# Seguridad y privacidad en línea

## Herramientas para una ciudadanía digital responsable

Una guía para estudiantes y docentes sobre cómo protegerse en el entorno digital y construir una ciudadanía digital responsable.

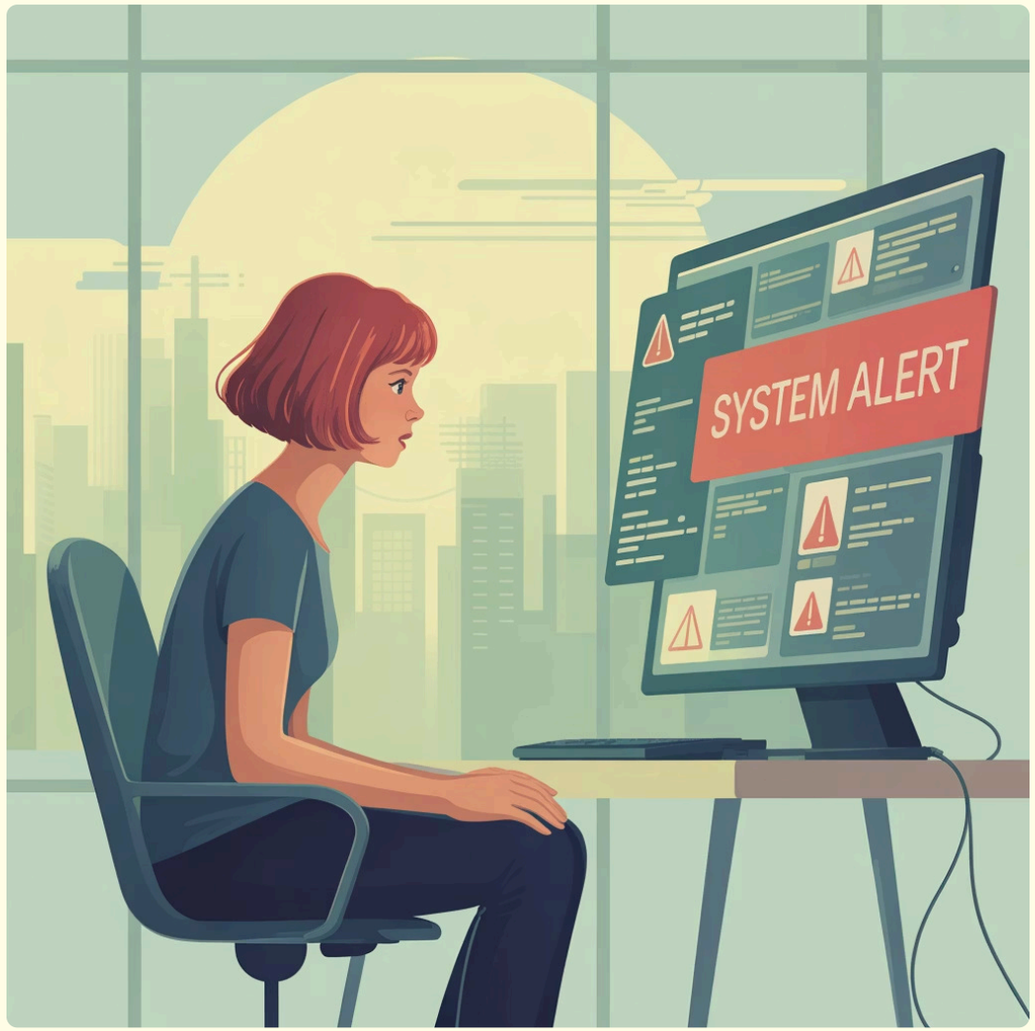
Por Mgtr. Gustavo Palacios

# La seguridad digital: un desafío actual

En la era digital, las herramientas en línea son fundamentales para el aprendizaje y la comunicación. Sin embargo, la información que compartimos puede enfrentar diversos riesgos:

- Robo de identidad
- Acceso no autorizado a cuentas personales
- Exposición de información privada
- Uso indebido de datos personales
- Ciberacoso y amenazas en línea

La seguridad digital no es solo una cuestión técnica, sino una responsabilidad compartida que afecta a toda la comunidad educativa.



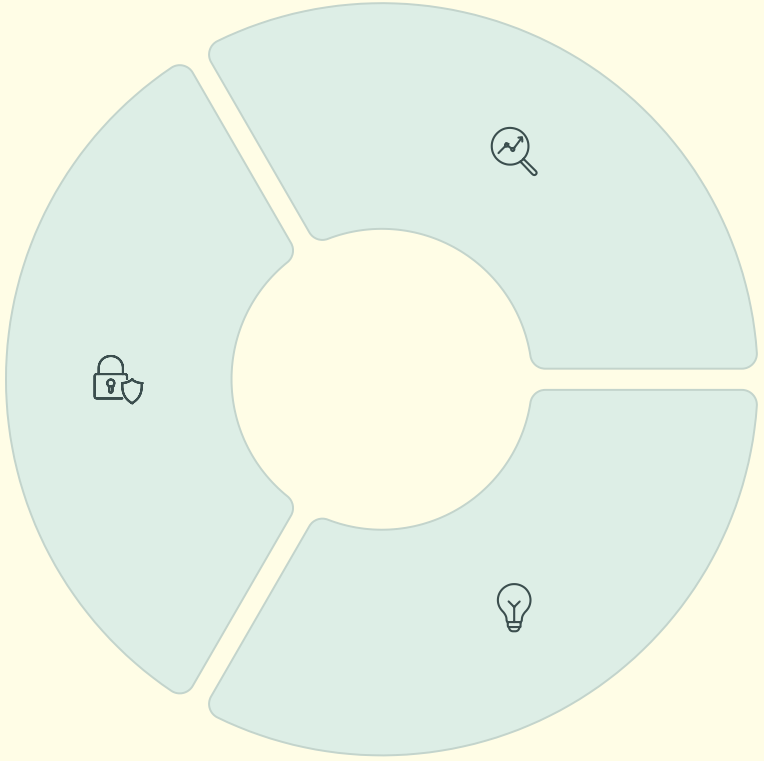

El 67% de los jóvenes ha experimentado algún tipo de problema de seguridad en línea

# Ciudadanía digital: pilares fundamentales

Según la UNESCO, la ciudadanía digital implica el uso crítico, responsable y creativo de las tecnologías digitales para el ejercicio de derechos y deberes en línea.

### Protección

Capacidad para protegerse a uno mismo y a los demás de los riesgos en entornos digitales.



### Análisis crítico

Habilidad para comprender y evaluar de forma crítica el contenido digital y sus fuentes.

### Creatividad

Competencia para crear y compartir contenido digital de manera ética y responsable.

Estas competencias son esenciales para navegar de forma segura en el mundo digital y contribuir positivamente a la sociedad en línea.

# Ciudadanía digital en la práctica

## Redes sociales

Configuración adecuada de privacidad, verificación de fuentes, comportamiento respetuoso, y conciencia sobre el impacto de nuestras publicaciones.

## Reputación en línea

Lo que publicamos construye nuestra identidad digital, que puede ser consultada por futuros empleadores, instituciones educativas o contactos personales.

## Huella digital

Conjunto de rastros que dejamos al navegar: comentarios, "me gusta", búsquedas, compras y registros. Esta información puede persistir durante años.

La ciudadanía digital no es solo teórica, sino que se construye con cada interacción en línea que realizamos.

# Las contraseñas: llaves de nuestra vida digital

Las contraseñas son nuestra primera línea de defensa para proteger:

- Cuentas de correo electrónico
- Redes sociales
- Plataformas educativas
- Servicios bancarios
- Datos personales y académicos

Una contraseña comprometida puede dar acceso a información sensible, permitiendo la suplantación de identidad o el robo de datos.

# Malos hábitos con contraseñas

### Contraseñas demasiado simples

Utilizar combinaciones obvias como "123456", "contraseña" o "qwerty" que pueden ser fácilmente adivinadas.

### Misma clave para todo

Usar la misma contraseña en múltiples servicios, exponiendo todas las cuentas si una es comprometida.

### Datos predecibles

Emplear información personal fácil de averiguar: nombres, fechas de nacimiento o nombres de mascotas.

### Contraseñas sin actualizar

Mantener la misma contraseña durante años sin cambiarla, incrementando el riesgo de exposición.

### Compartir contraseñas

Divulgar nuestras claves con amigos o compañeros, perdiendo el control sobre quién tiene acceso.

# Buenas prácticas con contraseñas

## 1 Combina diversos caracteres

Utiliza mayúsculas, minúsculas, números y símbolos. Ejemplo: "M4rt@.E5tud!a*2023"

## 2 Claves distintas para servicios importantes

Especialmente para correo, banca y redes sociales. Evita que una brecha comprometa todas tus cuentas.

## 3 Usa gestores de contraseñas

Aplicaciones como LastPass, KeePass o Bitwarden que almacenan tus contraseñas de forma segura y cifrada.

## 4 Activa la verificación en dos pasos

Añade una capa extra de seguridad mediante códigos enviados a tu móvil o generados por apps.

Una contraseña segura es tu mejor defensa digital

# Principales riesgos digitales

## Ciberacoso

Hostigamiento sistemático a través de medios digitales. Incluye mensajes amenazantes, difusión de rumores y exclusión deliberada.

**Dato:** Afecta al 30% de estudiantes en España.

## Sexting no consentido

Difusión de imágenes íntimas sin autorización, a menudo tras rupturas o como forma de presión.

**Consecuencias:** Legales, psicológicas y sociales.

## Noticias falsas

Información manipulada que circula rápidamente para desinformar o generar confusión.

**Riesgo:** Toma de decisiones basadas en información errónea.

## Estafas en línea

Intentos de obtener información personal o dinero mediante engaños (phishing, premios falsos, etc.).

**Objetivo:** Robo de identidad o fraude económico.

# Prevención y respuesta

## Consejos de seguridad

- Revisa periódicamente la configuración de privacidad de tus cuentas
- No compartas información personal con desconocidos
- Verifica la procedencia de mensajes y enlaces antes de hacer clic
- Actualiza regularmente tus dispositivos y aplicaciones
- Utiliza redes WiFi seguras o VPN cuando estés fuera de casa
- Guarda evidencias de posibles situaciones de acoso (capturas de pantalla)

## Entidades de apoyo en España

### Policía Nacional

Unidad de Ciberdelincuencia y delitos tecnológicos

### INCIBE

Instituto Nacional de Ciberseguridad

### AEPD

Agencia Española de Protección de Datos

# Una responsabilidad compartida

> **"La seguridad digital no es solo un asunto técnico, sino una competencia esencial para la ciudadanía del siglo XXI"**

## Reflexión final

La educación digital es un pilar fundamental para construir una sociedad en línea segura y responsable. Todos somos agentes de cambio:

- Estudiantes: aplicando buenas prácticas y ayudando a sus compañeros
- Docentes: incorporando la seguridad digital en su práctica educativa
- Familias: acompañando y dialogando sobre hábitos digitales saludables

**El objetivo común:** Formar ciudadanos digitales críticos, responsables y seguros.

# Referencias clase 13


·Bassignana, C. (s.f.). *La ciudadanía digital y las razones para enseñarla*. Universidad San Francisco de Quito. Recuperado de **https://www.usfq.edu.ec**

·Cirion Technologies. (2023). *Ciberseguridad: buenas prácticas para proteger tu vida digital*. Cirion Technologies. Recuperado de **https://www.ciriontechnologies.com**

·Ecuador Verifica. (2021). *¿Qué es la ciudadanía digital según la UNESCO?*. Ecuador Verifica. Recuperado de **https://ecuadorverifica.org**

·Microsoft. (2020). *Esenciales de seguridad digital*. Microsoft. Recuperado de **https://www.microsoft.com**

·Ministerio de Gobierno del Ecuador. (2020). *Guía de seguridad digital para ciudadanos*. Gobierno del Ecuador. Recuperado de **https://www.ministeriodegobierno.gob.ec**

·Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). (2018). *Políticas de ciberseguridad y prevención de ciberdelitos en Ecuador*. Quito: Gobierno del Ecuador.

·Organización de Estados Americanos (OEA). (2019). *Fortalecimiento de la ciberseguridad en América Latina y el Caribe*. OEA. Recuperado de **https://www.oas.org**

·Primicias. (2019, 18 de julio). *Las contraseñas son las llaves de su privacidad: Guía para usarlas mejor*. Primicias. Recuperado de **https://www.primicias.ec**

·Unión Internacional de Telecomunicaciones (UIT). (2017). *Global Cybersecurity Index 2017*. ITU Publications.