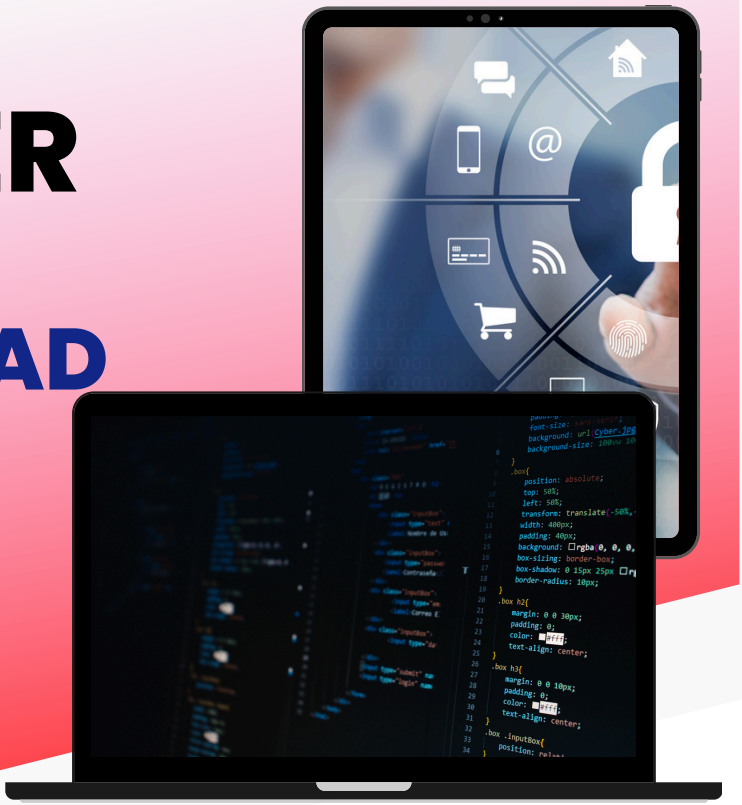
NEWSLETTER

CIBERSEGURIDAD

julio 2024



FRASE DEL MES:

La ciberseguridad es la responsabilidad de todos. Protege tu información, protege tu futuro.

CONSEJOS DE CONCIENTIZACIÓN SOBRE BACKUP:

1. **Actualiza tus Sistemas Regularmente:** Mantén tus sistemas operativos, software y aplicaciones actualizados. Las actualizaciones suelen incluir parches de seguridad esenciales que corrigen vulnerabilidades conocidas y protegen contra amenazas recientes.
2. **Usa Autenticación Multifactor (MFA):** Implementa MFA en todas tus cuentas importantes. Esta capa adicional de seguridad requiere que los usuarios proporcionen dos o más formas de verificación antes de acceder, reduciendo significativamente el riesgo de acceso no autorizado.
3. **Realiza Copias de Seguridad Frecuentes:** Asegúrate de hacer copias de seguridad regulares de tus datos críticos. Almacena estas copias en una ubicación segura y diferente de tus sistemas principales. Esto te permitirá recuperar la información en caso de ataques de ransomware o fallos del sistema.

S&T

SOLUCIONES & TECNOLOGIA S.A.S.

Sus desafios digitales, nuestras soluciones personalizadas

www.solytec.com.co

Especialistas en Ciberprotección

datasafecloud

✓ Guardianes Digitales: Agradecimiento y Consejos en Ciberseguridad

En este mundo cada vez más conectado, la ciberseguridad no es solo una responsabilidad de las grandes empresas, sino de cada uno de nosotros. La protección de nuestra información personal y profesional es fundamental para evitar problemas mayores. A continuación, les comparto algunos consejos esenciales para mantener su seguridad mientras navegan por la web:

1. Protege tus Dispositivos:
Asegúrate de que todos tus dispositivos (computadoras, tablets, smartphones) tengan un software de seguridad actualizado y en funcionamiento. Utiliza antivirus y anti-malware reconocidos y mantenlos actualizados para protegerte contra las amenazas más recientes.

2. Sé Cauto con los Correos Electrónicos:
El phishing sigue siendo una de las técnicas más comunes utilizadas por los ciberdelincuentes. Desconfía de los correos electrónicos no solicitados o sospechosos, especialmente aquellos que contienen enlaces o archivos adjuntos. No hagas clic en enlaces ni descargues archivos de fuentes desconocidas.

3. Crea Contraseñas Fuertes y Únicas:
Las contraseñas son tu primera línea de defensa. Crea contraseñas que sean difíciles de adivinar, utilizando una combinación de letras mayúsculas y minúsculas, números y símbolos. Evita utilizar la misma contraseña para múltiples cuentas y considera el uso de un gestor de contraseñas para mantenerlas seguras.

4. Configura la Autenticación Multifactor (MFA):
Añadir una capa extra de seguridad mediante la MFA es una de las formas más efectivas de proteger tus cuentas. Esta herramienta requiere una segunda forma de verificación además de tu contraseña, como un código enviado a tu teléfono móvil o una aplicación de autenticación.

5. Mantén tu Información Personal Privada:
En las redes sociales y otros sitios web, limita la cantidad de información personal que compartes públicamente. Los delincuentes pueden utilizar estos datos para realizar ataques dirigidos o suplantar tu identidad.

6. Realiza Copias de Seguridad Regulares:
Nunca subestimes la importancia de tener copias de seguridad actualizadas de tus datos más importantes. Utiliza servicios de almacenamiento en la nube o dispositivos externos para asegurar que tus archivos estén protegidos contra pérdidas por fallos del sistema o ataques de ransomware.

7. Mantente Informado:
La ciberseguridad es un campo en constante evolución. Mantente al día con las últimas noticias y tendencias en ciberseguridad. Suscríbete a boletines, sigue blogs especializados (como Guardiandigitals) y participa en webinars para estar siempre informado. https://guardiandigitals.blogspot.com/

8. Utiliza Redes Wi-Fi Seguras:
Evita conectarte a redes Wi-Fi públicas y no seguras, especialmente para realizar transacciones sensibles. Si necesitas utilizar una red pública, considera el uso de una VPN (Red Privada Virtual) para cifrar tu conexión y proteger tus datos.

9. Configura Alertas de Seguridad:
Activa las alertas de seguridad en tus cuentas bancarias y de correo electrónico. Estas alertas te informarán de actividades inusuales o intentos de acceso no autorizados, permitiéndote reaccionar rápidamente ante posibles amenazas.

10. Educación Continua:
La educación en ciberseguridad es esencial. Participa en cursos y talleres para mejorar tus habilidades y conocimientos. Educa también a tus familiares y compañeros de trabajo sobre las mejores prácticas de seguridad en línea.