Conceptos de Ciberseguridad

Guia de estudio para comprender como proteger informacion, cuentas, dispositivos y sistemas digitales.

Recurso descargable

Este PDF complementa el recurso web de ByteNova con explicaciones ampliadas, ejemplos y diagramas para estudiantes, jovenes y personas que estan comenzando en seguridad digital.

La meta no es memorizar terminos, sino comprender habitos y conceptos que ayudan a reducir riesgos en la vida digital diaria.

Contenido	Aprenderas
Fundamentos	Confidencialidad, integridad y disponibilidad
Amenazas comunes	Phishing, malware, robo de cuentas y errores humanos
Buenas practicas	Contrasenas, MFA, actualizaciones, copias y privacidad
Checklist final	Acciones para estudiar y aplicar desde hoy

1. ¿Que es la ciberseguridad?

La ciberseguridad es el conjunto de practicas, procesos, herramientas y conocimientos que ayudan a proteger la informacion y los sistemas digitales frente a riesgos como robo de datos, accesos no autorizados, perdida de archivos o interrupciones de servicios.

En palabras sencillas, la ciberseguridad busca que una cuenta, un dispositivo, una red o una pagina web se mantengan protegidos y disponibles para quienes realmente deben usarlos.

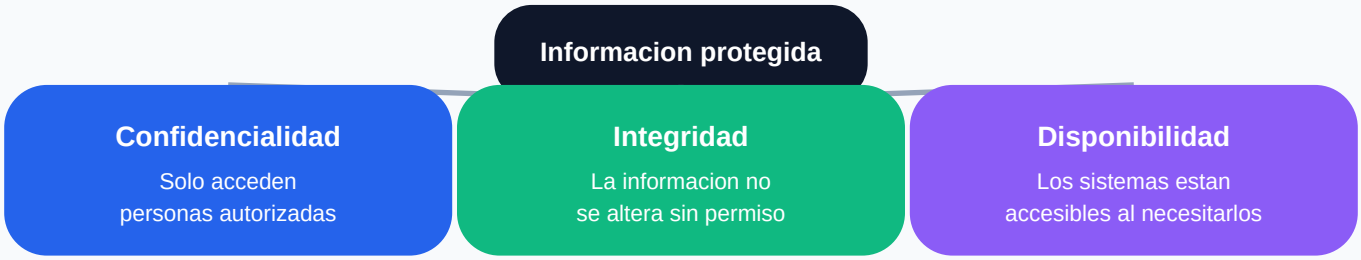
No es solo para expertos

Muchas personas creen que la seguridad digital solo pertenece a empresas o especialistas. En realidad, cualquier persona que use internet necesita habitos basicos de proteccion: estudiantes, trabajadores, creadores de contenido, familias y negocios pequenos.

Objetivos principales

- Evitar que personas no autorizadas accedan a informacion privada.
- Reducir el riesgo de perdida, alteracion o robo de datos.
- Mantener cuentas y dispositivos funcionando correctamente.
- Crear una cultura de cuidado digital y pensamiento critico.

Triada de la seguridad de la informacion



2. La triada CIA: tres ideas clave

La base de muchos temas de seguridad se resume en tres conceptos: confidencialidad, integridad y disponibilidad. A menudo se conoce como triada CIA por sus siglas en ingles: Confidentiality, Integrity y Availability.

Confidencialidad

Significa que la informacion solo puede ser vista por personas autorizadas. Ejemplos: una contrasena, un expediente academico, una conversacion privada o los datos de una cuenta bancaria.

Integridad

Significa que la informacion se mantiene correcta y no ha sido modificada sin permiso. Si alguien cambia una nota, una factura o un archivo importante sin autorizacion, la integridad se ve afectada.

Disponibilidad

Significa que los sistemas y datos estan disponibles cuando se necesitan. Un sitio caido, una cuenta bloqueada o archivos inaccesibles afectan la disponibilidad.

Ejemplo aplicado

Imagina una plataforma educativa. La confidencialidad protege los datos de los estudiantes; la integridad evita cambios no autorizados en notas o contenidos; y la disponibilidad permite que las clases y materiales se puedan consultar cuando sea necesario.

3. Amenazas digitales comunes

Una amenaza es cualquier situacion o tecnica que puede causar dano a una cuenta, dispositivo, sistema o informacion. No todas las amenazas son iguales: algunas dependen de errores humanos, otras de fallos tecnicos y otras de enganos bien preparados.

Amenazas frecuentes

- Phishing: mensajes falsos que intentan robar contrasenas o datos.
- Malware: software malicioso que puede danar, espiar o bloquear un dispositivo.
- Robo de cuentas: acceso no autorizado a correos, redes sociales o servicios.
- Contraseñas debiles: claves faciles de adivinar o reutilizadas.
- Redes Wi-Fi inseguras: conexiones sin proteccion adecuada.
- Errores humanos: descargar archivos sospechosos o confiar en enlaces falsos.

Ejemplo de ataque de phishing

La mejor defensa empieza por aprender a reconocer senales de riesgo antes de hacer clic, descargar archivos o ingresar datos personales.

4. Phishing: el engano mas comun

El phishing es una tecnica de engaño. El atacante se hace pasar por una empresa, escuela, banco, servicio conocido o persona confiable para lograr que la victima entregue informacion sensible.

Senales de alerta

- Mensajes con urgencia exagerada: "tu cuenta sera cerrada hoy".
- Enlaces raros, acortados o con dominios parecidos al real.
- Errores de escritura, logos de baja calidad o saludos genericos.
- Solicitudes de contrasenas, codigos de verificacion o datos bancarios.
- Archivos adjuntos inesperados.

Como actuar

Antes de ingresar datos, revisa el remitente, escribe la direccion del sitio manualmente en el navegador y evita abrir enlaces de mensajes sospechosos. Si un mensaje parece urgente, confirma por otro canal oficial.

Mini ejercicio

Cuando recibas un mensaje inesperado, preguntate: ¿yo solicite esto?, ¿el dominio es real?, ¿me estan presionando?, ¿me piden datos que no deberian pedir por mensaje?

5. Contrasenas seguras y MFA

Una contrasena es una de las primeras barreras de proteccion. Pero una contrasena corta, repetida o facil de adivinar puede poner en riesgo muchas cuentas a la vez.

Buenas practicas

- Usa contrasenas largas. Una frase de paso puede ser mas facil de recordar y mas dificil de adivinar.
- No reutilices la misma contrasena en todas tus cuentas.
- Activa autenticacion en dos pasos cuando este disponible.
- Considera usar un gestor de contrasenas confiable.
- No compartas codigos de verificacion con otras personas.

Ejemplo de frase de paso

Una frase como "CafeVerdeNubeLibro27" puede ser mas fuerte que una palabra simple con un numero al final. La clave es combinar longitud, variedad y dificultad de adivinacion.

6. Malware y archivos sospechosos

Malware es una palabra que agrupa diferentes tipos de software malicioso. Puede estar diseñado para robar informacion, espiar actividad, bloquear archivos, mostrar publicidad invasiva o controlar un equipo sin permiso.

Tipos comunes

- Virus: se propaga al ejecutar archivos infectados.
- Troyano: parece una aplicacion normal, pero oculta funciones maliciosas.
- Ransomware: bloquea o cifra archivos y exige pago para recuperarlos.
- Spyware: intenta espiar informacion, actividad o credenciales.

Como reducir el riesgo

- Descarga programas solo de sitios oficiales o tiendas confiables.
- Evita ejecutar archivos desconocidos o recibidos por mensajes sospechosos.
- Mantén actualizado el sistema operativo y el navegador.
- Realiza copias de seguridad de archivos importantes.

Ejemplos de nombres sospechosos

```
No abras: factura_urgente.exe
Cuidado con: documento.pdf.exe
Verifica extensiones y remitentes antes de descargar.
```

7. Seguridad de dispositivos

Un dispositivo seguro reduce la posibilidad de que otras personas accedan a informacion privada. Esto aplica a computadoras, celulares, tablets y equipos compartidos en escuelas o trabajos.

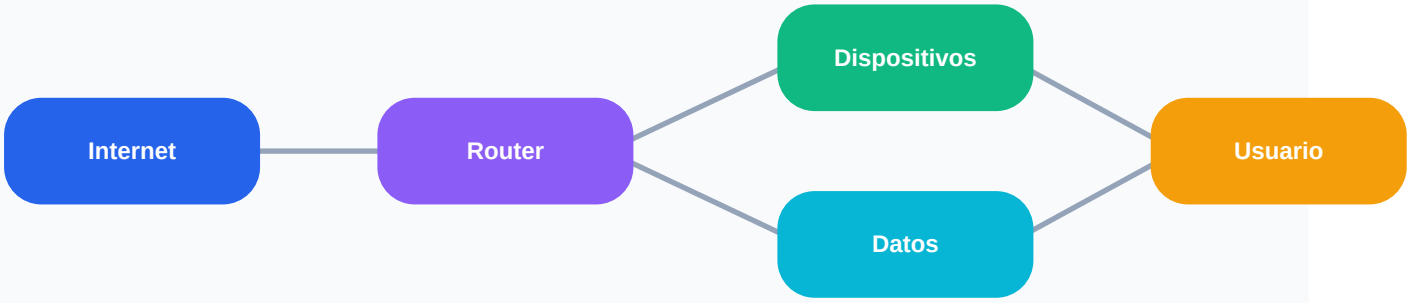
Medidas basicas

- Bloquea la pantalla con PIN, contrasena, huella o reconocimiento seguro.
- Actualiza aplicaciones y sistema operativo.
- Desinstala aplicaciones que no usas o que no reconoces.
- Evita prestar dispositivos desbloqueados con cuentas abiertas.
- No conectes memorias USB desconocidas sin precaucion.

Permisos de aplicaciones

Revisa que las aplicaciones no tengan permisos innecesarios. Por ejemplo, una calculadora no deberia necesitar acceso a tus contactos, ubicacion o microfono.

Seguridad basica en una red domestica o escolar



Puntos clave: contrasena Wi-Fi fuerte, actualizaciones, red de invitados y cuidado con enlaces falsos.

8. Redes Wi-Fi y navegacion segura

La red es el camino por donde viajan datos entre tu dispositivo y los servicios de internet. Una red mal configurada o una conexion publica insegura puede aumentar riesgos.

Wi-Fi seguro

- Usa contrasena fuerte para la red Wi-Fi.
- Cambia contrasenas por defecto del router cuando sea posible.
- Usa cifrado moderno como WPA2 o WPA3 si el equipo lo permite.
- Crea una red de invitados para visitantes.
- Evita compartir la clave principal de la red con muchas personas.

Navegacion segura

Verifica que los sitios importantes usen HTTPS, revisa bien los dominios y evita ingresar informacion personal en paginas desconocidas. En redes publicas, evita operaciones sensibles si no estas seguro de la conexion.

Tambien es importante cerrar sesion en equipos compartidos y no guardar contrasenas en computadoras que no son tuyas.

9. Copias de seguridad y recuperacion

Una copia de seguridad es una copia extra de archivos importantes. Sirve para recuperarlos si el dispositivo se pierde, se dana, se infecta con malware o se borra informacion por error.

Que respaldar

- Documentos importantes de estudio o trabajo.
- Fotos, proyectos, archivos personales y certificados.
- Contratos, facturas y documentos que no puedas reemplazar facilmente.

Buenas practicas

No basta con hacer una copia una sola vez. Lo ideal es tener una rutina: semanal, mensual o despues de crear archivos importantes. Tambien conviene probar de vez en cuando que puedes recuperar los archivos respaldados.

La regla 3-2-1 ayuda a recordar una estrategia simple: tres copias, en dos tipos de almacenamiento y una fuera del equipo principal.

10. Privacidad y huella digital

La privacidad digital se relaciona con el control de la informacion que compartes en internet. Cada publicacion, registro, comentario, permiso o cuenta puede formar parte de tu huella digital.

Cuida lo que compartes

- Evita publicar informacion personal como direccion, documentos o datos bancarios.
- Revisa la privacidad de tus redes sociales.
- Piensa antes de subir fotos, ubicaciones o informacion de otras personas.
- No compartas codigos de verificacion, enlaces privados o capturas con datos sensibles.

Datos sensibles

Datos sensibles son aquellos que pueden causar dano si se exponen: contrasenas, codigos, ubicacion, documentos, informacion bancaria, datos medicos o acceso a cuentas.

Pregunta clave

Antes de publicar o enviar algo, preguntate: ¿me afectaria si esto se comparte con alguien mas?, ¿contiene datos privados?, ¿realmente necesito compartirlo?

11. Checklist de estudio y practica

La ciberseguridad mejora con habitos. Usa este checklist como punto de partida para proteger tus cuentas y estudiar los conceptos principales.

- [ ] Identifico la diferencia entre confidencialidad, integridad y disponibilidad.
- [ ] Reviso enlaces y remitentes antes de ingresar datos personales.
- [ ] Uso contrasenas largas y diferentes para cuentas importantes.
- [ ] Activo autenticacion en dos pasos en correo y redes sociales.
- [ ] Mantengo actualizado el sistema, navegador y aplicaciones.
- [ ] Descargo programas solo desde fuentes oficiales.
- [ ] Realizo copias de seguridad de archivos importantes.
- [ ] Evito compartir informacion sensible por mensajes o formularios dudosos.
- [ ] Cierro sesion en equipos compartidos.
- [ ] Pienso antes de hacer clic, descargar o publicar informacion.

Resumen final

La ciberseguridad no se trata de tener miedo a internet, sino de aprender a usar la tecnologia con criterio. Con buenas practicas, atencion a las senales de riesgo y conocimiento basico, es posible reducir muchos problemas digitales.

ByteNova recomienda seguir aprendiendo de forma gradual: primero los conceptos, luego los habitos, y finalmente herramientas mas avanzadas como administradores de contrasenas, analisis de redes y fundamentos de seguridad web.