Prevención de Amenazas Informáticas

Ejemplos Prácticos para Evitar su Propagación

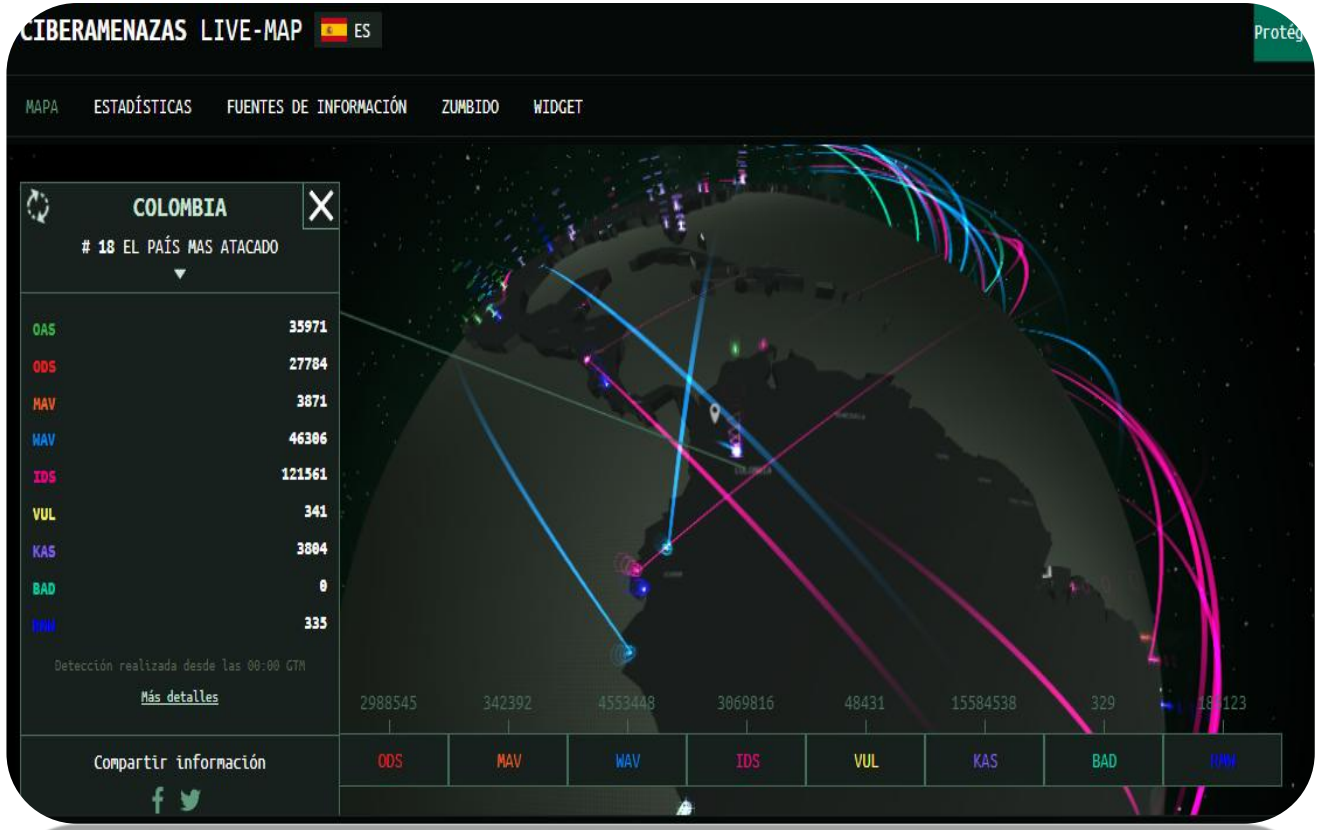
TECHNOLOGICAL SUPPLIES

Sobre la importancia de la ciberseguridad.

La ciberseguridad es vital para las empresas en Colombia porque protege contra el robo de datos, fraudes y ataques que pueden paralizar operaciones. Con el aumento de ciberataques, asegurar la información sensible y los sistemas es crucial para mantener la confianza de los clientes, cumplir con regulaciones y garantizar la continuidad del negocio. Una sólida ciberseguridad también ayuda a evitar pérdidas financieras y daños a la reputación de la empresa.

TECHNOLOGICAL SUPPLIES

Sobre la importancia de la ciberseguridad.



En 2025, la ciberseguridad en Colombia se enfrenta a un panorama desafiante y en constante evolución. Aquí algunos puntos clave sobre la situación actual y las proyecciones:

- **Aumento de amenazas cibernéticas:** Colombia ha experimentado un incremento significativo en los ciberataques, con más de 20 mil millones de incidentes reportados en 2024. Esto posiciona al país como uno de los más atacados en América Latina.
- **Inversiones en ciberseguridad:** Se espera que la inversión en ciberseguridad crezca un 19% en 2025, impulsada por la necesidad de proteger infraestructuras críticas y datos sensibles.

TECHNOLOGICAL SUPPLIES

Sobre la importancia de la ciberseguridad.

- **Tendencias tecnológicas:** Las tecnologías emergentes, como la inteligencia artificial (IA) y la computación cuántica, están transformando tanto las amenazas como las soluciones de ciberseguridad. Los ataques impulsados por IA son cada vez más sofisticados, lo que exige medidas de seguridad más avanzadas.
- **Adopción de estrategias avanzadas:** Las empresas están implementando enfoques como la autenticación multifactorial y el modelo de "confianza cero" (Zero Trust) para fortalecer su seguridad digital.
- **Crecimiento del mercado:** El mercado de ciberseguridad en Colombia está en expansión, con un crecimiento anual compuesto del 14,7% proyectado entre 2025 y 2034.

TECHNOLOGICAL SUPPLIES

¿Cuál es mi papel en Ciberseguridad?

1. Directores o Administración Escolar:

Establecen políticas generales de ciberseguridad para el colegio.

Asignan recursos para la protección digital y la formación en este ámbito.

Supervisan el cumplimiento de regulaciones y normas locales de privacidad de datos.

2. Profesores:

Incorporan buenas prácticas de seguridad digital en su enseñanza.

Enseñan a los estudiantes a identificar amenazas en línea, como phishing o malware.

Actúan como modelos de comportamiento seguro al utilizar dispositivos y plataformas en clase.

3. Estudiantes:

Aprenden y aplican buenas prácticas de seguridad, como usar contraseñas seguras y no compartir información personal en línea.

Reportan cualquier actividad sospechosa a los profesores o al personal de TI.

4. Personal de Tecnología (TI):

Configuran y supervisan la infraestructura digital del colegio.

Protegen la red escolar de ataques y supervisan actividades sospechosas.

Implementan medidas como firewalls, sistemas antivirus y actualizaciones regulares.

5. Padres o Tutores:

Promueven hábitos de ciberseguridad en casa, como el uso responsable de dispositivos.

Supervisan el comportamiento en línea de los estudiantes fuera del entorno escolar.

Colaboran con el colegio en la enseñanza de valores relacionados con la seguridad digital.

6. Personal Administrativo:

Gestionan datos confidenciales (como registros de estudiantes) de manera segura.

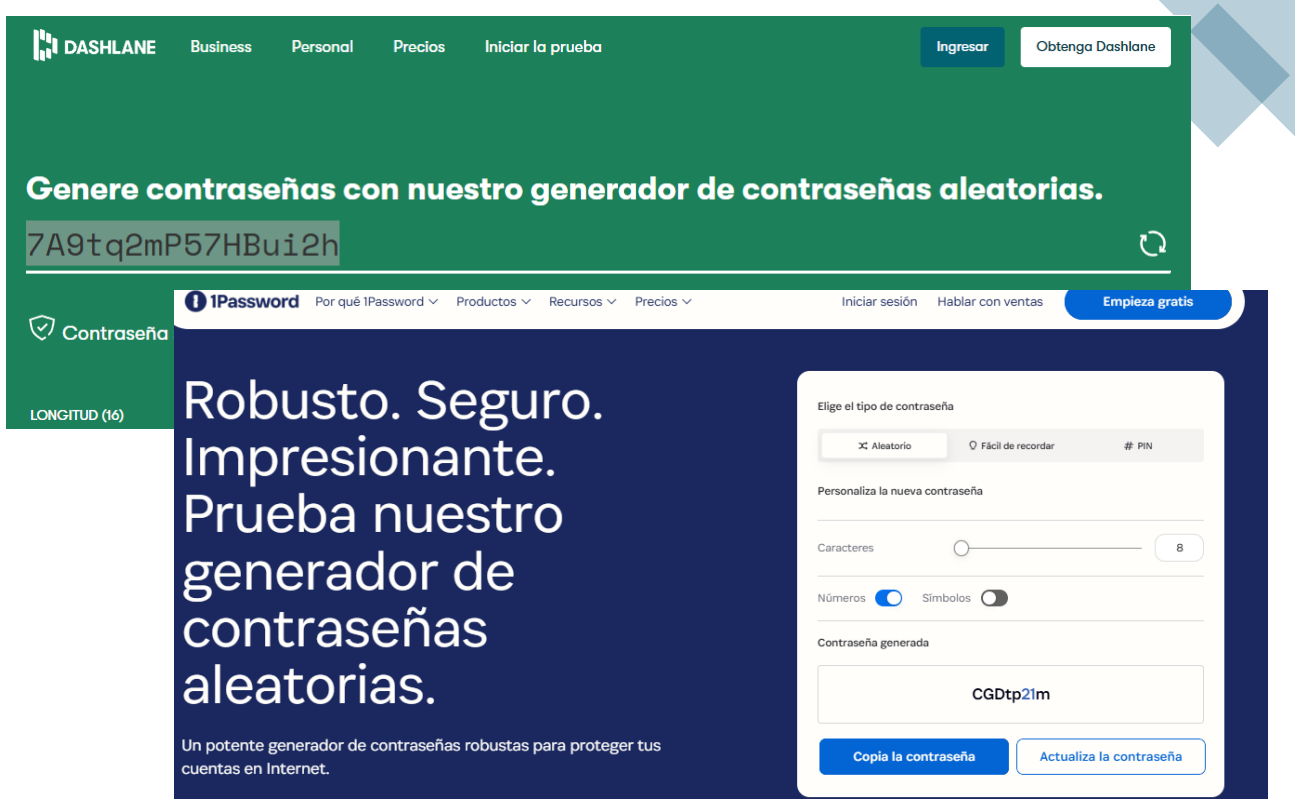
Implementan controles de acceso para proteger la información almacenada en sistemas escolares.

TECHNOLOGICAL SUPPLIES

Uso de Contraseñas Seguras

Crear contraseñas seguras es fundamental para proteger tu información personal y cuentas en línea. Aquí tienes algunos consejos para crear contraseñas robustas:

1. **Longitud**: Asegúrate de que tu contraseña tenga al menos 12 caracteres.
2. **Combinación de caracteres**: Usa una mezcla de letras mayúsculas y minúsculas, números y símbolos.
3. **Evita información personal**: No uses nombres, fechas de nacimiento o palabras comunes.
4. **Frases de contraseña**: Considera usar una frase larga y única que sea fácil de recordar, pero difícil de adivinar.
5. **Gestores de contraseñas**: Utiliza un gestor de contraseñas para generar y almacenar contraseñas seguras.



TECHNOLOGICAL SUPPLIES

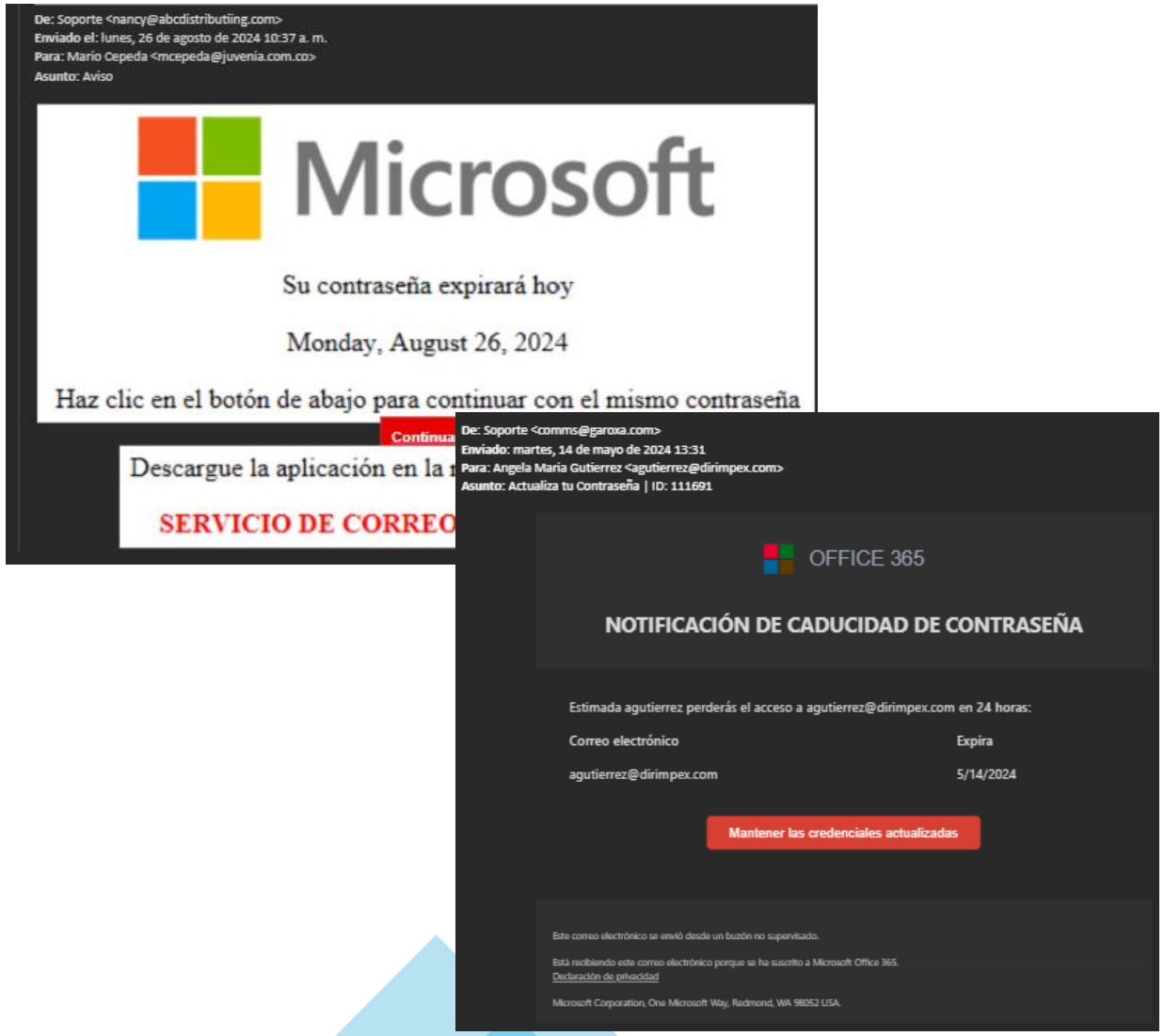
Actualizaciones de Software

Las actualizaciones de software son esenciales para mantener tus dispositivos seguros y funcionando de manera óptima. Aquí tienes algunos puntos clave sobre las actualizaciones de software:

1. **Seguridad**: Las actualizaciones suelen incluir parches de seguridad que corrigen vulnerabilidades y protegen contra amenazas recientes.
2. **Rendimiento**: Mejoran el rendimiento del software, corrigiendo errores y optimizando el funcionamiento.
3. **Nuevas Funciones**: A menudo, las actualizaciones añaden nuevas características y funcionalidades que mejoran la experiencia del usuario.
4. **Compatibilidad**: Mantienen la compatibilidad con otros programas y dispositivos, asegurando que todo funcione sin problemas.
5. **Estabilidad**: Corrigen errores y problemas que pueden causar fallos o inestabilidad en el software.

TECHNOLOGICAL SUPPLIES

Phishing y Correos Electrónicos Sospechosos



Como identificarlos:

Remitente Desconocido: Si recibes un correo de alguien que no conoces o de una dirección de correo sospechosa, ten cuidado.

Errores Ortográficos y Gramaticales: Los correos de phishing a menudo contienen errores ortográficos o gramaticales.

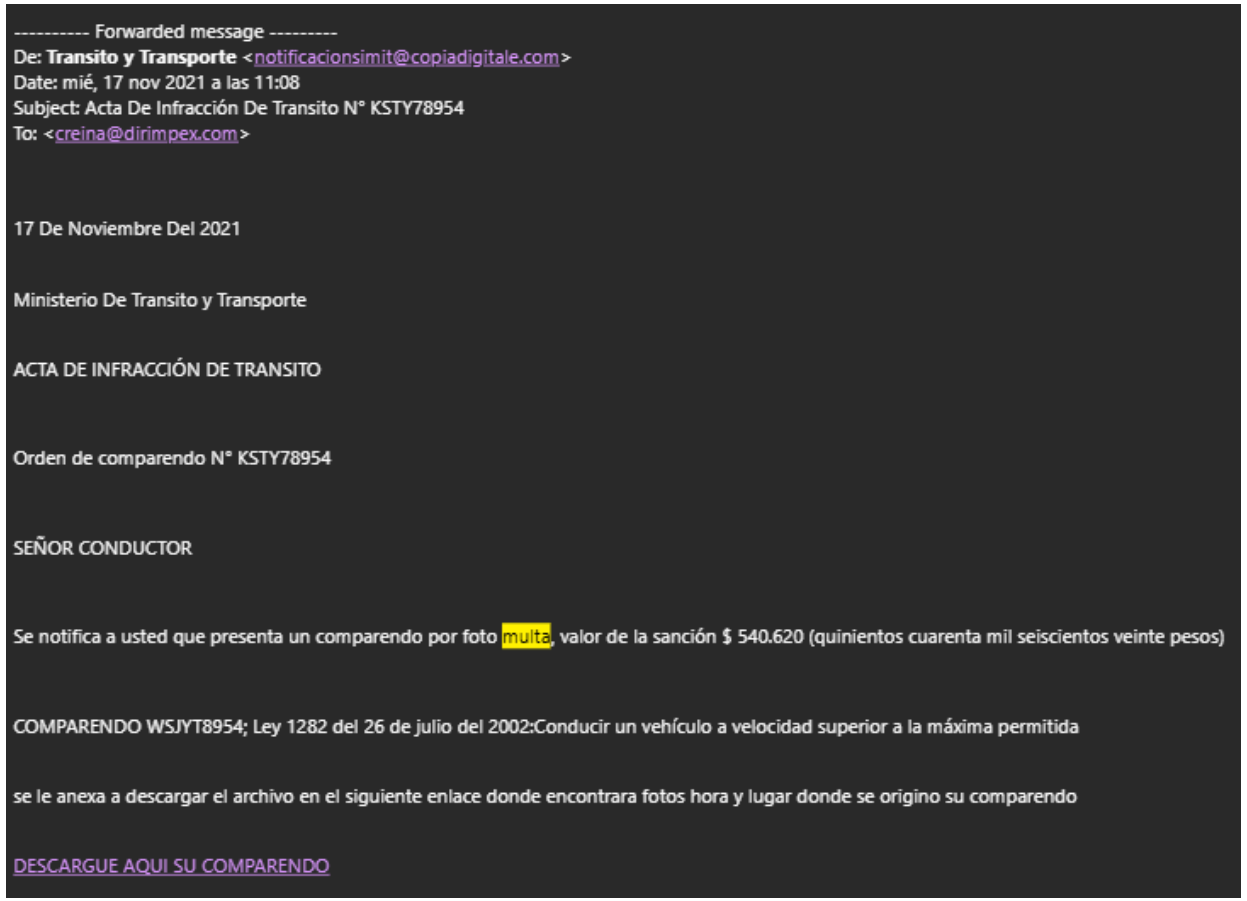
Enlaces Sospechosos: Pasa el cursor sobre los enlaces sin hacer clic para ver la URL real. Si parece sospechosa o no coincide con el remitente, no hagas clic.

Solicitudes de Información Personal: Las empresas legítimas nunca te pedirán información personal o contraseñas a través de correo electrónico.

Urgencia o Amenazas: Los correos que intentan asustarte con amenazas o urgencia para que actúes rápidamente suelen ser fraudulentos.

TECHNOLOGICAL SUPPLIES

Phishing y Correos Electrónicos Sospechosos



---------- Forwarded message ---------
De: **Transito y Transporte** <notificacionsimit@copiadigitale.com>
Date: mié, 17 nov 2021 a las 11:08
Subject: Acta De Infracción De Transito N° KSTY78954
To: <creina@dirimpex.com>

17 De Noviembre Del 2021

Ministerio De Transito y Transporte

ACTA DE INFRACCIÓN DE TRANSITO

Orden de comparendo N° KSTY78954

SEÑOR CONDUCTOR

Se notifica a usted que presenta un comparendo por foto multa, valor de la sanción $ 540.620 (quinientos cuarenta mil seiscientos veinte pesos)

COMPARENDO WSJYT8954; Ley 1282 del 26 de julio del 2002:Conducir un vehículo a velocidad superior a la máxima permitida

se le anexa a descargar el archivo en el siguiente enlace donde encontrara fotos hora y lugar donde se origino su comparendo

DESCARGUE AQUI SU COMPARENDO

Como protegerte:

No Hagas Clic en Enlaces Sospechosos: Si tienes dudas sobre un correo, no hagas clic en ningún enlace ni descargues archivos adjuntos.

Verifica la Fuente: Contacta directamente a la empresa o persona a través de un medio de comunicación confiable para verificar la autenticidad del correo.

Usa Software de Seguridad: Mantén actualizado tu software antivirus y antimalware.

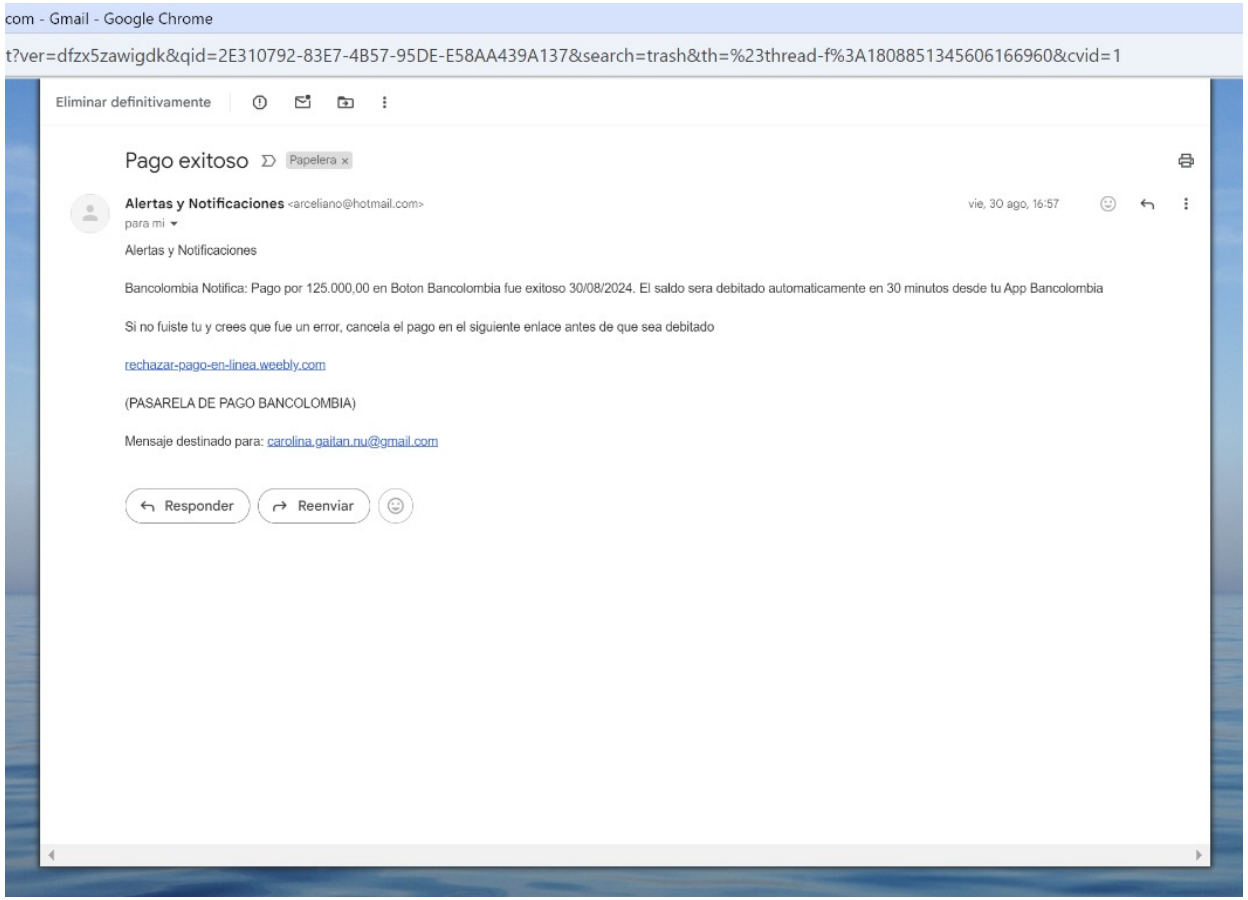
Activa la Autenticación de Dos Factores (2FA): Añade una capa extra de seguridad a tus cuentas.

Educa a Otros: Informa a tus amigos y familiares sobre los riesgos del phishing y cómo protegerse.

Reporta al departamento de tecnología a través de la mesa de ayuda en WhatsApp o el correo sistemas@incodema.edu.co

TECHNOLOGICAL SUPPLIES

Ingeniería Social



Correos electrónicos sospechosos: Los ataques de phishing son muy comunes. Si recibes un correo de un remitente desconocido o que parece legítimo pero tiene errores ortográficos o enlaces sospechosos, es mejor no interactuar con él.

Solicitudes urgentes: Los atacantes suelen crear un sentido de urgencia para que actúes sin pensar. Por ejemplo, un correo que dice que tu cuenta será bloqueada si no proporcionas información inmediatamente.

Ofertas demasiado buenas para ser verdad: Si recibes una oferta increíble, como ganar un premio sin haber participado en un concurso, es probable que sea un intento de ingeniería social.

Llamadas telefónicas inesperadas: Los atacantes pueden hacerse pasar por representantes de empresas legítimas para obtener información personal. Siempre verifica la identidad del llamante antes de proporcionar cualquier dato.

Mensajes en redes sociales: Los atacantes pueden usar perfiles falsos para ganarse tu confianza y obtener información personal. Sé cauteloso al aceptar solicitudes de amistad o al compartir información personal en línea.

Solicitudes de información personal: Si alguien te pide información personal o financiera sin una razón clara, es mejor desconfiar y verificar la solicitud por otros medios.

TECHNOLOGICAL SUPPLIES

Ingeniería Social

Educación y Conciencia: Aprende sobre las tácticas comunes de ingeniería social, como el phishing, el pretexting y el baiting. Mantente informado sobre las últimas amenazas.

Verificación de Identidad: Siempre verifica la identidad de la persona que solicita información confidencial. No compartas datos sensibles sin confirmar la autenticidad de la solicitud.

Contraseñas Seguras: Utiliza contraseñas fuertes y únicas para cada cuenta. Considera el uso de un gestor de contraseñas para mantenerlas seguras.

Doble Autenticación: Habilita la autenticación de dos factores (2FA) en todas tus cuentas importantes. Esto añade una capa extra de seguridad.

Cuidado con los Enlaces y Archivos Adjuntos: No hagas clic en enlaces ni descargues archivos adjuntos de correos electrónicos o mensajes sospechosos.

Políticas de Seguridad: Sigue las políticas de seguridad de tu organización y reporta cualquier actividad sospechosa a tu departamento de TI.

Actualizaciones de Software: Mantén tu software y sistemas operativos actualizados para protegerte contra vulnerabilidades conocidas.

TECHNOLOGICAL SUPPLIES

Uso de Redes Wi-Fi Seguras

Evita redes WiFi públicas para transacciones sensibles: No realices operaciones bancarias ni compras en línea cuando estés conectado a una red WiFi pública1.

Usa una VPN: Una Red Privada Virtual (VPN) cifra tu conexión a Internet, protegiendo tus datos de posibles interceptaciones2.

Verifica el nombre de la red: Asegúrate de conectarte a la red correcta y no a una red falsa creada por cibercriminales1.

Desactiva la conexión automática: Configura tu dispositivo para que no se conecte automáticamente a redes WiFi abiertas1.

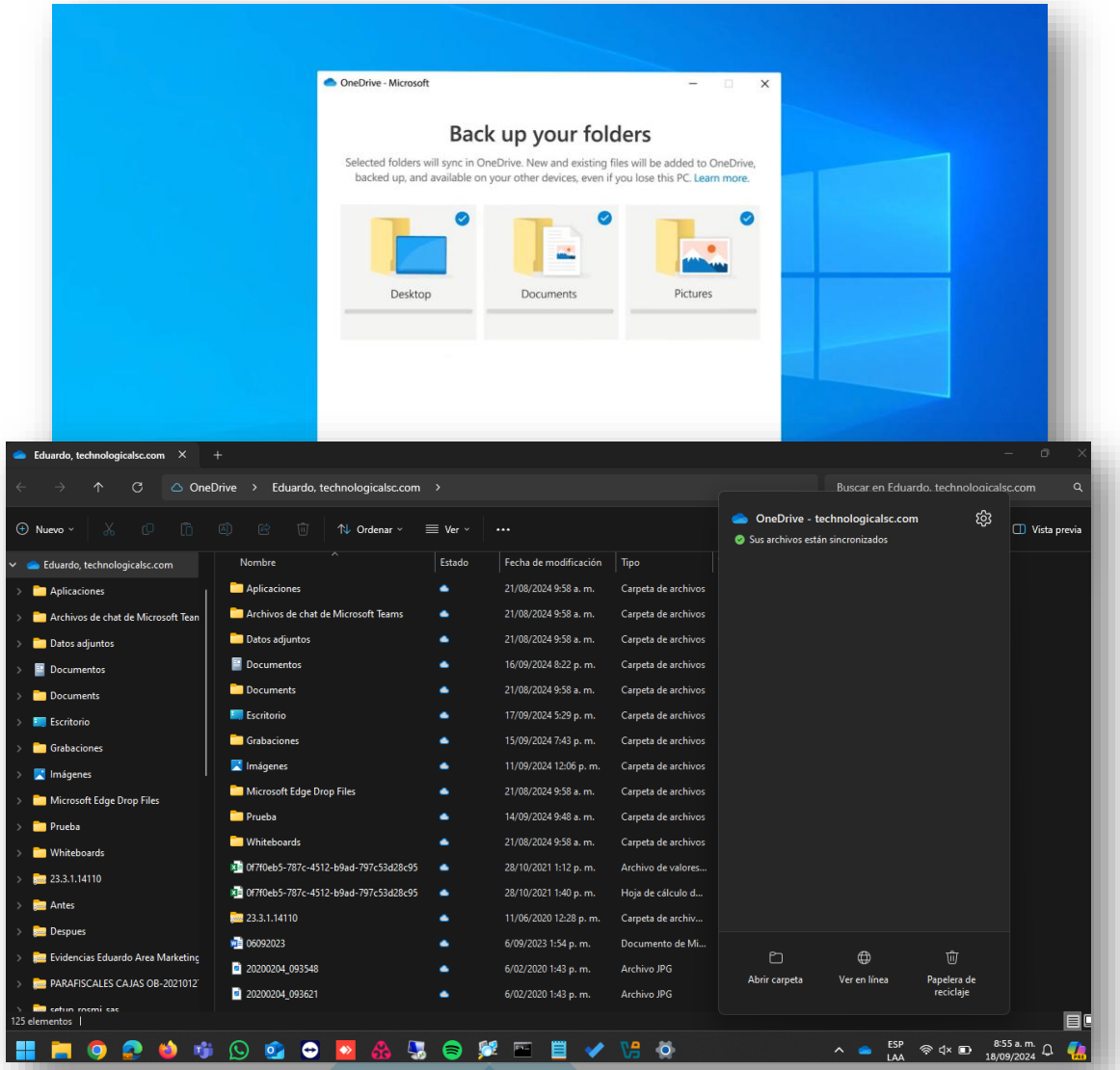
Mantén tu software actualizado: Asegúrate de que tu sistema operativo y aplicaciones estén siempre actualizados para protegerte contra vulnerabilidades conocidas2.

Usa autenticación de dos factores: Activa la autenticación de dos factores en tus cuentas para añadir una capa extra de seguridad2.

Desactiva el WiFi cuando no lo uses: Esto no solo ahorra batería, sino que también reduce el riesgo de que tu dispositivo se conecte a redes no seguras

TECHNOLOGICAL SUPPLIES

Copias de Seguridad – OneDrive.



Al usar OneDrive para hacer copias de seguridad, los usuarios pueden beneficiarse de varias garantías importantes:

Protección contra pérdida de datos: OneDrive asegura que tus archivos estén respaldados en la nube, lo que significa que puedes recuperarlos en caso de pérdida, daño o robo de tu dispositivo.

Acceso desde cualquier lugar: Tus archivos respaldados en OneDrive están disponibles desde cualquier dispositivo con conexión a Internet, permitiéndote acceder a ellos en cualquier momento y lugar.

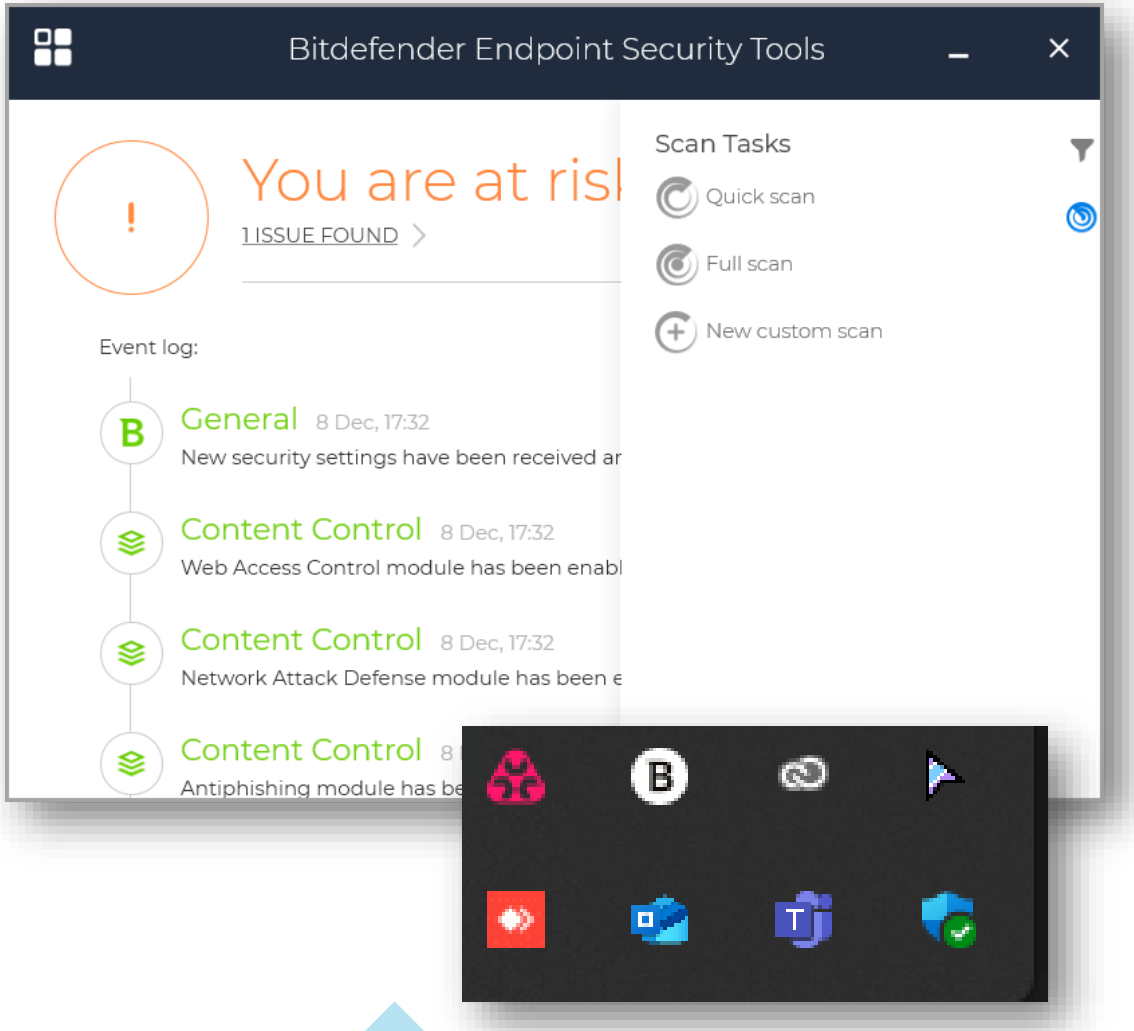
Historial de versiones: OneDrive guarda versiones anteriores de tus archivos por hasta 30 días, lo que te permite restaurar versiones anteriores si es necesario.

Almacén personal: Para documentos importantes, OneDrive ofrece un Almacén personal con verificación de identidad adicional para mayor seguridad3.

Sincronización automática: Los cambios en tus archivos se sincronizan automáticamente en todos tus dispositivos, asegurando que siempre trabajes con la versión más reciente.

TECHNOLOGICAL SUPPLIES

Software Antivirus y Antimalware



Protección contra amenazas: Estos programas están diseñados para detectar, prevenir y eliminar virus, malware, spyware, adware y otras formas de software malicioso que pueden dañar tu sistema o robar información.

Seguridad de datos: Ayudan a proteger la integridad y privacidad de tus datos, evitando accesos no autorizados y posibles filtraciones de información confidencial.

Prevención de fraudes: Al bloquear software malicioso, reducen el riesgo de fraudes en línea, como el robo de identidad y el acceso no autorizado a cuentas bancarias.

Rendimiento del sistema: Mantienen el rendimiento óptimo de tu dispositivo al eliminar programas que pueden ralentizarlo o causar fallos.

Actualizaciones constantes: Los programas antivirus y antimalware se actualizan regularmente para proteger contra las últimas amenazas conocidas, asegurando una defensa continua y efectiva.

Tranquilidad: Saber que tus dispositivos están protegidos te permite navegar por Internet y realizar actividades en línea con mayor confianza y seguridad.

TECHNOLOGICAL SUPPLIES

Educación y Concienciación

Reducción de errores humanos: La mayoría de los incidentes de ciberseguridad se deben a errores humanos, como hacer clic en enlaces maliciosos o usar contraseñas débiles. La formación ayuda a los usuarios a reconocer y evitar estos errores.

Protección de datos personales: Conocer las mejores prácticas de seguridad permite a los usuarios proteger su información personal y evitar el robo de identidad.

Prevención de ataques: La educación en ciberseguridad enseña a los usuarios a identificar y responder a amenazas como el phishing, el malware y otros tipos de ataques cibernéticos.

Cultura de seguridad: Fomentar una cultura de seguridad dentro de una organización o comunidad ayuda a que todos los miembros sean más conscientes de los riesgos y adopten comportamientos seguros en línea.

Adaptación a nuevas amenazas: El panorama de amenazas cibernéticas está en constante evolución. La formación continua asegura que los usuarios estén al tanto de las últimas tácticas y técnicas utilizadas por los ciberdelincuentes.

Responsabilidad compartida: La ciberseguridad no es solo responsabilidad del departamento de TI; todos los usuarios deben estar involucrados y ser responsables de mantener la seguridad de la información.

TECHNOLOGICAL SUPPLIES

¡Gracias por su atención!