



Universidad Tecnológica de Panamá
Facultad de Ingeniería de Sistemas Computacionales
Licenciatura en Desarrollo de Software



“Normas de Autoprotección”

Asignatura:

Seguridad en los Sistemas de Información

Integrantes:

Arcia, Raúl	2-753-1259
Medina, Johny	8-954-566
Rodríguez, Josué	8-986-1766

Profesora:

Oliva, Susan

Fecha:

15 de mayo del 2025

I SEMESTRE – 2025

Contenido	
INTRODUCCIÓN	ii
OBJETIVOS.....	iii
JUSTIFICACIÓN.....	iv
CONTENIDO.....	1
 ¿QUÉ SON LAS NORMAS DE AUTOPROTECCIÓN?	1
 Importancia en la Seguridad Informática:	1
 CONSECUENCIAS DE NO APLICAR LA AUTOPROTECCIÓN:.....	2
 EJEMPLOS BÁSICOS PERO CRUCIALES DE AUTOPROTECCIÓN:	5
 NORMAS Y BUENAS PRÁCTICAS DE AUTOPROTECCIÓN DIGITAL	8
 Educación Continua y Fomento de una Cultura de Seguridad:	12
 APLICACIÓN EN ENTORNOS ACADÉMICOS Y PROFESIONALES	12
 CONCLUSIONES Y RECOMENDACIONES	v
 INFOGRAFÍA	vii
 ANEXOS	ix

INTRODUCCIÓN

En la era digital actual, donde el acceso a la información es constante y cada vez más procesos se realizan de manera virtual, la seguridad de los datos y de los sistemas se ha convertido en una prioridad. Dentro de este amplio campo, uno de los aspectos más críticos es la participación de los usuarios en la protección de su propia información y la de las organizaciones a las que pertenecen. Las **normas de autoprotección** surgen precisamente como un conjunto de prácticas preventivas y hábitos conscientes que los individuos deben adoptar para reducir riesgos en entornos digitales.

Estas normas no solo tienen como objetivo evitar ataques o pérdidas de información, sino también fomentar una **cultura de seguridad informática**, donde cada usuario sea capaz de identificar amenazas, responder adecuadamente y contribuir a un ecosistema digital más seguro. La autoprotección se convierte así en un componente esencial dentro de la **Seguridad en los Sistemas de Información**, al ayudar a prevenir errores humanos, una de las principales causas de incidentes cibernéticos.

En este trabajo se abordarán los principales conceptos relacionados con la autoprotección en el ámbito de la seguridad informática, así como una serie de buenas prácticas recomendadas para preservar la seguridad personal y organizacional. También se explorará cómo estas normas se aplican en contextos académicos y laborales, con el fin de resaltar la importancia de formar usuarios conscientes, responsables y preparados para actuar frente a posibles amenazas en el entorno digital.

OBJETIVOS

Objetivo General

- Analizar la importancia y aplicación de las normas de autoprotección digital como parte fundamental de la seguridad en los sistemas de información, promoviendo una cultura de prevención ante amenazas cibernéticas.

Objetivos Específicos

- Identificar el concepto y la relevancia de la autoprotección en entornos digitales y su impacto en la seguridad informática.
- Describir las principales normas y buenas prácticas que deben aplicar los usuarios para proteger sus datos y dispositivos frente a riesgos comunes como el malware, phishing o accesos no autorizados.
- Explicar cómo se aplican las normas de autoprotección en contextos académicos y profesionales, destacando el papel del usuario responsable en la protección de la información institucional.
- Concientizar sobre las consecuencias de no adoptar medidas de autoprotección, como la pérdida de datos personales, suplantación de identidad y vulneración de sistemas.

JUSTIFICACIÓN

En la actualidad, vivimos en una sociedad cada vez más conectada, donde gran parte de nuestras actividades personales, académicas y profesionales dependen del uso de sistemas de información y tecnologías digitales. Esta creciente digitalización, si bien ofrece múltiples beneficios, también conlleva riesgos significativos para la seguridad de los datos y la privacidad de los usuarios. Las amenazas cibernéticas, como el robo de identidad, los ataques de malware, el phishing o los accesos no autorizados, se han vuelto más frecuentes y sofisticadas, afectando a individuos y organizaciones por igual.

Frente a este panorama, es indispensable que los usuarios desarrollen una actitud proactiva en la protección de la información, adoptando normas y buenas prácticas de autoprotección. Estas normas permiten reducir las vulnerabilidades humanas, que suelen ser el punto de entrada más común para los atacantes, y fortalecen la ciberseguridad en todos los niveles. Conocerlas y aplicarlas no solo protege los dispositivos y la información personal, sino que también contribuye a la seguridad general de las instituciones y redes a las que se pertenece.

Este trabajo resulta relevante porque busca promover la conciencia y responsabilidad en el uso de las tecnologías de información, fomentando la formación de usuarios informados y capaces de reconocer y responder adecuadamente ante amenazas digitales. Al comprender la importancia de la autoprotección, se fortalece la cultura de seguridad, elemento esencial en el desarrollo de sistemas de información seguros y confiables.

CONTENIDO

¿QUÉ SON LAS NORMAS DE AUTOPROTECCIÓN?

Las normas de autoprotección en el ámbito de la ciberseguridad se definen como un **conjunto integral de medidas, tanto preventivas como reactivas, que cada individuo o usuario debe conocer, comprender y aplicar diligentemente para resguardarse de los innumerables riesgos y amenazas inherentes al mundo digital**. Estos entornos digitales abarcan desde la navegación web cotidiana, el uso de redes sociales, la banca en línea, el correo electrónico, hasta plataformas educativas y sistemas de información corporativos.

Para la Seguridad en los Sistemas de Información, estas normas adquieren una relevancia crítica porque buscan **minimizar las vulnerabilidades humanas**. Es un hecho reconocido que, a menudo, el ser humano, por desconocimiento, descuido o susceptibilidad al engaño, se convierte en el eslabón más frágil de la cadena de seguridad. Los atacantes explotan la psicología humana a través de técnicas como la ingeniería social, donde manipulan a las personas para que revelen información confidencial o realicen acciones que comprometan su seguridad o la de su organización.

Importancia en la Seguridad Informática:

La trascendencia de la autoprotección en la seguridad informática es multifacética y fundamental:

1. **El usuario es frecuentemente el eslabón más débil:** A pesar de las robustas defensas tecnológicas que puedan existir, una gran proporción de las brechas de seguridad exitosas tienen su origen en una acción humana. Un simple clic en un enlace malicioso recibido por correo, la elección de una contraseña predecible y fácil de adivinar, o la pérdida física de un dispositivo sin las medidas de bloqueo adecuadas, pueden ser suficientes para desencadenar un incidente de seguridad con graves consecuencias.

2. **Mejora la ciberhigiene general:** La autoprotección fomenta y consolida **hábitos seguros y responsables** en el uso diario de la tecnología. La "ciberhigiene" se refiere a un conjunto de prácticas rutinarias, análogas a la higiene personal, que ayudan a mantener la salud y seguridad de los sistemas y la información. Esto incluye acciones como verificar la autenticidad de los remitentes de correo, ser cauto con las descargas, y mantener el software actualizado.
3. **Complementa indispensablemente las medidas técnicas:** Las organizaciones y los individuos pueden implementar herramientas de seguridad sofisticadas como firewalls (cortafuegos), sistemas de detección de intrusos, software antivirus y antimalware. Sin embargo, si el usuario final no posee una conciencia clara de los riesgos y no practica la autoprotección, estas defensas técnicas pueden ser eludidas o volverse ineficaces. Por ejemplo, un firewall no puede impedir que un usuario descargue voluntariamente un archivo infectado de un correo de phishing convincente.

CONSECUENCIAS DE NO APLICAR LA AUTOPROTECCIÓN:

La omisión o aplicación deficiente de las normas de autoprotección puede acarrear un abanico de consecuencias negativas, a menudo interconectadas:

- **Suplantación de Identidad (Phishing y Ataques de Ingeniería Social):**
 - Supongamos que un atacante, haciéndose pasar por una entidad legítima (un banco, una red social, un servicio técnico, o incluso un profesor o superior), podría engañarte para que reveles tus credenciales de acceso o información personal.
 - **Impacto Detallado:** Podrían acceder a tus plataformas académicas para alterar notas o entregar trabajos fraudulentos, usar tus redes sociales para difundir información falsa o estafar a tus contactos, o realizar transacciones no autorizadas desde tus cuentas bancarias. El uso indebido de tu nombre para enviar mensajes maliciosos o comprometedores puede dañar severamente tu reputación personal,

académica o profesional, con efectos que pueden ser difíciles de revertir.

- **Robo o Pérdida de Datos Personales y Sensibles:**

La falta de contraseñas robustas, la conexión a redes Wi-Fi inseguras sin protección, o la caída en trampas de malware pueden exponer tu información más íntima.

La Información crítica como tu número de cédula, dirección física, detalles bancarios completos, historial médico o académico, fotografías privadas, o propiedad intelectual, podría ser sustraída. Estos datos son altamente cotizados en el **mercado negro digital (Dark Web)**, donde se venden para cometer fraudes (apertura de créditos a tu nombre, compras fraudulentas), extorsión, o incluso para la creación de identidades falsas completas.

- **Infecciones por Malware (Software Malicioso) o Ransomware:**

Descargar un archivo de una fuente no confiable, hacer clic en un anuncio engañoso, o incluso visitar un sitio web comprometido puede introducir software dañino en tu dispositivo.

El **malware** puede tener múltiples propósitos: dañar archivos del sistema operativo, corromper o borrar tus documentos importantes (tesis, proyectos, recuerdos fotográficos), espiar tu actividad (spyware), o convertir tu equipo en un "zombi" para lanzar ataques a otros sistemas (botnets). El **ransomware**, una variante particularmente perniciosa, cifra todos tus archivos personales, volviéndolos inaccesibles, y los ciberdelincuentes exigen un rescate económico (generalmente en criptomonedas) para supuestamente devolverte el acceso, sin garantías de que cumplan su palabra tras el pago. Este tipo de infecciones pueden propagarse rápidamente a través de redes locales compartidas, como las de un laboratorio de computación universitario o la red Wi-Fi institucional, afectando a múltiples usuarios.

- **Acceso No Autorizado a Cuentas Sensibles y Críticas:**

El uso de contraseñas débiles o reutilizadas, o la falta de autenticación de dos factores, facilita que los atacantes tomen el control de tus perfiles en línea.

Perderías el control total sobre tus cuentas de correo electrónico (pudiendo interceptar comunicaciones importantes), plataformas educativas (comprometiendo tu progreso académico), redes sociales (afectando tu imagen pública), o servicios de almacenamiento en la nube (exponiendo archivos personales o laborales). Los intrusos podrían modificar o borrar registros académicos, tareas entregadas, proyectos colaborativos, o incluso robar archivos personales, fotografías, videos o documentos confidenciales almacenados en estas cuentas.

- **Pérdida Significativa de Tiempo y Productividad:**

Sufrir cualquiera de los incidentes anteriores inevitablemente conlleva una interrupción de tus actividades normales.

El proceso de identificar el problema, mitigar el daño, recuperar el acceso a cuentas comprometidas, restaurar datos desde copias de seguridad (si existen), y limpiar sistemas infectados puede consumir una cantidad considerable de tiempo y esfuerzo, extendiéndose por horas, días o incluso semanas. Esta dedicación forzada al incidente desvía la atención de tus responsabilidades académicas o laborales, afectando negativamente tu rendimiento y generando estrés.

- **Posibles Consecuencias Legales o Disciplinarias:**

Si a través de la negligencia en las prácticas de autoprotección se compromete información sensible perteneciente a una institución educativa o empresa.

Las universidades y empresas suelen tener políticas de seguridad de la información muy estrictas. Si una brecha de seguridad se origina o se facilita por un descuido (por ejemplo, compartiendo credenciales institucionales o introduciendo malware en la red corporativa), podría enfrentar sanciones

disciplinarias internas. En casos más graves, si se filtran datos protegidos por leyes de privacidad, podrás incluso incurrir en responsabilidades legales.

EJEMPLOS BÁSICOS PERO CRUCIALES DE AUTOPROTECCIÓN:

- 1. No compartir contraseñas, ni siquiera con amigos, compañeros o familiares:**

Cada cuenta es estrictamente personal e intransferible. Una contraseña es la llave a una identidad digital y a información. Aunque se confíe plenamente en la persona, compartir una contraseña diluye la responsabilidad. Si esa persona, por descuido o compromiso de su propia seguridad, expone esa contraseña, todas las cuentas vinculadas quedan vulnerables.

- 2. Evitar el uso de redes Wi-Fi públicas sin una Red Privada Virtual (VPN):**

Redes abiertas en cafeterías, aeropuertos, bibliotecas, hoteles o transporte público son inherentemente inseguras.

Estas redes a menudo carecen de cifrado robusto, lo que permite a atacantes en la misma red interceptar fácilmente el tráfico de datos que se envía y se recibe (incluyendo contraseñas, mensajes, o información de navegación). Esto se conoce como ataque "Man-in-the-Middle" (MitM). Una **VPN** crea un túnel cifrado y seguro entre el dispositivo e Internet, protegiendo los datos de miradas indiscretas incluso en redes no confiables.

- 3. Sospechar sistemáticamente de correos electrónicos no solicitados que contengan enlaces o archivos adjuntos:**

El phishing es una de las técnicas de ataque más comunes y efectivas. Los correos fraudulentos pueden ser muy convincentes, imitando la apariencia de comunicaciones legítimas de bancos, servicios de suscripción, instituciones educativas (profesores, administración) o incluso entidades gubernamentales.

Siempre se debe verificar la dirección completa del remitente (no solo el nombre que se muestra). Desconfiar de mensajes que crean un sentido de urgencia exagerado, soliciten información personal o pidan hacer clic en

enlaces sospechosos. Nunca se debe archivar adjuntos con extensiones ejecutables (.exe, .bat, .com), comprimidos (.zip, .rar si se los espera) o documentos de Office con macros habilitadas (.docm, .xlsm) sin confirmar verbalmente o por un canal alternativo y seguro la legitimidad del envío con el supuesto remitente.

4. Cerrar sesión correctamente en todas las plataformas al usar equipos compartidos o públicos:

Equipos en bibliotecas, laboratorios de informática, cibercafés, o cualquier dispositivo que no sea exclusivamente propio.

Simplemente cerrar la ventana del navegador no suele ser suficiente para cerrar la sesión. Si se deja una sesión activa, la siguiente persona que use el equipo podría acceder a esas cuentas, ver la información personal, enviar mensajes en nombre de otro o realizar otras acciones malintencionadas. Es recomendable también usar el **modo incógnito o privado** del navegador en estos equipos, ya que ayuda a no guardar historial, cookies o datos de sesión tras cerrarlo, y siempre finalizar cerrando todas las ventanas y pestañas.

5. Actualizar el sistema operativo, navegador web y todas las aplicaciones regularmente:

Los desarrolladores de software publican constantemente actualizaciones y parches.

Estas actualizaciones no solo introducen nuevas funcionalidades o mejoran el rendimiento, sino que, crucialmente, **corrigen vulnerabilidades de seguridad** que han sido descubiertas. Los cibercriminales están siempre al acecho de sistemas desactualizados para explotar estos fallos conocidos (a veces llamados "exploits de día cero" si se usan antes de que exista un parche, o "exploits de día-N" si se usan contra sistemas que no han sido parcheados). Mantener todo actualizado es una de las defensas más efectivas.

6. Evitar descargar e instalar software "pirata", "crackeado" o de fuentes desconocidas y no oficiales:

La tentación de obtener software de pago de forma gratuita puede ser alta. Estos programas modificados o distribuidos a través de canales no oficiales (sitios de torrents, foros dudosos) son un vehículo extremadamente común para la distribución de malware. A menudo, el software "gratuito" viene con troyanos, spyware, adware o incluso ransomware oculto. Utilizar siempre las **páginas oficiales de los desarrolladores** o las tiendas de aplicaciones verificadas (Google Play Store, Apple App Store, Microsoft Store) para las descargas.

7. Realizar copias de seguridad (backups) de forma periódica y sistemática:

Los archivos importantes (trabajos académicos, tesis, proyectos profesionales, fotografías, documentos personales) son valiosos.

Los dispositivos pueden fallar, ser robados, dañarse accidentalmente, o ser víctimas de ransomware. Sin una copia de seguridad reciente, toda esa información podría perderse irremediablemente. Es recomendable seguir la **regla 3-2-1**: al menos **tres** copias de tus datos, en **dos** tipos de almacenamiento diferentes, y al menos **una** copia fuera de la ubicación física principal (por ejemplo, un disco duro externo guardado en otro lugar y/o servicios de almacenamiento en la nube confiables y debidamente protegidos).

NORMAS Y BUENAS PRÁCTICAS DE AUTOPROTECCIÓN DIGITAL

PRINCIPALES NORMAS Y BUENAS PRÁCTICAS APLICABLES EN EL USO DE SISTEMAS DE INFORMACIÓN:

1. Contraseñas Seguras y Gestión Adecuada:

Las contraseñas son la primera línea de defensa para nuestras cuentas. Una contraseña "segura" no solo combina letras (mayúsculas y minúsculas), números y símbolos (!@#\$%^&*()), sino que también debe ser **larga** (mínimo 12-16 caracteres, idealmente más). Considerar usar **frases de contraseña** (una secuencia de palabras fácil de recordar para ti pero difícil de adivinar, ej: "MiPerroChocolateComio3Zanahorias!") en lugar de palabras complejas pero cortas.

Prácticas Clave:

- a. **Unicidad Absoluta:** Jamás utilices la misma contraseña, ni siquiera variaciones leves, en distintas plataformas. Si una cuenta se ve comprometida y reutilizas contraseñas, todas tus otras cuentas que usen esa misma credencial quedan instantáneamente vulnerables (esto se llama "credential stuffing").
- b. **Gestores de Contraseñas:** Utilizar un **gestor de contraseñas** (como Bitwarden, 1Password, KeePass) es altamente recomendable. Estas herramientas generan contraseñas muy fuertes y únicas para cada sitio, las almacenan de forma cifrada y las autocompletan, necesitando que solo recuerdes una contraseña maestra robusta.
- c. **Cambio Periódico Razonable:** Aunque la recomendación histórica era cambiar contraseñas muy frecuentemente, el énfasis actual está más en la fortaleza y unicidad. Cambia tus contraseñas importantes periódicamente (cada 3-6 meses) o inmediatamente si sospechas que una cuenta ha sido comprometida.
- d. **Confidencialidad Total:** Nunca compartir las contraseñas con nadie, ni por correo, ni por chat, ni verbalmente. Ninguna entidad legítima solicitará nuestra contraseña completa.

2. Actualización Constante y Oportuna de Software:

El ciclo de vida de una vulnerabilidad es crítico: un investigador o un actor malicioso la descubre, el proveedor desarrolla un parche, y los usuarios deben aplicarlo. Los atacantes explotan la "ventana de vulnerabilidad" entre el momento en que un parche está disponible y el momento en que el usuario lo instala.

- a. **Automatización:** Habilita las actualizaciones automáticas siempre que sea posible para tu sistema operativo, navegador web, antivirus y otras aplicaciones críticas.
- b. **Revisión Manual:** Para software que no se actualiza automáticamente, establece recordatorios para verificar e instalar actualizaciones manualmente de forma regular.
- c. **Software Obsoleto (End-of-Life):** Prestar especial atención al software que ya no recibe soporte ni actualizaciones de seguridad por parte del fabricante (conocido como "End-of-Life" o EOL). Usar software EOL es extremadamente arriesgado, ya que las vulnerabilidades descubiertas no serán corregidas.

3. Cifrado de Datos (Encriptación):

El cifrado transforma tus datos legibles en un formato codificado (texto cifrado) que solo puede ser descifrado y leído con la clave de cifrado correcta. Es una salvaguarda esencial incluso si tus datos son interceptados o robados.

Prácticas Clave:

- a. **Cifrado en Tránsito:** Asegurarnos de que las comunicaciones sensibles por internet usen HTTPS (el candado en el navegador). Utilizar aplicaciones de mensajería que ofrezcan cifrado de extremo a extremo (E2EE), como Signal o WhatsApp (en sus configuraciones por defecto para mensajes privados). Para correos sensibles, considerar herramientas de cifrado como PGP/GPG.

- b. **Cifrado en Reposo:** Habilitar el cifrado de disco completo en tus dispositivos (BitLocker en Windows, FileVault en macOS, opciones similares en Linux y móviles). Esto protege tus datos si nuestro dispositivo es perdido o robado. Si se utiliza almacenamiento en la nube, verificar las opciones de cifrado que ofrece el proveedor y considerar cifrar los archivos antes de subirlos para una mayor seguridad.

4. Uso Estratégico de Antivirus y Firewall:

Estas herramientas son componentes esenciales de una defensa en capas.

- a. **Antivirus/Antimalware:** Un software antivirus moderno no solo se basa en firmas de malware conocido (listas de virus identificados), sino que también utiliza análisis heurístico y basado en comportamiento para detectar amenazas nuevas o desconocidas.
- b. **Firewall (Cortafuegos):** Actúa como un filtro de tráfico de red, controlando las conexiones entrantes y salientes de tu dispositivo o red. Puede ser basado en software (instalado en PC) o en hardware (integrado en el router).

Prácticas Clave:

- c. **Antivirus de Reputación:** Elegir un producto antivirus de un proveedor reconocido y mantenerlo siempre actualizado (tanto el motor del programa como las definiciones de virus). Realizar escaneos completos del sistema periódicamente.
- d. **Configuración del Firewall:** Asegúrarse de que el firewall del sistema operativo esté activado. El firewall del router doméstico también debe estar habilitado y configurado correctamente (por ejemplo, cambiando las credenciales de administrador por defecto).

5. Implementación de la Autenticación de Dos Factores (2FA) o Múltiples Factores (MFA):

La 2FA/MFA añade una capa crítica de seguridad al proceso de inicio de sesión. Incluso si un atacante logra robar la contraseña (factor 1: algo que se sabe), necesitará un segundo factor para acceder a la cuenta.

Prácticas Clave:

a. Tipos de Segundo Factor:

- i. **Algo que se tiene:** Un código de un solo uso generado por una aplicación de autenticación (Google Authenticator, Authy, Microsoft Authenticator), un código enviado por SMS (aunque este método es considerado menos seguro que las apps debido al riesgo de SIM swapping), o una llave de seguridad física (YubiKey, Google Titan).
- ii. **Algo que se es:** Autenticación biométrica como huella dactilar, reconocimiento facial o de iris.

b. **Habilitación Universal:** Activar la 2FA en todas las cuentas que la ofrezcan, especialmente en las más críticas: correo electrónico principal, banca en línea, redes sociales, gestores de contraseñas y almacenamiento en la nube.

c. **Códigos de Recuperación:** Cuando se configure un 2FA, guardar los códigos de recuperación en un lugar muy seguro (preferiblemente offline), ya que permitan acceder a la cuenta si se pierde acceso al segundo factor.

Educación Continua y Fomento de una Cultura de Seguridad:

El panorama de ciberamenazas es dinámico y evoluciona constantemente. Lo que hoy es una práctica segura, mañana podría no serlo. La educación no es un evento único, sino un proceso continuo.

Prácticas Clave:

- d. **Mantenerse Informado:** Seguir fuentes confiables de noticias sobre ciberseguridad (blogs de empresas de seguridad, sitios web de agencias gubernamentales de ciberseguridad como INCIBE en España o CISA en EE.UU., o equivalentes al país).
- e. **Reconocer Nuevas Amenazas:** Aprender a identificar las tácticas más recientes de phishing, los tipos emergentes de malware y las nuevas técnicas de ingeniería social.
- f. **Compartir Conocimiento:** Fomentar una cultura de autoprotección dentro de tu círculo (familia, amigos, compañeros de estudio o trabajo). Compartir buenas prácticas y alertar sobre posibles amenazas ayuda a reducir el riesgo colectivo. Las organizaciones deben invertir en programas de concienciación y capacitación regulares para sus empleados.

APLICACIÓN EN ENTORNOS ACADÉMICOS Y PROFESIONALES

La aplicación de normas de autoprotección en contextos universitarios y laborales es especialmente crítica debido al valor y la sensibilidad de la información que se maneja, así como a las regulaciones y políticas internas que deben cumplirse.

Autoprotección en Universidades y Centros Laborales:

1. Correo Institucional (Académico o Corporativo):

El correo institucional es un canal oficial y, por ende, un objetivo primordial para los atacantes que buscan acceder a información confidencial o infiltrarse en las redes de la organización. Los ataques de **spear phishing** (phishing dirigido y personalizado) son comunes, donde los correos parecen provenir de colegas, superiores, o departamentos internos.

Prácticas Esenciales:

- a. **Verificación Rigurosa del Remitente:** No confiar ciegamente en el nombre que se muestra. Examinar detenidamente la dirección de correo electrónico completa. Desconfiar de dominios ligeramente alterados (ej: universidad-soporte.com en lugar de soporte.universidad.edu).
- b. **Cautela Extrema con Enlaces y Adjuntos:** Antes de hacer clic en un enlace, pasar el cursor sobre él para previsualizar la URL real. Si es sospechosa o no coincide con lo esperado, no hacer clic. No abrir archivos adjuntos inesperados, incluso si parecen provenir de un contacto conocido (su cuenta podría haber sido comprometida). Confirmar por un canal alterno (llamada telefónica, mensaje directo) si se tiene dudas.
- c. **Reporte de Correos Sospechosos:** Utilizar las herramientas o procedimientos que la institución provea para reportar correos de phishing al departamento de TI o seguridad.

2. Acceso a Plataformas Educativas y Sistemas Corporativos (Moodle, SIU, ERPs, CRMs, etc.):

Estas plataformas almacenan datos críticos: calificaciones, expedientes académicos, información personal de estudiantes y empleados, datos financieros, proyectos de investigación, propiedad intelectual de la empresa, etc. El acceso no autorizado puede tener consecuencias devastadoras.

Prácticas Esenciales:

- a. **Cierre de Sesión Sistemático:** Siempre cerrar sesión explícitamente al terminar de usar estas plataformas, especialmente en dispositivos compartidos o públicos. El simple cierre de la pestaña o del navegador puede no invalidar la sesión, dejando los datos expuestos al siguiente usuario.
- b. **Precaución en Dispositivos Públicos:** Evitar en lo posible acceder a estas plataformas desde cibercafés o computadoras de acceso

- público. Si es inevitable, utilizar el modo de navegación privada/incógnito, no permitir que el navegador guarde las credenciales y asegúrese de cerrar sesión y limpiar el historial/cookies (si es posible y permitido) al finalizar.
- c. **Conciencia de las Cookies de Sesión:** Tener en cuenta que las "session cookies" pueden mantener la sesión activa. El cierre adecuado de sesión las invalida.

3. **Seguridad de Dispositivos Personales (Laptops, Smartphones, Tablets) usados para fines académicos o laborales (Contexto BYOD - Bring Your Own Device):**

Cada vez es más común usar dispositivos personales para el trabajo o el estudio. Esto introduce riesgos adicionales, ya que la seguridad de estos dispositivos puede no estar al mismo nivel que los gestionados por la institución.

Prácticas Esenciales:

- a. **Bloqueo Robusto del Dispositivo:** Configurar un mecanismo de bloqueo fuerte: un PIN complejo (no fechas de nacimiento o secuencias obvias), una contraseña alfanumérica, o métodos biométricos (huella dactilar, reconocimiento facial). Configurar el bloqueo automático tras un corto periodo de inactividad.
- b. **Cifrado del Dispositivo:** Habilitar el cifrado de disco completo en laptops y el cifrado de almacenamiento en dispositivos móviles.
- c. **Software de Seguridad Móvil:** Considerar instalar software de seguridad en tus smartphones y tablets.
- d. **Copias de Seguridad (Backups) de Información Crítica:** Regularmente respaldar la información importante almacenada en estos dispositivos, ya sea relacionada con estudios o trabajo.
- e. **Conexiones Seguras:** Utilizar VPNs si se accede a recursos institucionales sensibles desde redes no confiables.

- f. **Cuidado con Apps Instaladas:** Descargar aplicaciones solo de tiendas oficiales y revisa los permisos que solicitan.

4. **El Rol Fundamental del Usuario Responsable y Consciente:**

La seguridad no es solo responsabilidad del departamento de TI; cada usuario tiene un papel activo que desempeñar en la protección de la información y los sistemas. Una cultura de seguridad robusta se basa en la colaboración y la proactividad de todos.

Prácticas Esenciales:

- a. **Reporte Inmediato de Incidentes:** Si se detecta actividad sospechosa (intentos de inicio de sesión fallidos en cuentas que no realizaste, correos extraños, comportamiento anómalo del sistema, posible brecha de seguridad), reportarlo inmediatamente al departamento de soporte técnico o seguridad informática de la institución. Una notificación temprana puede marcar la diferencia en la contención de un incidente.
- b. **No Compartir Credenciales Institucionales:** Las credenciales de acceso (nombre de usuario y contraseña) son personales e intransferibles. No se deben compartir bajo ninguna circunstancia, ni con compañeros, ni con amigos, ni siquiera si alguien que se identifica como del soporte técnico y las pide de forma no habitual (el soporte legítimo raramente necesita la contraseña).
- c. **Adherencia a las Políticas de Uso Aceptable:** Familiarizarse y cumplir con las políticas de uso de los recursos tecnológicos de la institución.

5. **Alineación y Comprensión de las Políticas Institucionales de Seguridad:**

Las normas de autoprotección individual no existen en el vacío; están intrínsecamente ligadas y deben estar en consonancia con las **políticas de seguridad de la información** establecidas por la universidad o la empresa. Estas políticas son el marco formal que guía la protección de los activos de información.

Prácticas Esenciales:

- a. **Conocimiento de las Políticas:** Informarse sobre las políticas de seguridad de la institución. Estas suelen cubrir áreas como el uso de contraseñas, el manejo de datos confidenciales, el uso del correo electrónico, el acceso remoto, la respuesta a incidentes, etc.
- b. **Comprendión de los Principios CIA:** Las políticas de seguridad buscan garantizar la **Confidencialidad** (que la información solo sea accesible por personal autorizado), la **Integridad** (que la información sea precisa, completa y no haya sido modificada sin autorización) y la **Disponibilidad** (que la información y los sistemas estén accesibles para los usuarios autorizados cuando los necesiten). Las acciones de autoprotección contribuyen directamente a mantener estos tres pilares.
- c. **Participación Activa:** Al cumplir con las normas de autoprotección y las políticas institucionales, no solo se protege a uno mismo, sino que también se fortalece la postura de seguridad general de la organización, reduce los riesgos colectivos y promueve una cultura digital más madura y segura para todos sus miembros.

CONCLUSIONES Y RECOMENDACIONES

 **Raúl Arcia**

Conclusión:

Comprender el concepto de autoprotección dentro del ámbito de la seguridad en los sistemas de información es fundamental para reconocer que la mayoría de las amenazas no solo se originan en errores tecnológicos, sino también en fallos humanos. La autoprotección comienza con la conciencia de los riesgos digitales y la necesidad de adoptar hábitos preventivos como una responsabilidad individual.

Recomendación:

Se recomienda fomentar la educación digital desde etapas tempranas, tanto en entornos académicos como personales, para que las personas interioricen las normas básicas de autoprotección y las apliquen de manera constante en su vida diaria.

 **Josué Rodríguez**

Conclusión:

Las normas y buenas prácticas de autoprotección digital son herramientas esenciales para prevenir accesos no autorizados, robo de información y otras amenazas informáticas. La implementación de contraseñas seguras, actualizaciones constantes, uso de antivirus y cifrado de datos forman una primera línea de defensa ante los ciberataques.

Recomendación:

Se recomienda integrar estas buenas prácticas dentro de políticas institucionales de uso de tecnologías, promover talleres periódicos de formación en seguridad digital y evaluar continuamente los hábitos de los usuarios para fortalecer sus competencias digitales.

 **Johny Medina****Conclusión:**

La autoprotección no solo es necesaria en el ámbito personal, sino también en los contextos académicos y profesionales, donde el uso de sistemas de información es diario y constante. La prevención de amenazas depende directamente del compromiso del usuario con el uso responsable de plataformas, dispositivos y datos.

Recomendación:

Se recomienda establecer protocolos claros en instituciones educativas y laborales sobre el uso seguro de herramientas tecnológicas, promover la denuncia de actividades sospechosas y reforzar la importancia de respetar las políticas de seguridad institucionales.

INFOGRAFÍA

- Datos101. (2023). *Medidas de seguridad informática*. Recuperado el 11 de mayo de 2025, de <https://www.datos101.com/blog/medidas-de-seguridad-informatica/>
- Fleet. (2025). *Normas de ciberseguridad: las herramientas que necesita para cumplirlas*. Recuperado el 12 de mayo de 2025, de <https://fleet.co/es/blog/normas-de-ciberseguridad%3A-las-herramientas-que%20necesita-para-cumplirlas%20>
- FTC (Comisión Federal de Comercio). (2025). *Marco de ciberseguridad NIST*. Recuperado el 11 de mayo de 2025, de <https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist>
- Quirón Prevención. (2020). *Daños a la salud por exposición a pantallas y equipos informáticos*. Recuperado el 13 de mayo de 2025, de <https://www.quironprevencion.com/blogs/es/prevenidos/danos-salud-exposicion-pantallas-equipos-informaticos>
- Red Seguridad. (2023, septiembre 8). *Diferencias entre vulnerabilidad, amenaza y riesgo en seguridad TI*. Recuperado el 13 de mayo de 2025, de https://www.redseguridad.com/actualidad/diferencias-vulnerabilidad-amenaza-riesgo-seguridad-ti_20230908.html
- Right People Group. (2025). *5 consecuencias devastadoras de ignorar la gestión de riesgos informáticos (con ejemplos reales)*. Recuperado el 11 de mayo de 2025, de <https://rightpeoplegroup.com/es/blog/5-consecuencias-devastadoras-de-ignorar-la-gestion-de-riesgos-informaticos-con-ejemplos-reales>
- UDEst Istmo. (2022). *10 consejos para proteger tu información en Internet*. Recuperado el 11 de mayo de 2025, de <https://www.udelistmo.edu/blogs/10-consejos-para-proteger-tu-informacion-en-internet>
- UNIR Formación Profesional. (2025). *Principios básicos de la seguridad informática*. Recuperado el 11 de mayo de 2025, de

<https://unirfp.unir.net/revista/ingenieria-y-tecnologia/principios-seguridad-informatica/>

- esedsl. (2025). *¿Qué normativas de ciberseguridad debe cumplir tu empresa?* Recuperado el 13 de mayo de 2025, de <https://www.esedsl.com/blog/que-normativas-de-ciberseguridad-debe-cumplir-tu-empresa>

ANEXOS

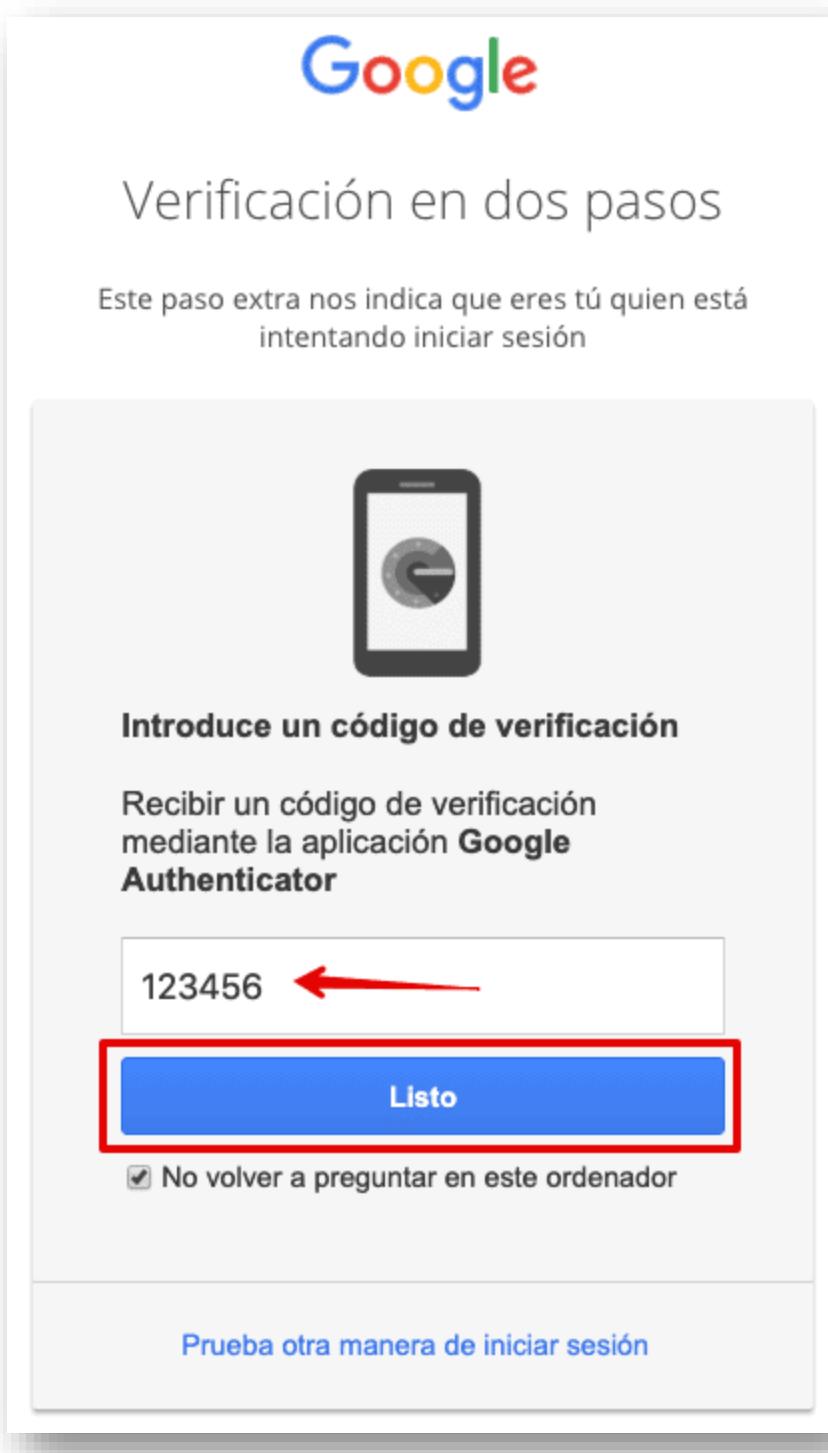
- **Ejemplo visual de un correo phishing**



- **Cuadro comparativo de herramientas de seguridad**

Herramienta	Función principal	Ejemplo recomendado
Antivirus	Detección y eliminación de malware	Avast, Bitdefender
VPN	Protección en navegación	NordVPN, ProtonVPN
Gestor de contraseñas	Almacén seguro de claves	LastPass, Bitwarden
Firewall	Bloqueo de accesos no autorizados	ZoneAlarm, Comodo
Autenticación 2FA	Verificación adicional de identidad	Google Authenticator, Authy

- Pantalla de activación del 2FA en una cuenta de Google



[x]

- Generador de contraseña segura.

The screenshot shows the LastPass password generator interface. At the top, it says "LastPass •••" and "HERRAMIENTA DE GENERACIÓN DE CONTRASEÑAS". Below that, a large heading says "Genere una contraseña segura". A sub-instruction reads: "Utilice nuestro generador de contraseñas en línea para crear de forma instantánea una contraseña aleatoria y segura." A generated password "832*ZbhNnc0I" is displayed in a text input field with copy and refresh icons. Below this, a section titled "Personalice su contraseña" allows users to adjust settings. It includes a slider for "Longitud de la contraseña" set to 12, and three radio button options: "Fácil de decir", "Fácil de leer", and "Todos los caracteres", with the last one being selected. To the right, four checkboxes are checked: "Mayúsculas", "Minúsculas", "Números", and "Símbolos". Red arrows point from the text labels to their corresponding checked boxes. At the bottom is a red "Copiar contraseña" button.