Seguridad digital y autonomía responsable

En el mundo digital actual, cada vez más interconectado, nuestra seguridad y autonomía se vuelven aspectos cruciales. La seguridad digital, definida como la protección de nuestros datos, dispositivos y privacidad online, es fundamental para mantener el control sobre nuestra vida digital y evitar caer víctimas de amenazas cibernéticas.

La autonomía responsable en el ámbito digital implica ser conscientes de las vulnerabilidades del entorno digital, adoptar buenas prácticas de seguridad informática y estar preparados para afrontar los desafíos que plantean los ciberdelitos. Esta presentación explorará estos temas en profundidad, ofreciendo consejos prácticos y herramientas para que puedas navegar por el ciberespacio de forma segura y autónoma.

Ing. Elba María Bodero Poveda, PhD.

Vulnerabilidades en el entorno digital

1 **Software desactualizado**

Los sistemas operativos, programas y aplicaciones desactualizados pueden contener vulnerabilidades conocidas que los hackers pueden aprovechar para acceder a tus datos.

2 **Conexiones Wi-Fi públicas**

Las redes Wi-Fi públicas, como las que se encuentran en cafés o aeropuertos, suelen ser menos seguras. Es importante evitar realizar transacciones financieras o acceder a información confidencial en estas redes.

3 **Phishing**

Los ataques de phishing son intentos de engañarte para que reveles información personal o financiera. Pueden presentarse en forma de correos electrónicos, mensajes de texto o páginas web falsas.

4 **Falta de conciencia**

La falta de conciencia sobre las amenazas digitales y las buenas prácticas de seguridad informática es una de las principales causas de vulnerabilidad.

Amenazas cibernéticas: Tipos y tendencias

Malware

Software malicioso diseñado para dañar tu dispositivo, robar información o controlar tu sistema.

Ransomware

Un tipo de malware que bloquea el acceso a tus archivos y exige el pago de un rescate para recuperarlos.

Ataques DDoS

Ataques de denegación de servicio que saturan un servidor con tráfico artificial para dejarlo inaccesible.

Buenas prácticas de seguridad informática

1. **Mantén tu software actualizado**
   Las actualizaciones de software suelen incluir parches de seguridad que corrigen vulnerabilidades conocidas.

2. **Usa contraseñas seguras**
   Crea contraseñas fuertes y únicas para cada cuenta. Evita utilizar palabras fáciles de adivinar o información personal.

3. **Habilita la autenticación de dos factores**
   La autenticación de dos factores (2FA) agrega una capa adicional de seguridad al requerir que ingreses un código único generado por tu dispositivo móvil o correo electrónico.

4. **Ten cuidado con los enlaces y archivos adjuntos**
   No hagas clic en enlaces sospechosos o abras archivos adjuntos de remitentes desconocidos, ya que podrían contener malware.

5. **Instala un antivirus y un firewall**
   Un antivirus detecta y elimina malware, mientras que un firewall bloquea el acceso no autorizado a tu dispositivo.

6. **Realiza copias de seguridad de tus datos**
   Las copias de seguridad regulares te ayudan a recuperar tus datos en caso de pérdida o daño.

Gestión de contraseñas y autenticación

Utiliza un administrador de contraseñas

Los administradores de contraseñas almacenan todas tus contraseñas en un lugar seguro y te permiten acceder a ellas desde cualquier dispositivo.

Crea contraseñas complejas

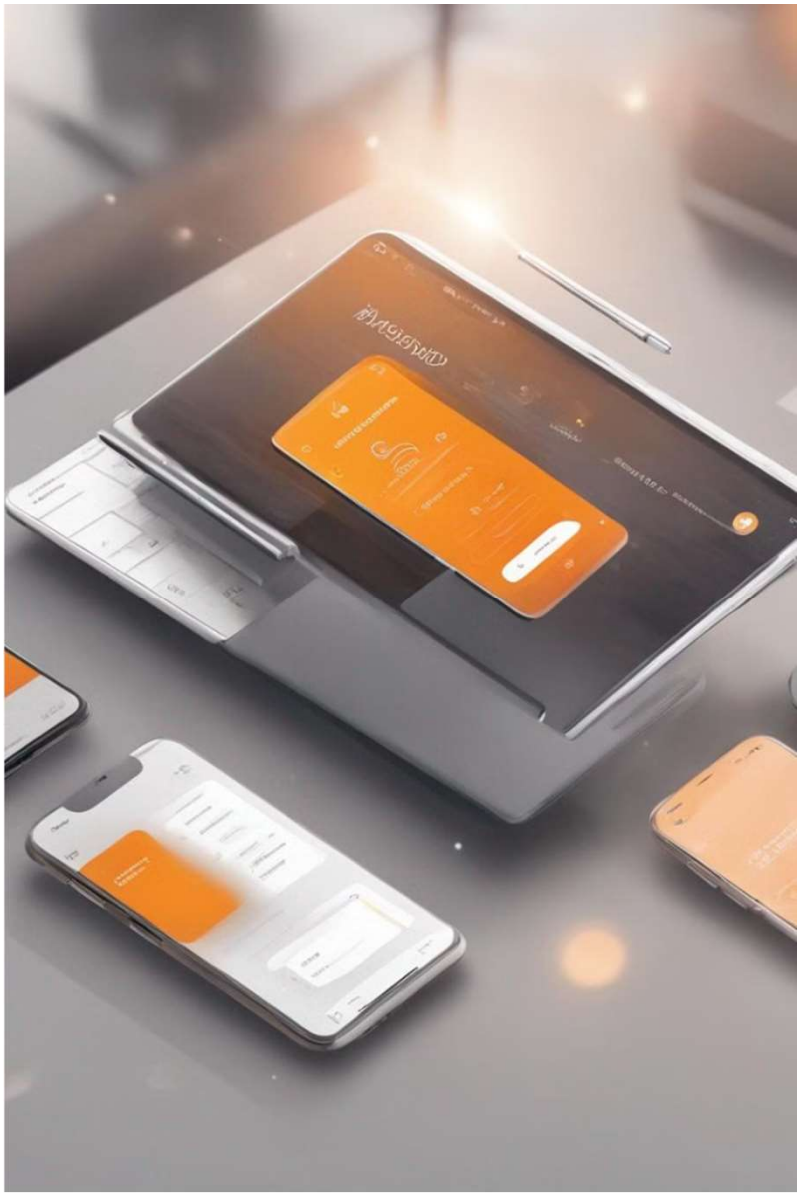
Utiliza una combinación de letras mayúsculas y minúsculas, números y símbolos para crear contraseñas difíciles de adivinar.

Evita usar la misma contraseña para varias cuentas

Si una contraseña se ve comprometida, todos tus otros sitios web podrían ser vulnerables.

Habilita la autenticación de dos factores

La autenticación de dos factores agrega una capa adicional de seguridad al requerir que ingreses un código único generado por tu dispositivo móvil o correo electrónico.



Protección de datos y privacidad

1

Lee las políticas de privacidad

Antes de proporcionar información personal, lee las políticas de privacidad de los sitios web y aplicaciones para comprender cómo se recopilan, usan y comparten tus datos.

2

Controla la configuración de privacidad

Configura la configuración de privacidad de tus cuentas en redes sociales, sitios web y aplicaciones para limitar la información que compartes y la cantidad de anuncios personalizados que ves.

3

Usa una VPN

Una VPN cifra tu conexión a internet y protege tu privacidad mientras navegas en redes Wi-Fi públicas o accedes a sitios web que no están seguros.

4

Sé consciente del seguimiento

Muchos sitios web y aplicaciones utilizan cookies para rastrear tu actividad en línea. Considera usar un bloqueador de anuncios para evitar que estas cookies recopilen información sobre ti.

Navegación segura en internet

Verifica la seguridad de los sitios web

Asegúrate de que el sitio web que estás visitando es seguro al verificar que la dirección URL comienza con "https" y que hay un candado en la barra de direcciones.

Evita descargar archivos de fuentes desconocidas

Los archivos descargados de fuentes sospechosas pueden contener malware o virus.

Ten cuidado con los mensajes sospechosos

No hagas clic en enlaces o abras archivos adjuntos de remitentes desconocidos.

Busca información confiable

Verifica la información que encuentras en línea en fuentes confiables, como sitios web oficiales o publicaciones académicas.

Ciberdelitos: Definición y consecuencias

Tipo de ciberdelito	Descripción	Consecuencias
Robo de identidad	El robo de información personal, como números de tarjetas de crédito o datos bancarios.	Pérdida financiera, daños a la reputación y problemas legales.
Extorsión	Amenazas para causar daño a tu dispositivo o datos a cambio de un pago.	Pérdida financiera, daños a la reputación y pérdida de datos.
Ataques de denegación de servicio (DDoS)	Ataques que saturan un servidor con tráfico artificial para dejarlo inaccesible.	Pérdida de ingresos, daños a la reputación y pérdida de clientes.

Herramientas y recursos para la ciberseguridad

1 **Software antivirus**

Protege tu dispositivo contra malware, virus y otras amenazas.

2 **Firewall**

Bloquea el acceso no autorizado a tu dispositivo y protege tu información personal.

3 **Administrador de contraseñas**

Almacena todas tus contraseñas en un lugar seguro y te permite acceder a ellas desde cualquier dispositivo.

4 **VPN**

Cifra tu conexión a internet y protege tu privacidad mientras navegas en redes Wi-Fi públicas o accedes a sitios web que no están seguros.

Conclusión y recomendaciones finales

En un mundo digital cada vez más complejo, la seguridad y la autonomía responsables son cruciales para protegernos de las amenazas cibernéticas. La falta de conciencia sobre los riesgos digitales y las buenas prácticas de seguridad informática nos hace más vulnerables a los ataques.

Es importante estar al tanto de las nuevas amenazas y tecnologías, y adaptar nuestras prácticas de seguridad en consecuencia. Al adoptar medidas preventivas y utilizar las herramientas y recursos disponibles, podemos navegar por el ciberespacio de forma segura y autónoma, manteniendo el control sobre nuestra vida digital y protegiendo nuestra privacidad.

Seguridad digital y autonomía responsable

Ing. Elba María Bodero Poveda, PhD.