

Herramientas Digitales

Seguridad y privacidad en línea

Clase 13



PUCE Virtual - Tecnologías

La excelencia no se improvisa



1. INTRODUCCIÓN

En el mundo actual de las ventas, las herramientas digitales no solo son una ventaja, ¡son esenciales! Ya sea que uses plataformas en la nube para gestionar clientes, almacenar documentos importantes o comunicarte con tu equipo, estas herramientas te abren un universo de posibilidades para ser más eficiente y llegar a más personas. Son el motor que impulsa tu negocio hacia adelante, permitiéndote operar desde cualquier lugar y en cualquier momento, adaptándote a un mercado en constante evolución.

Sin embargo, así como estas herramientas nos brindan grandes oportunidades, también conllevan responsabilidades y ciertos riesgos. La facilidad de acceso y la cantidad de información que manejamos a diario nos exigen ser proactivos en cómo protegemos nuestros datos, los de nuestros clientes y nuestra reputación profesional. Es por eso que, en esta clase, exploraremos los aspectos fundamentales de la seguridad y privacidad en línea, para que puedas navegar en el entorno digital con confianza, responsabilidad y, sobre todo, de manera segura.

2. Clase 13. Seguridad y privacidad en línea

RDA 2: Utiliza herramientas en la nube de comunicación y almacenamiento a través de diferentes plataformas.

2.1 Ciudadanía digital

En un mundo cada vez más conectado, no solo somos ciudadanos de un país, sino también del vasto universo de internet (Figura 1). La ciudadanía digital es una herramienta esencial para la vida. Así como tenemos reglas y principios en el mundo real, necesitamos pautas para funcionar en el entorno digital de manera segura y respetuosa.

Figura 1. Uso de dispositivos en un coworking

Palacios, G. A. (2025). Google ImageFX.



La Unesco (como se menciona en Ecuador Verifica,) define la ciudadanía digital como un conjunto de competencias que te permiten acceder, comprender, analizar, producir y utilizar el entorno digital de forma crítica, ética y creativa. Esto abarca tres dimensiones claves: protección y seguridad; reflexión y análisis; y creatividad y participación.

Título del enlace relacionado: ¿Somos los ecuatorianos ciudadanos digitales?

Descripción breve del enlace relacionado: Ecuador Verifica explica que estar conectado no equivale a ser ciudadano digital

Enlace: <https://ecuadorverifica.org/2022/04/27/somos-los-ecuatorianos-ciudadanos-digitales/>

Como explica Carolina Bassignana (USFQ), la ciudadanía digital te brinda los métodos, reglas y criterios para navegar en internet de forma segura, respetando la propiedad intelectual y protegiéndote a ti y a quienes con los que interactúas. Su propósito es desarrollar una comprensión profunda de lo que implica interactuar en el mundo digital, fomentando la responsabilidad y construyendo un código de honor personal.

¿Alguna vez has visto o compartido algo en línea y luego te has arrepentido? ¿Te has preguntado cómo perciben los demás tu presencia digital? Tu huella digital, esa marca única e indeleble que creamos con cada publicación o interacción, dice mucho de ti y puede incluso revelar más información de la que quisieras (Figura 2). En ventas, tu



reputación en línea es tu tarjeta de presentación. Ser un buen ciudadano digital significa proteger esa reputación y generar confianza.

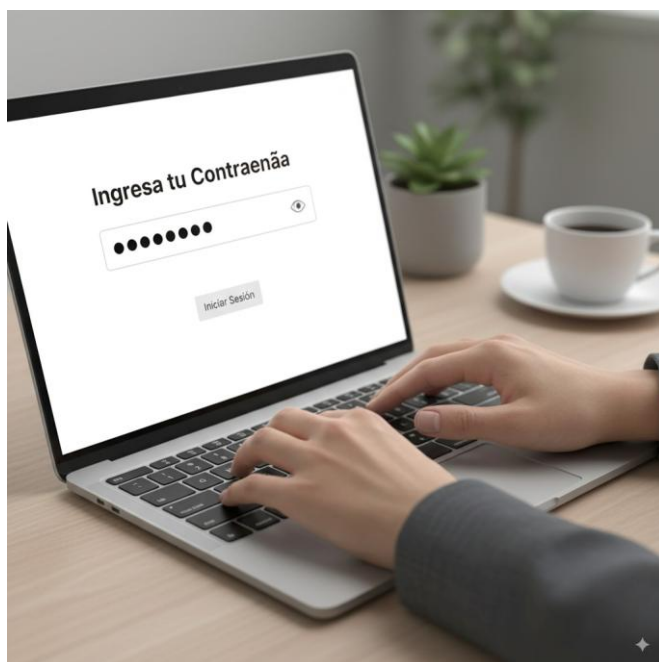
Figura 2 . Uso de redes sociales en una laptop

Palacios, G. A. (2025). Google ImageFX.

Si como profesional de ventas utilizas redes sociales para interactuar con tus clientes, la ciudadanía digital te guía para mantener una comunicación respetuosa, proteger la privacidad de tus contactos y verificar la información antes de compartirla. Esto no solo te protege a ti, sino que también fomenta un ambiente digital más tolerante y positivo.

2.2 Contraseñas

Las contraseñas son, sin exagerar, las llaves de tu vida digital, tu acceso a datos personales, tu identidad e incluso tu dinero. Francisco Guzmán (Cirion Technologies)



subraya la importancia de una postura proactiva en ciberseguridad; las contraseñas (Figura 3) son su pilar fundamental.

Figura 3. Ingreso de contraseñas en dispositivo

Palacios, G. A. (2025). Google ImageFX.

¿Qué hábitos debes evitar? Según el portal noticioso Primicias, hay siete malos hábitos comunes:

- Usar secuencias sencillas como '123456'.
- Tener la misma clave para todo, esto da 'pase libre' a un ciberdelincuente a todos tus sistemas.
- Usar información pública y predecible, como tu número de teléfono, cédula, nombre o fecha de nacimiento.
- Crear dos o tres claves y solo cambiarles el orden para diferentes plataformas.
- Compartir nombre de usuario y contraseña por medios digitales inseguros como WhatsApp o correo electrónico.
- No cambiar las claves al menos una vez al año. El Ministerio de Gobierno también recomienda cambiarlas con regularidad.

- Guardar contraseñas en los gestores que ofrecen los navegadores, por las dudas sobre el manejo de datos de estas empresas.

Primicias nos da tres consejos importantes:

- Deben tener un mínimo de seis caracteres y combinar letras, números y caracteres especiales. Microsoft también recomienda incluir letras, números y símbolos fáciles de recordar pero difíciles de adivinar.
- Utiliza una clave completamente diferente para cada sistema y evita usar referencias personales que las hagan predecibles. Piensa en el caso de Angélica (Esenciales de Seguridad Digital), cuya contraseña sencilla y reutilizada llevó a que suplantaran su identidad en redes.
- Considera el uso de gestores de contraseñas. Estas aplicaciones guardan tus claves de forma segura, pueden generar claves aleatorias y detectan si alguna de tus claves ya existe en un sitio web ingresado. Solo necesitas memorizar la clave de tu computadora y la del gestor, que idealmente no deben ser guardadas digitalmente sino anotadas y memorizadas hasta que puedas destruir el papel. Al elegir un gestor, Primicias aconseja leer sus políticas de privacidad, verificar la calificación de usuarios, asegurarse de que no estén implicados en escándalos de filtración de datos y que encripten la información.

2.3 Prevención de riesgos

El Ministerio de Gobierno advierte sobre la astucia de ciertas personas que se aprovechan de ciudadanos, como en el caso Publifast y denuncias de modelos que recibieron propuestas laborales fraudulentas. Por ello, es crucial:

- Verificar la existencia y legalidad de las empresas con las que harás negocios, a través de entidades como el Servicio de Rentas Internas (SRI), la Superintendencia de Compañías, el Instituto Ecuatoriano de Seguridad Social (IESS) y la Cámara de Comercio. Si no aparecen, es mejor evitar la negociación.
- Nunca proporcionar las claves de tus tarjetas de crédito y evitar realizar pagos online desde computadoras públicas o redes wifi.
- Evitar responder correos electrónicos que te anuncien como ganador de loterías (Figura 4) o de trabajos que no has solicitado.

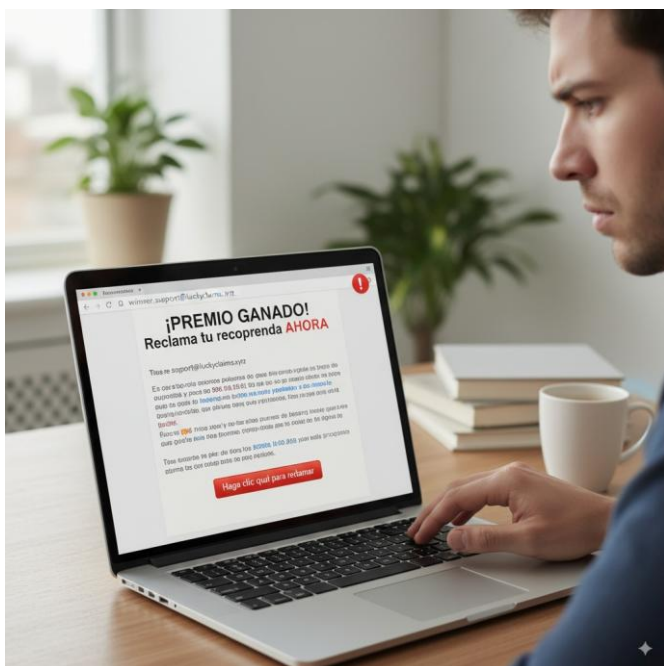


Figura 4. Riesgos de estafas digitales

Palacios, G. A. (2025). Google ImageFX.

- Según Microsoft (Esenciales de Seguridad Digital) protege tus datos personales. Piensa antes de dar clic en anuncios emergentes o antes de publicar cualquier información, no descargues aplicaciones de sitios desconocidos o con contenido ilegal, no hables con personas extrañas en línea, no aceptes términos y condiciones sin leerlos y no publiques tu ubicación constantemente.
- En tus redes sociales, mantén tus cuentas privadas, solo acepta a personas que conozcas y no compartas información personal tuya o de tus amigos. Revisa la configuración de privacidad y evita dar pistas sobre tu ubicación exacta. Recuerda que lo que publicas puede durar para siempre; una vez que subes algo, ‘DEJA DE SER TUYO’.

La Policía Nacional de Ecuador creó, en enero de 2012, una Unidad de Investigación de Cibercrimen para detectar, identificar, localizar y neutralizar el accionar de personas con conductas ilícitas a través de la tecnología. Si necesitas su colaboración, debes presentar una denuncia en la Fiscalía para que tu caso sea derivado a estos expertos informáticos. En el contexto del cyberbullying, Microsoft también recomienda pedir ayuda a un adulto de confianza, reportar publicaciones o perfiles que amenacen la seguridad y guardar evidencia con capturas de pantalla.

Esfuerzos en Ecuador: Ecuador está trabajando en la prevención de ‘ciberdelitos’

Título del enlace relacionado: Ecuador experimentó un crecimiento del 4,9 % en amenazas

Descripción breve del enlace relacionado: IT-Ahora informa que Ecuador fue el tercer país más atacado en Latinoamérica en 2024

Enlace: <https://itahora.com/2025/02/20/ecuador-experimento-un-crecimiento-del-49-en-amenazas/>

El Ministerio de Telecomunicaciones y de la Sociedad de la Información (Mintel) ha desarrollado proyectos para este fin. Según el Índice Global de Ciberseguridad 2017 de la UIT, Ecuador se encuentra en una etapa de ‘maduración’, desarrollando compromisos complejos en prevención de delitos cibernéticos y participando en iniciativas de seguridad.

La Organización de Estados Americanos (OEA) también ha reconocido los avances de Ecuador en el fortalecimiento de su capacidad para prevenir y manejar amenazas informáticas (Figura 5), destacando el Código Integral Penal (COIP) y el funcionamiento del Centro de Respuesta a Incidentes Informáticos del Ecuador (EcuCERT). EcuCERT recibe diariamente reportes de incidentes y vulnerabilidades, y



los comunica a los proveedores de servicios de telecomunicaciones para que tomen las medidas necesarias.

Figura 5

Representación organismos de ciberseguridad

Palacios, G. A. (2025). Google ImageFX.

3. 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.

4. Glosario clase 13

- **Ciudadanía digital.** Conjunto de habilidades y competencias que permiten a una persona acceder, comprender, analizar, producir y utilizar el entorno digital de manera crítica, ética y creativa, asegurando su protección y seguridad en línea.
- **Ciberseguridad.** Políticas, procedimientos y medidas implementadas para proteger la infraestructura tecnológica y los activos de información de amenazas que comprometen la información procesada, almacenada y transportada por los componentes tecnológicos interconectados.

5. Recurso de profundización clase 13

- **Título del recurso relacionado:** ‘Seguridad y privacidad en línea: ciudadanía digital, contraseñas y prevención de riesgos’

- **Descripción del recurso:** este material complementario presenta un resumen visual en diez diapositivas que refuerzan los temas trabajados en la clase 13. Incluye los conceptos clave de ciudadanía digital, la importancia de una gestión adecuada de contraseñas y las principales medidas de prevención frente a riesgos en línea. El recurso está diseñado para apoyar la reflexión crítica y la práctica responsable en el entorno digital, brindando a los estudiantes una herramienta clara y dinámica que facilita la apropiación de los contenidos.
- **Tipo de documento:** Presentación en formato PDF



La excelencia no se improvisa

síguenos

