UNIVERSIDAD SERGIO ARBOLEDA | Colsubsidio

Diplomado de Ciberseguridad y Gestión de Seguridad de la Información

Modulo 1:

Introducción a la Ciberseguridad y Seguridad de la Información

Sesión 1:

Amenazas comunes en entornos digitales y Cultura de Seguridad

OBJETIVO DE LA SESIÓN:

Identificar los principales tipos de amenazas en internet, cómo actúan y cómo prevenirlos.
Reflexionar sobre la importancia de adoptar comportamientos seguros.

¿Qué es una amenaza en ciberseguridad?

Una **amenaza** es cualquier evento o acción que puede poner en riesgo la **confidencialidad, integridad o disponibilidad** de la información (Modelo CIA). Estas amenazas pueden ser:

- **Internas:** provienen de dentro de la organización (por error humano o sabotaje).
- **Externas:** provienen de atacantes o actores maliciosos fuera de la organización.

En el entorno digital, las amenazas evolucionan constantemente. A continuación, te explico las más comunes y cómo afectan al usuario promedio o a una empresa.

Phishing (Suplantación de identidad)

Es un tipo de fraude en el que un atacante se hace pasar por una entidad legítima (como un banco, universidad o empresa de tecnología) para engañar al usuario y obtener información confidencial, como contraseñas, números de tarjeta de crédito o datos personales.

¿Cómo funciona?

- El atacante envía un correo electrónico (o mensaje de texto) que parece real.
- Te pide hacer clic en un enlace y proporcionar datos personales o descargar un archivo.
- Al hacerlo, los datos van al atacante o se instala un software malicioso.

Ejemplo

Recibes un correo que dice: "Su cuenta de Netflix fue suspendida por falta de pago. Ingrese aquí para reactivarla.“

El enlace lleva a una página falsa que luce como Netflix. Al ingresar tu usuario y contraseña, se roban estos datos.

¿Cómo prevenirlo?

- Verifica el dominio del correo (ej. @netflix.com vs. @netflix-support.info)
- No hagas clic en enlaces sospechosos
- Nunca ingreses datos sensibles en sitios que no estén verificados
- Usa autenticación multifactor (MFA)

Ejercicio 1: Análisis de correos simulados

En grupo los estudiantes deben identificar cuál de las 3 imágenes presentadas, Son correos falsos

José Luis Rivas

De: Iñaki Urdangarin [iurdangarin@noos.com]
Enviado el: jueves, 08 de abril de 2004 13:06
Para: jlrivas@laboratoriodeseguridadtelematica.com
Asunto: Reunión acordada

Hola José,

Despues de hablar con mi suegro me ha dicho que no hay problema, y me voy a encontrar con ellos el dia 22 en el Palacio después de finalizar la audiencia.

Salu2,
Iñaki

P.D. Recuerdos a tu familia, Cristina y yo nos acordamos mucho de las navidades pasadas. Que buenos recuerdos!!!!

Iñaki Urdangarin
Responsable de Proyectos Europeos
Instituto Noos

Outlook

Dear User,

All Hotmail customers have been upgraded to Outlook.com. Your Hotmail Account services has expired.

Due to our new system upgrade to Outlook. In order for it to remain active
follow the link Sign in Re-activate your account to Outlook. https://account.live.com

Thanks,
The Microsoft account team

MO

Wed 10/5/2016 11:21 PM

Microsoft Outlook <msoutlook94@service.out1ook.com>

Your Password Has Expired

To

Password Expired.

Your password for the Microsoft Outlook account [redacted] has expired.

For your account's security, your current password will cease to work shortly .

You are now required to **change your password** immediately.

Click below to change your password
http://msoutlook.service.outlook.com/msacks/reset.html

This is a system notification not an email message and you can't reply to it.

Malware (Software malicioso)

El término “malware” viene de “**malicious software**”. Es un conjunto de programas diseñados para dañar, infiltrarse, robar información o controlar un dispositivo sin que el usuario lo sepa.

Tipos principales de malware

Tipo	Qué hace	Ejemplo común
Virus	Se adhiere a archivos ejecutables y se activa cuando se abren.	Archivos de Word infectados
Gusano (Worm)	Se propaga solo a través de redes.	Propagación por correo electrónico a todos tus contactos
Troyano (Trojan)	Se presenta como un software útil, pero tiene funciones ocultas.	Un convertidor de PDF que en realidad roba archivos
Spyware	Espía lo que haces en tu equipo.	Graba teclas para robar contraseñas
Adware	Muestra publicidad excesiva o no deseada.	Pop-ups que abren páginas sin control

¿Cómo prevenirlo?

- No descargar programas de sitios desconocidos
- Usar antivirus actualizados
- Evitar conectar USBs desconocidos
- Mantener el sistema operativo al día

Analogía: Un troyano es como recibir una caja bonita (programa gratuito) que contiene una bomba (malware oculto). Parece útil, pero te perjudica al instalarlo.

Melissa (1999)

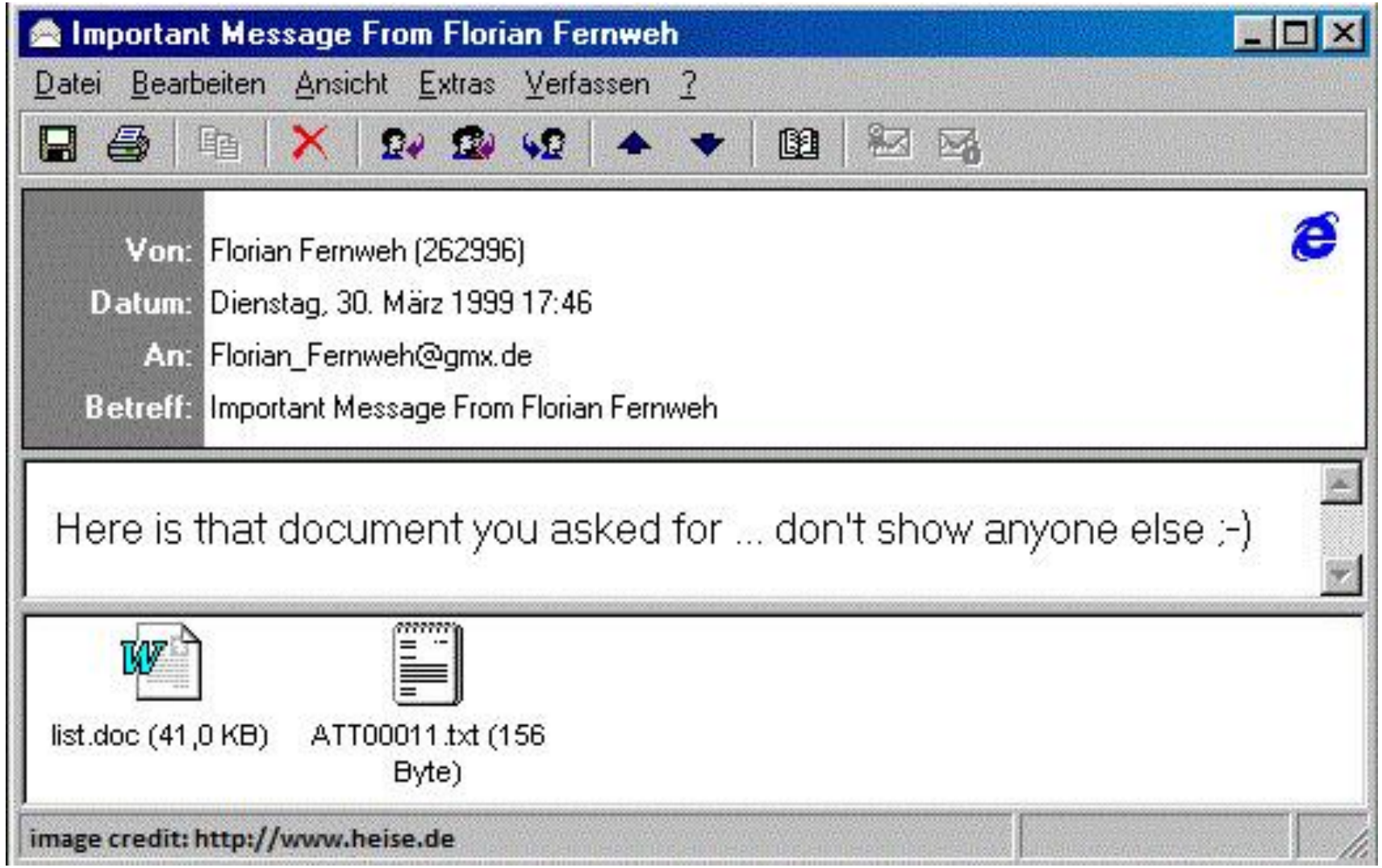
El virus Melissa fue un macrovirus que se propagó a través de correos electrónicos con documentos de Word adjuntos en 1999. Al abrir el archivo infectado, el virus se activaba y se enviaba automáticamente a las primeras 50 direcciones de la libreta de contactos del usuario afectado, causando una gran congestión en las redes. Fue creado por David L. Smith y se considera uno de los virus más rápidos en propagarse en su momento, causando millones de dólares en daños.

Cómo funcionaba:

- Un usuario recibía un correo electrónico con un documento de Word adjunto.
- Si el usuario abría el archivo adjunto, el virus se activaba y se copiaba en la plantilla de documentos de Word del usuario.
- El virus deshabilitaba la configuración de seguridad de macros de Microsoft Word.
- Luego, utilizando Microsoft Outlook, el virus enviaba copias de sí mismo a las primeras 50 direcciones de correo electrónico de la libreta de contactos del usuario.
- Este proceso se repetía cada vez que un usuario infectado abría un documento de Word.

Infectó >100,000 PCs en 5 días, el más rápido de su época. Sobrecargó servidores de email (e.g., Microsoft y gobiernos), causando caídas y pérdidas de $80 millones en productividad. No destruía archivos, pero facilitaba spam y exposición de datos personales.

Melissa



El creador de 'Melissa', David L. Smith, reconoció su culpabilidad aunque aseguró que no esperaba un perjuicio económico tan elevado. Este malware fue creado en memoria de una bailarina de topless de Florida de la cual se había enamorado.

https://www.pandasecurity.com/es/mediacenter/virus-melissa/

Gusano Conficker (2008-2009)

El gusano Conficker, también conocido como Downadup, apareció en octubre de 2008 y se convirtió en una de las amenazas más extendidas de su época. Diseñado para infectar sistemas Windows, se propagaba automáticamente por redes y dispositivos USB, creando una botnet masiva. Fue notable por su persistencia y sofisticación, afectando millones de dispositivos en todo el mundo.

Cómo funcionaba:

- Explotación de vulnerabilidad: Aprovechaba una falla en el servicio Server de Windows (MS08-067, buffer overflow) en sistemas XP, 2000, 2003, Vista y Server.
- Propagación autónoma: Escaneaba redes locales e internet para infectar máquinas vulnerables a través de puertos SMB (445). También se copiaba a dispositivos USB mediante AutoRun.
- Infección silenciosa: Una vez en el sistema, descargaba actualizaciones desde dominios generados dinámicamente (250 al día), dificultando su bloqueo.
- Persistencia: Deshabilitaba Windows Update, bloqueaba antivirus y modificaba configuraciones de seguridad para permanecer activo.
- Botnet: Convertía los dispositivos infectados en parte de una red controlada remotamente, lista para spam, DDoS o robo de datos.

Infectó entre 10 y 15 millones de PCs en 190 países, incluyendo gobiernos (e.g., Francia, Reino Unido) y empresas críticas.Creó una de las botnets más grandes de la historia, aunque no se usó para ataques destructivos masivos.Causó pérdidas estimadas en $9 mil millones por costos de remoción, interrupciones en redes y esfuerzos de mitigación.

Troyano Zeus (2007-2010)

Zeus, también conocido como Zbot, emergió en 2007 y alcanzó su pico entre 2009 y 2010. Fue un troyano bancario diseñado para robar credenciales financieras, disfrazado como software legítimo. Su código fuente se filtró en 2011, dando lugar a variantes como GameOver Zeus. Fue una de las principales amenazas financieras de su tiempo.

Cómo funcionaba:

- Distribución: Se distribuía mediante correos de phishing con adjuntos (e.g., facturas falsas), descargas drive-by en sitios comprometidos o actualizaciones falsas.
- Disfraz: Se presentaba como software útil, como un "plugin de seguridad" o "descargador de videos".
- Man-in-the-browser: Instalaba un componente que interceptaba sesiones HTTPS de banca online, modificando formularios o capturando credenciales en tiempo real.
- Exfiltración: Enviaba datos robados (e.g., contraseñas, números de cuenta) a servidores de comando y control (C2) usando conexiones cifradas.
- Botnet: Formaba redes de bots para spam, DDoS o distribución de más malware.

Infectó 3.6 millones de PCs en 2009, robando más de $100 millones en fondos bancarios globales.Comprometió 74,000 cuentas FTP, facilitando ataques a servidores web.Operaciones policiales (2010) desmantelaron redes, pero las variantes continuaron hasta 2014.Resaltó la necesidad de autenticación multifactor y detección de comportamiento en banca online.

Spyware Pegasus (2016-Presente)

Pegasus, desarrollado por NSO Group (Israel), es un spyware avanzado usado principalmente por gobiernos para vigilancia. Expuesto en 2016 y ampliamente documentado en 2021 (Proyecto Pegasus), ha sido utilizado para espiar a periodistas, activistas y políticos. Es conocido por sus exploits zero-click, que no requieren interacción del usuario.

Cómo funciona:

- Infección inicial: Originalmente vía spear-phishing (SMS/emails con enlaces maliciosos). Desde 2019, usa exploits zero-click (e.g., iMessage o WhatsApp) que infectan sin interacción.
- Acceso total: Una vez instalado, accede a mensajes, llamadas, correos, cámara, micrófono, GPS y apps cifradas (e.g., Signal) en iOS/Android.
- Persistencia: Se ejecuta en memoria, evitando detección. Se actualiza desde servidores C2 para mantener control.
- Exfiltración: Envía datos a servidores remotos mediante conexiones cifradas, a menudo en horarios nocturnos.
- Evasión: Usa técnicas anti-forenses para borrar rastros en el dispositivo.

Espió a más de 50,000 objetivos (periodistas, activistas, líderes) en 50+ países en 2021. Generó escándalos diplomáticos, demandas contra NSO y sanciones (e.g., EE.UU. lo incluyó en lista negra en 2021). Subrayó riesgos de spyware estatal y la necesidad de actualizaciones de seguridad en móviles.

Adware Superfish (2014-2015)

Superfish fue un adware preinstalado por Lenovo en laptops consumer entre septiembre de 2014 y enero de 2015. Diseñado para inyectar publicidad en páginas web, comprometió la seguridad al instalar certificados root inseguros. Fue descubierto en 2015, causando un escándalo por violaciones de privacidad.

Cómo funcionaba:

- Preinstalación: Venía preinstalado en laptops Lenovo (e.g., Yoga, IdeaPad) como "optimizador visual".
- Inyección de anuncios: Interceptaba sesiones HTTPS, insertando anuncios personalizados en sitios web visitados.
- Certificado inseguro: Instalaba un certificado root auto-firmado, permitiendo ataques man-in-the-middle al descifrar tráfico HTTPS.
- Persistencia: Ejecutado como servicio de sistema, difícil de desinstalar sin herramientas específicas.
- Monetización: Recopilaba datos de navegación para dirigir anuncios, enviándolos a servidores de Superfish.

Afectó 750,000 laptops, comprometiendo la privacidad de usuarios al exponer datos HTTPS. Causó ralentización del sistema y pop-ups intrusivos, afectando la experiencia del usuario. Lenovo enfrentó demandas ($3.5M multa en EE.UU.) y daño reputacional severo..

Lee los siguientes escenarios y clasifica el malware (Conficker, Zeus, Pegasus, Superfish).

Escenarios:

- Descargas un "plugin de video" y tu banco reporta transacciones no autorizadas.
- Tu laptop Lenovo muestra anuncios en cada sitio web, incluso en HTTPS.T
- u red empresarial se ralentiza, y todos los PCs muestran actualizaciones bloqueadas.
- Recibes un SMS que activa un programa que graba tus llamadas sin interacción.

Lee los siguientes escenarios y clasifica el malware (Conficker, Zeus, Pegasus, Superfish).

Escenarios:

- **Descargas un "plugin de video" y tu banco reporta transacciones no autorizadas.**
- Tu laptop Lenovo mue
  HTTPS.T
- u red empresarial se i ones
  bloqueadas.
- Recibes un SMS que activa un programa que graba tus llamadas sin interacción.

Zeus: Propagación por phishing; roba credenciales bancarias. Mitigación: Habilita MFA, escanea con antivirus.

Lee los siguientes escenarios y clasifica el malware (Conficker, Zeus, Pegasus, Superfish).

Escenarios:

- Descargas un "plug o autorizadas.
- **Tu laptop Lenovo muestra anuncios en cada sitio web, incluso en HTTPS.**
- Tu red empresarial se ralentiza, y todos los PCs muestran actualizaciones bloqueadas.
- Recibes un SMS que activa un programa que graba tus llamadas sin interacción.

Superfish: Preinstalado, inyecta ads.
Mitigación: Usa AdwCleaner, elimina certificados sospechosos.

Lee los siguientes escenarios y clasifica el malware (Conficker, Zeus, Pegasus, Superfish).

Escenarios:

- Descargas un "plugin de video" y tu banco reporta transacciones no autorizadas.
- Tu laptop Lenovo muestra anuncios en cada sitio web, incluso en HTTPS.
- **Tu red empresarial se ralentiza, y todos los PCs muestran actualizaciones bloqueadas.**
- Recibes un SMS que activa [redacted] interacción.

Conficker: Propagación por red. Mitigación: Aplica parche MS08-067, desconecta red.

Lee los siguientes escenarios y clasifica el malware (Conficker, Zeus, Pegasus, Superfish).

Escenarios:

- Descargas un "plugin de video" y tu banco reporta transacciones no autorizadas.
- Tu laptop Lenovo muestra anuncios en cada sitio web, incluso en HTTPS.
- Tu red empresarial se ralentiza, y todos los PCs muestran actualizaciones bloqueadas.
- **Recibes un SMS que activa un programa que graba tus llamadas sin interacción.**

Pegasus: Zero-click via SMS. Mitigación: Actualiza iOS/Android, usa Signal.

Actividad Simulada: SPYWARE

Simule un spyware para entender su funcionamiento, inspirado en casos reales como Pegasus. El programa debe ejecutarse en Google Colab, simulando un comportamiento malicioso (registro de datos) de forma oculta, mientras se disfraza como una aplicación útil.

Objetivo:

- Comprender cómo los spywares espían actividades de usuarios sin ser detectados.
- Diseñar un programa educativo que simule espionaje éticamente, sin dañar sistemas.
- Reflexionar sobre medidas de detección y prevención.

Escribe un programa en Python que:

- Funcionalidad visible: Ofrezca una utilidad simple (e.g., calculadora, conversor de texto, generador de notas).
- Funcionalidad oculta: Registre datos simulados (e.g., "teclas" ficticias, timestamps) en un archivo de log usando un hilo en segundo plano (threading).
- Ejecución discreta: Muestre como mensaje los datos simulados capturados.

No debe intentar capturar datos reales ni conectarse a redes externas (solo simulación en Colab).

¿Cómo se compara tu spyware con casos reales como Pegasus?

¿Qué medidas tomarías para proteger tu PC de un spyware real?

Ransomware (Secuestro de información)

Es un tipo específico de malware que **“secuestra” tu información**: cifra (bloquea) tus archivos y exige el pago de un rescate (normalmente en criptomonedas) para recuperarlos.

¿Cómo funciona?

1. Se instala en el equipo mediante un archivo o sitio web malicioso.
2. Encripta todos los archivos importantes.
3. Aparece un mensaje exigiendo un pago (con cuenta de bitcoin) para recuperar el acceso

Ejemplo

El ransomware “WannaCry” afectó hospitales, empresas y universidades en más de 150 países.
Secuestró datos críticos, y muchos no pudieron recuperarlos.
Pagar el rescate **NO garantiza** que recuperarás tus archivos.

¿Cómo prevenirlo?

- Tener respaldos automáticos y en la nube
- No abrir archivos ZIP o EXE que no esperas
- No usar equipos sin antivirus en redes públicas
- Aplicar parches de seguridad (actualizaciones del sistema)

Ingeniería Social

Es el conjunto de técnicas psicológicas que un atacante utiliza para manipular a una persona y lograr que esta entregue información o acceda a sistemas sin darse cuenta.

¿Cómo funciona?

Porque explota comportamientos humanos comunes como:

- La confianza
- El miedo
- El deseo de ayudar
- La urgencia

Ejemplo

- Llamada falsa de “soporte técnico” pidiéndote tu contraseña
- Persona disfrazada de mensajero que accede al edificio sin control
- Alguien que finge necesitar ayuda para entrar a una sala restringida

¿Cómo prevenirlo?

- No entregar información sensible por teléfono, email o redes sociales
- Verificar la identidad antes de actuar
- Desconfiar de urgencias no confirmadas
- Reportar comportamientos sospechosos

Analogía: Es como un ladrón que se disfraza de plomero para entrar a tu casa, sin romper nada. En vez de vulnerar un sistema, vulnera **a la persona**.

Ataques combinados

Los atacantes combinan amenazas para lograr su objetivo. Por ejemplo:

- Envían un correo falso (phishing)
- El usuario hace clic → descarga un troyano
- El troyano abre la puerta para instalar ransomware
- Se bloquea todo el sistema y se pide rescate

Ejercicio 2: Caso aplicado

Situación: Recibes una llamada de alguien que dice ser del área de TI y te pide tu contraseña.

Pregunta

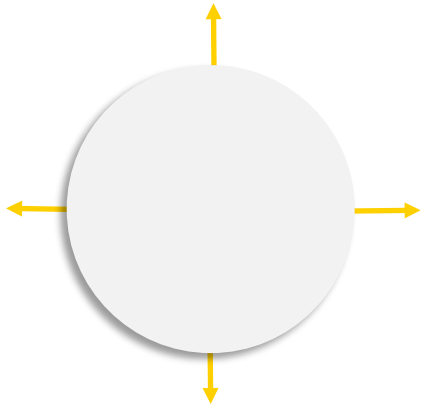
¿Qué harías?
¿Qué tipo de amenaza es?

¿Qué significa “Cultura de Seguridad”?

La cultura de seguridad de la información es el reflejo de cómo las personas entienden, valoran y actúan frente a la protección de los datos y recursos tecnológicos. Implica no solo conocer normas y herramientas, sino **adoptar una mentalidad proactiva y responsable** sobre lo que hacemos con la información.

¿Por qué es relevante?

Porque el eslabón más débil en la ciberseguridad no es la tecnología: **somos las personas.**



Una empresa puede tener políticas perfectas en papel, pero si sus colaboradores no las aplican, son ineficaces.

95% de los incidentes de ciberseguridad están relacionados con errores humanos (según IBM, 2022).

Componentes de una Cultura de Seguridad

Componente	Explicación	Ejemplo aplicado
Conciencia	Reconocer que la seguridad es importante y que los riesgos existen.	Saber que una USB desconocida puede contener virus.
Conocimiento	Saber cómo identificar y reaccionar ante una amenaza.	Ver un correo sospechoso y no hacer clic.
Actitudes	Tener disposición a actuar con cautela, sin subestimar los riesgos.	No compartir la contraseña con un compañero.
Práctica	Aplicar comportamientos seguros como hábito.	Usar contraseña diferente para cada cuenta.
Responsabilidad colectiva	Entender que todos somos responsables de la seguridad, no solo TI.	Informar si se detecta una anomalía en la red.

¿Cómo se construye una Cultura de Seguridad?

Se construye con acciones constantes, no con una charla aislada. **Ejemplos:**

Capacitación periódica

Talleres, videos, boletines.

Ejemplos visibles

Que los líderes practiquen y promuevan comportamientos seguros.

Refuerzo positivo

Reconocer buenas prácticas.

Políticas claras

Guías fáciles de entender, no documentos técnicos complejos.

Buenas Prácticas Digitales

(para la vida diaria y el trabajo)

Se construye con acciones constantes, no con una charla aislada. **Ejemplos:**

Contraseñas

Evita

123456, contraseña, tu nombre o fecha de nacimiento.

Usa frases

“MiPerroCome#1KiloDe Carne” es segura y fácil de recordar.

Nunca la reutilices

Cada servicio debe tener su clave única.

Gestores de contraseñas

Herramientas como Bitwarden o KeePass ayudan a generar y guardar contraseñas seguras.

Buenas Prácticas Digitales

(para la vida diaria y el trabajo)

Se construye con acciones constantes, no con una charla aislada. **Ejemplos:**

Doble autenticación (MFA)

Combina algo que sabes (clave) + algo que tienes (SMS, app de autenticación).

Incluso si te roban la clave, el atacante no podrá entrar sin el segundo factor.

Buenas Prácticas Digitales

(para la vida diaria y el trabajo)

Se construye con acciones constantes, no con una charla aislada. **Ejemplos:**

Navegación segura

- Sitios web confiables comienzan con **https**.
- Evita redes Wi-Fi abiertas sin protección (ej. en centros comerciales).
- Desconfía de ventanas emergentes o mensajes tipo “¡Felicidades! Has ganado…”

Buenas Prácticas Digitales

(para la vida diaria y el trabajo)

Se construye con acciones constantes, no con una charla aislada. **Ejemplos:**

Actualizaciones y parches

Las actualizaciones corrigen errores y cierran puertas que usan los atacantes.

No postergues la actualización del sistema operativo o el antivirus.

Buenas Prácticas Digitales

(para la vida diaria y el trabajo)

Se construye con acciones constantes, no con una charla aislada. **Ejemplos:**

Copias de seguridad

Respalda tu información personal: fotos, documentos, trabajo.

Puedes usar almacenamiento en la nube (Google Drive, OneDrive) o discos externos.

Buenas Prácticas Digitales

(para la vida diaria y el trabajo)

Se construye con acciones constantes, no con una charla aislada. **Ejemplos:**

Cuidado con la información que compartes

Todo lo que publicas en redes puede ser usado por atacantes para suplantarte.

Ej.: mostrar la cédula, boletos de avión, ubicación en tiempo real, datos bancarios.

Evita retos virales donde se expone información personal (nombre de tu mascota + año de nacimiento, etc.).

Prácticas en entornos organizacionales

En una empresa, universidad o institución, la cultura de seguridad debe ser una política transversal, no algo exclusivo del área de TI.

¿Qué se espera de cada área?

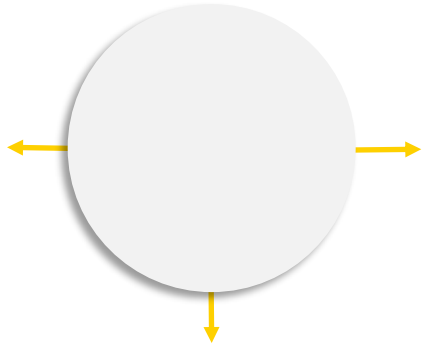
Área	Rol en la seguridad
Dirección	Establecer políticas, promover el ejemplo
Administrativos	Gestionar documentos e información con controles de acceso
Estudiantes/Empleados	Cumplir las normas y reportar anomalías
Soporte TI	Aplicar controles técnicos, monitorear la red
Comunicaciones	Asegurar el uso responsable de canales digitales

Prácticas en entornos organizacionales

En una empresa, universidad o institución, la cultura de seguridad debe ser una política transversal, no algo exclusivo del área de TI.

Política de uso aceptable

Todo entorno laboral debe contar con una política de “Uso Aceptable de Recursos”, que cubra aspectos como:



- Qué está permitido y qué no en el uso del correo, internet, dispositivos USB.
- Protocolos de respuesta ante incidentes.
- Normas sobre el uso de redes sociales desde el trabajo.

Conductas de riesgo que debilitan la cultura de seguridad

Conducta insegura	Consecuencia
Anotar la clave en un post-it	Cualquiera puede acceder
Dejar la sesión abierta al irse del escritorio	Robo de información
Enviar archivos sensibles por WhatsApp	No hay cifrado ni control
Ignorar alertas del antivirus	Riesgo de malware activo
Reírse del phishing porque “eso no me pasa”	Vulnerabilidad por exceso de confianza

Incluso si no trabajas en una empresa o institución, como ciudadano digital tienes responsabilidades

Enseñar a niños y mayores sobre seguridad básica.

Fomentar un entorno digital respetuoso y seguro.

Rol ciudadano en la era digital

Verificar noticias antes de compartir (evitar desinformación).

Denunciar fraudes o delitos cibernéticos.

Ejercicio 3: Política personal de seguridad

A partir de lo aprendido en el módulo, redacta una política personal de seguridad digital en la que especifiques al menos cinco compromisos o prácticas que aplicarás en tu vida diaria (como estudiante, trabajador o ciudadano digital).Puedes usar la plantilla entregada o escribirla desde cero, pero asegúrate de que sea concreta, realista y aplicable.

Referencias

1. Bishop, M. (2003). *Computer Security.*
2. Briceño, E. (2021). *Seguridad De La Información*
3. Kremer, E. Et al. (2019). *Ciberseguridad*
4. Ozkaya, E. (2019). *Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity*
5. Conficker, el gusano por el que Windows ofreció una millonaria recompensa. (s/f). Eset.com. Recuperado el 15 de agosto de 2025, de https://www.eset.com/latam/blog/cultura-y-seguridad-digital/conficker-el-gusano-por-el-que-windows-ofrecio-una-millonaria-recompensa/
6. Onuma. (2015, febrero 24). Superfish: adware preinstalado en los portátiles de Lenovo. Kaspersky. https://www.kaspersky.es/blog/superfish-adware-preinstalado-en-los-portatiles-de-lenovo/5437/
7. Panda Security. (2013, octubre 18). Los virus más famosos de la historia: Melissa. Panda Security Mediacenter. https://www.pandasecurity.com/es/mediacenter/virus-melissa/
8. Quiocho, C. (2024, noviembre 14). ¿Qué es el virus Melissa? Ninjaone.com. https://www.ninjaone.com/es/it-hub/endpoint-security/virus-melissa/
9. Zeus: El malware troyano. (2017, diciembre 7). /. https://latam.kaspersky.com/resource-center/threats/zeus - virus?srsltid=AfmBOopa8AQqDR5p7bSZ6piq0kJQfAgUu1G9pQuMWa3c0DL7A_2uq7gH
10. Zola, A., & Rosencrance, L. (2024, mayo 10). Pegasus malware. Search Security; TechTarget. https://www.techtarget.com/searchsecurity/definition/Pegasus-malware