Guía de seguridad digital

Este manual te ofrece consejos prácticos y herramientas actualizadas para navegar en internet de forma segura.

Objetivo: Que docentes y estudiantes.

Actividad: Ya sea en equipos de forma personal los estudiantes deberán actualizar esta guía con información que consideren fundamental para sus seguridad digital

1. Reglas básicas de seguridad

1. Respalda tu información

- **En la nube:** Guarda copias de archivos importantes en servicios cifrados (Google Drive, Dropbox, etc.).
- **En discos duros externos**: Usa dispositivos físicos para información sensible y mantenlos en un lugar seguro.
- **Cifrado:** Protege tus respaldos con contraseñas fuertes o herramientas como VeraCrypt.

2. Realiza actualizaciones constantes

- **Sistemas operativos:** Activa las actualizaciones automáticas en tu computadora, celular y tablet.
- **Aplicaciones:** Mantén actualizados navegadores, antivirus y apps de comunicación.
- **Dispositivos de red:** Actualiza el firmware de tu router y módem para evitar vulnerabilidades.

3. Usa Antivirus

- Instala soluciones confiables como Bitdefender, Malwarebytes o Windows Defender.
- Realiza escaneos periódicos y evita descargar software pirata.

4. Protégete de engaños (Phishing)

- **Verifica enlaces:** Pasa el cursor sobre URLs antes de hacer clic.
- **No compartas datos:** Bancos y servicios legítimos nunca piden contraseñas por correo o mensaje.
- **Usa autenticación en dos pasos (2FA):** Habilítala en todas tus cuentas importantes.

5. Genera contraseñas seguras

- **Crea contraseñas robustas:** Combina letras, números y símbolos (ejemplo: S3gur1d4d_2024!).
- **Usa un gestor de contraseñas:** Como Bitwarden o LastPass para almacenarlas de forma cifrada.
- **Evita reutilizarlas:** Cada cuenta debe tener una contraseña única.

6. Usa comunicación cifrada

- **Mensajería:** Usa apps como Signal o WhatsApp (con cifrado E2E).
- **Correos:** Prefiere servicios como ProtonMail o Tutanota.
- **Navegación:** Verifica que los sitios web tengan HTTPS (en la barra de direcciones).

7. Protege tus cuentas

- Bloquea tus dispositivos con PIN, huella o reconocimiento facial. (al menos dos)
- Revisa la actividad reciente en Google (https://myaccount.google.com) o redes sociales.
- Elimina cuentas antiguas.

8. Si pierdes el acceso a una cuenta:

- Contacta al soporte del servicio (ejemplo: "Recuperar cuenta de Gmail").
- Proporciona pruebas de identidad (correo alternativo, número de teléfono).
- Cambia la contraseña y activa 2FA.

2. ¿Qué hacer ante ataques en redes sociales?

1. **Identifica:** Reconoce si es acoso, doxing (exposición de datos privados) o trolls.
2. **Documenta:** Guarda capturas de pantalla con fecha y hora.
3. **Denuncia:** Si es grave, acude a autoridades o organizaciones.
4. **Bloquea y reporta:** Usa las herramientas de la plataforma (ejemplo: "Reportar" en Twitter).

Doxing:
Publicación no consentida de datos personales.

- *Solución:* Elimina información expuesta y ajusta la privacidad de tus redes.

Bots y Trolls:
Cuentas falsas que difunden odio o desinformación.

- *Solución:* No interactúes, bloquea y reporta.

---

3. Cómo evitar el Phishing

Alerta

- Correos con errores gramaticales o remitentes sospechosos (ejemplo: "soportetecnico@servicio-guugle.com").
- Mensajes urgentes ("¡Tu cuenta será eliminada!").
- Enlaces acortados (como bit.ly/xxxx).

Recomendaciones

- Nunca descargues archivos adjuntos desconocidos.
- Usa correos temporales (https://temp-mail.org/) para registros en sitios no confiables.

4. Seguridad en dispositivos móviles

Protege tu teléfono:

- Habilita el bloqueo remoto: Usa Find My Device (Android) o Buscar mi iPhone (iOS).
- Evita redes WiFi públicas para transacciones bancarias.
- Instala apps solo desde tiendas oficiales (Google Play, App Store).

Ajustes fundamentales:

- Desactiva Bluetooth y GPS cuando no los uses.
- Revisa permisos de apps: Una app no necesita acceso a tus contactos.
- Usa VPNs como ProtonVPN o NordVPN en conexiones inseguras.

Ajustes en redes sociales

Facebook:

- Ve a *Configuración > Privacidad* y limita quién ve tus publicaciones.
- Desactiva el *rastreo* de ubicación en la app.

Intagram:

- Usa *Cuenta privada* y revisa las solicitudes de seguimiento.
- Elimina apps vinculadas no confiables en *Seguridad > Apps y sitios.*
- Desactiva rastreo de ubicación.

Crea un kit de emergencia digital

Si eres mayor de edad prepara estos elementos en una USB cifrada o nube segura:

- Copias de documentos (INE, pasaporte).
- Contactos de emergencia (abogados, familiares, organizaciones).
- Backup de comunicaciones importantes (correos, mensajes).

Ajustes en redes sociales

1. Documentar todo (fotos, logs, capturas)
2. Contactar a Access Now Helpline: https://www.accessnow.org/help/
3. Aislar dispositivos comprometidos
4. Notificar a contactos clave sobre posible infección
5. Aislar el dispositivo (modo avión + WiFi/BT apagados)
6. Documentar síntomas antes de limpiar
7. Formateo completo (no solo reinicio)
8. Restaurar desde copia limpia

Es tu momento, revisa con tus compañeros qué otras medidas son fundamentales para la seguridad digital.

Descripción