

Buenas prácticas de **Ciberseguridad** en Entornos educativos



¿Que es la vida digital?

“La **vida digital** es el conjunto de actividades, interacciones y decisiones que realizamos en el entorno virtual, donde cada acción deja un rastro y tiene impacto en nuestra vida real.”



Inclusión digital

La inclusión digital en la educación es garantizar que todos los estudiantes tengan acceso equitativo a las herramientas tecnológicas (computadoras, internet) y las habilidades necesarias para utilizarlas en su aprendizaje, superando barreras socioeconómicas y geográficas

Componentes clave de la inclusión digital en educación:

- ✓ **Acceso a la tecnología**
- ✓ **Alfabetización digital**
- ✓ **Contenido y aplicaciones**
- ✓ **Capacitación y soporte**



¿Cual es la importancia de la **ciberseguridad** en la Educación?

- ❖ La educación en ciberseguridad ayuda a fomentar una cultura de seguridad desde una edad temprana.
- ❖ Los estudiantes y profesores aprenden a valorar y practicar la seguridad digital, lo que contribuye a un entorno más seguro tanto en la escuela como fuera de ella.



“Si vivimos conectados... ¿cómo protegemos esta vida digital?”

AMENAZAS COMUNES



Malware

Software malicioso que puede dañar tu dispositivo, robar información personal o interferir con su funcionamiento.

Los virus, gusanos y troyanos son ejemplos de malware.



Phishing

Intentos de engañar a los usuarios para que revelen información personal confidencial, como contraseñas o datos financieros, mediante correos electrónicos, mensajes de texto o sitios web falsos.



Robo de identidad

El robo de identidad se produce cuando alguien obtiene información personal confidencial y la utiliza para hacerse pasar por ti, acceder a tus cuentas o cometer fraudes en tu nombre.

INTRODUCCION: <https://www.youtube.com/watch?v=eosBzE50H78>

PHISHING – INGENIERIA SOCIAL

La ingeniería social aprovecha la confianza natural del ser humano y sus tendencias psicológicas para conseguir sus objetivos sin recurrir a métodos técnicos complejos.

Revisar

la dirección del remitente: Los correos fraudulentos a menudo utilizan direcciones de correo que imitan a las legítimas, pero con ligeras variaciones.

Fíjate

en el saludo: Los correos electrónicos genuinos suelen usar tu nombre real. Los correos fraudulentos a menudo utilizan saludos genéricos como 'Estimado cliente'.

Analiza

el contenido: Cuidado con los mensajes que generan un sentido de urgencia ('¡Actúa ahora!') o te piden información personal o financiera.

Busca

errores gramaticales y ortográficos: Las empresas legítimas se esfuerzan en mantener un alto nivel de profesionalismo en su comunicación.



Smishing



Phishing por mensajes de texto SMS

QRishing



Phishing mediante códigos QR

Vishing



Voice phishing, o phishing a través de llamadas telefónicas

COMO PREVENIR LOS ATAQUES



MODO **INCÓGNITO**



Evitar las contraseñas de menos de 8 caracteres.

LONGITUD



PERSONAL

Tampoco debemos usar conceptos que se relacionen con nosotros, como: nombres de familiares, cumpleaños, matrícula de nuestro coche...

Intercala mayúsculas, minúsculas, números y caracteres especiales (\$, &, #...).

CARACTERES



VARIEDAD

No usar la misma contraseña en varios servicios. También deben cambiarse periódicamente.

Evita contraseñas fáciles de recordar o de estructura sencilla, como: "12345678" o "qwertyui"

COMPLEJIDAD



GESTOR DE CONTRASEÑAS

Si nos cuesta recordar todas las contraseñas, podemos usar un gestor de contraseñas.



Mantener los equipos informáticos **seguros y actualizados**



Roles y responsabilidades del usuario en ciberseguridad



Proactividad

Los usuarios deben ser proactivos en la protección de su información. Esto significa tomar medidas preventivas para evitar ataques cibernéticos.



Conciencia

Es esencial estar al tanto de las últimas amenazas y estrategias de seguridad. Actualizarse continuamente sobre ciberseguridad.



Cumplimiento

Los usuarios deben seguir las políticas y procedimientos de seguridad establecidos por su organización o institución. Cumplir con las normas.



Participación

Es fundamental informar sobre cualquier actividad sospechosa o incidente. Esto permite a las organizaciones responder de manera efectiva.