínima que puede ahorrarte grandes dolores de cabeza.*

Las contraseñas son la llave de entrada a tu vida digital. Si no son lo suficientemente fuertes o se reutilizan en diferentes cuentas, se vuelven un blanco fácil para los ciberdelincuentes. Una contraseña segura debe ser difícil de adivinar, contener una combinación de letras mayúsculas, minúsculas, números y símbolos, y evitar información personal.

¿POR QUÉ NECESITAS CAMBIARLA HABITUALMENTE?

- 🔁 *Reduce el riesgo de accesos no autorizados: Si alguna de tus contraseñas ha sido filtrada sin que lo sepas, cambiarla periódicamente limita el tiempo que un atacante podría tener acceso.*
- 🛡️ *Protege tus cuentas de hackeos silenciosos: A veces los atacantes acceden sin dejar rastro inmediato. Cambiar tus claves regularmente interrumpe este acceso.*
- 🔐 *Mejora tu seguridad general: Es una buena práctica para mantener hábitos digitales responsables, especialmente en cuentas críticas como correo, banca o redes sociales.*

2 LAS CONTRASEÑAS **DEBEN SER SEGURAS**



VAMOS A PONER A PRUEBA
TU CONTRASEÑA

#1
¿incluye letras y números?

#2
¿cuántos caracteres tiene?

#3
¿la actualizas habitualmente?

#4
¿utilizas la misma para todo?

3 TUS DATOS BANCARIOS

ERRORES COMUNES

❌ *Compartir información por mensajes o llamadas.*
Nunca reveles tu número de tarjeta, código de seguridad (CVV) o claves por WhatsApp, email o llamadas no verificadas, incluso si parecen oficiales.

❌ *Usar redes Wi-Fi públicas para transacciones.*
Las conexiones públicas pueden ser interceptadas fácilmente. Evita hacer pagos o ingresar a tu banca online desde cafés, aeropuertos o centros comerciales.

❌ *Usar la misma contraseña para todo.*
Si una sola cuenta se ve comprometida, todas tus finanzas pueden quedar expuestas. Usa contraseñas únicas y seguras para cada acceso.

❌ *No revisar tus movimientos bancarios.*
Muchos fraudes pasan desapercibidos porque no revisamos nuestras cuentas con frecuencia. Revisa tus movimientos bancarios al menos una vez a la semana.

❌ *Hacer clic en enlaces sospechosos*
Los correos falsos que simulan ser del banco son cada vez más sofisticados. No hagas clic en enlaces si no estás 100 % seguro de su origen.

ACIERTOS

✅ *Activar la verificación en dos pasos.*
Siempre que sea posible, activa la autenticación de dos factores (2FA) en tus apps bancarias. Esto añade una capa extra de seguridad al iniciar sesión o hacer transferencias.

✅ *Usar contraseñas fuertes y únicas.*
Crea claves con combinaciones de letras, números y símbolos. Evita repetir contraseñas en distintas plataformas y cámbialas regularmente.

✅ *Revisar tus cuentas con frecuencia.*
Consulta tus movimientos bancarios de forma regular para detectar cualquier operación sospechosa a tiempo.

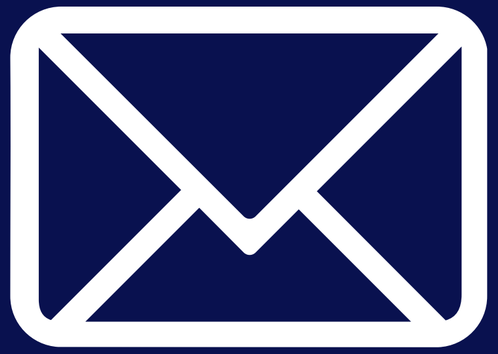
✅ *Conectar solo en redes seguras.*
Realiza operaciones bancarias únicamente desde redes Wi-Fi privadas y seguras. Si estás fuera, usa tu red móvil antes que una Wi-Fi pública.

✅ *Mantener tu dispositivo actualizado.*
Instala las actualizaciones de sistema operativo y antivirus. Las versiones más recientes suelen corregir vulnerabilidades de seguridad.

✅ *Activar alertas del banco.*
Configura notificaciones por correo o mensaje para cada operación. Así sabrás de inmediato si hay alguna transacción no autorizada.

Aunque parezcan mensajes legítimos, los SMS falsos son una de las formas más comunes de fraude digital. Esta técnica se llama smishing (phishing por SMS) y puede poner en riesgo tu información bancaria, contraseñas y hasta tus datos personales.

4 CUIDADO CON LOS SMS



⚠️ ¿Cómo reconocer un SMS peligroso?

- *Te pide que hagas clic en un enlace para "verificar tu cuenta", "actualizar información" o "evitar un bloqueo".*
- *Dice que has ganado un premio o que tienes una entrega pendiente, pero no tiene relación contigo.*
- *Simula ser de tu banco, courier, servicios públicos o plataformas populares (como Amazon o PayPal).*

🚫 Qué NO debes hacer:

- *No hagas clic en ningún enlace sospechoso.*
- *No compartas datos personales, bancarios ni códigos de verificación.*
- *No respondas el mensaje.*

✅ Qué hacer:

- *Borra el SMS sin abrirlo o márcalo como spam.*
- *Verifica la información desde el sitio oficial o la app de la empresa que supuestamente envía el mensaje.*
- *Activa filtros anti-spam y mantén tu dispositivo actualizado.*

PROTEGE TU INFORMACIÓN MIENTRAS NAVEGAS

5 NAVEGACIÓN SEGURA

***Verifica que el sitio tenga HTTPS**: Asegúrate de que la dirección web comience con https:// y que muestre un candado 🔒. Esto indica que la conexión está cifrada.*

***No ingreses datos en sitios sospechosos**: Si una página parece poco profesional, tiene errores de ortografía o pide información sensible sin razón, evita interactuar.*

***Evita hacer clic en anuncios llamativos o emergentes**: Muchos pop-ups y banners pueden contener malware o redirigirte a sitios peligrosos.*

***Mantén tu navegador actualizado:** Las versiones más recientes corrigen vulnerabilidades de seguridad importantes.*

***Usa bloqueadores de rastreo y extensiones confiables:** Herramientas como bloqueadores de anuncios o extensiones de privacidad (como uBlock, Privacy Badger o HTTPS Everywhere) mejoran tu seguridad.*

***Activa el modo de navegación privada cuando sea necesario:** Este modo no guarda tu historial ni cookies, útil si estás en un dispositivo compartido.*

CONSTRUYAMOS JUNTOS UNA CULTURA DIGITAL SEGURA

PREVENCIÓN INDIVIDUAL Y DIARIA, UN PILAR ESENCIAL EN LA CULTURA DIGITAL SEGURA

1

LA CIBERSEGURIDAD ES RESPONSABILIDAD DE TODOS

2

PROTEGER LA INFORMACIÓN DE LA EMPRESA ES ESENCIAL

3