CIBERSEGURIDAD

PROTECCIÓN EN LA ERA DIGITAL

Sara Martínez Navarro

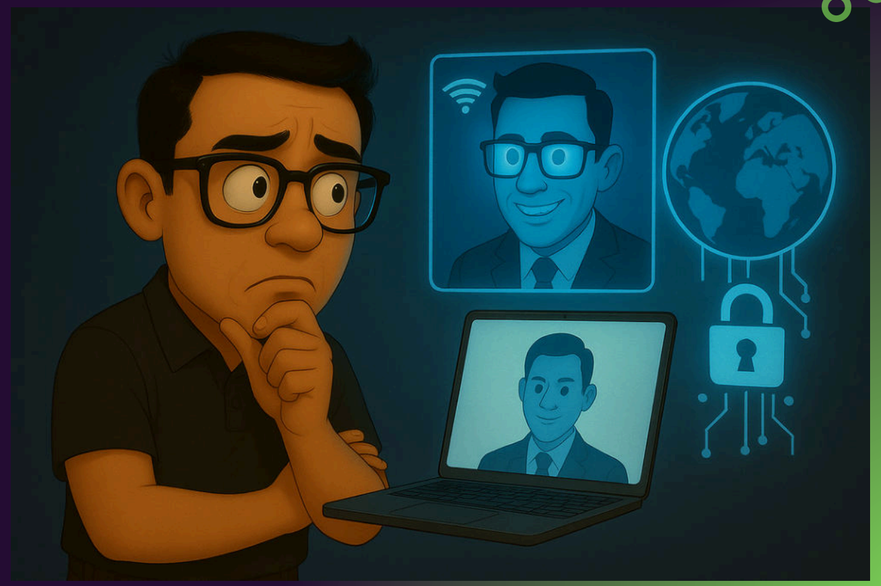
USO RESPONSABLE DE INTERNET

Debido a la cantidad de información que nos ofrece Internet es necesario respetar unas normas que nos permitan disfrutar de sus ventajas sin correr los riesgos que puede acarrear su uso.

Una actitud responsable nos asegurará la protección de los riesgos que Internet conlleva.

“LA CIBERSEGURIDAD PROTEGE DATOS DIGITALES DE AMENAZAS Y ATAQUES,GARANTIZANDO TU PRIVACIDAD”

Informe Borcelle, 2030



PROTECCIÓN DE LA IDENTIDAD Y LA PRIVACIDAD

La información que existe en la Red sobre nosotros proviene de los datos que nosotros mismos aportamos, de nuestras visitas y búsquedas, y de la información que los demás aportan sobre nosotros.

AMENAZAS

- Geolocalización
- Pérdida de privacidad
- Uso comercial de nuestra información
- Ciberbullying
- Grooming
- Extorsión
- Sexting
- Phishing

MEDIOS

- Chats
- Redes sociales
- Mensajería instantánea
- Publicidad de las páginas

Solicitud de datos en las aplicaciones

MEDIDAS

- Pensar antes de publicar y aceptar en la Red.
- Supervisar nuestra imagen en la Red
- Respetar los derechos de los demás.
- Controlar la lista de contactos.
- Vigilar los permisos otorgados a las aplicaciones.
- Revisar las condiciones de un servicio antes de aceptarlas.
- Configurar las opciones de privacidad y seguridad.
- Cerrar la sesión al terminar un servicio en línea.
- Usar patrones y contraseñas.

PROTECCIÓN DE LOS DISPOSITIVOS

Nuestros dispositivos están expuestos a ataques externos. El conjunto de programas que pueden ser nocivos para nuestros dispositivos se engloba en el término malware.
Un malware puede querer desde acceder a la información del ordenador o de datos personales hasta robar contraseñas.

AMENAZAS

- Virus y troyanos
- Gusanos
- Spyware
- Falsos antivirus
- Ransomware
- Kaylogger

VÍAS DE INFECCIÓN

- Correo electrónico
- Aplicaciones maliciosas
- Páginas web maliciosas
- Redes sociales
- Descarga de ficheros

MEDIDAS

- Instalar antivirus y cortafuegos y actualizaciones de software.
- Hacer copias de seguridad.
- Revisar los archivos y los ficheros compartidos y descargados.
- Revisar las condiciones de un servicio antes de aceptarlas.
- Comprobar las descargas de software antes de llevarlas a cabo.
- Usar patrones y contraseñas y precaución en redes wifi públicas.
- Descargar de forma segura las aplicaciones.

GROOMING

ACOSO Y ABUSO SEXUAL ONLINE

Son formas delictivas de acoso que implican a un adulto que se pone en contacto con un niño, niña o adolescente con el fin de ganarse poco a poco su confianza para luego involucrarle en una actividad sexual.

CONSECUENCIAS

Daños psicológicos en la víctima:

- Depresión
- Baja autoestima
- Desconfianza
- Cambios de humor
- Bajo rendimiento

Daños a nivel familiar:

- Empeoramiento de las relaciones
- Chantajes a la propia familia por parte del acosador

GROOMING

PROTECCIÓN

- No proporcionar imágenes, vídeos o informaciones personales a desconocidos.
- Evitar dar contraseñas.
- Proteger tu privacidad en imágenes e información personal.

OJO CON LO QUE SUBES A INTERNET

QUÉ HACER

- Valorar si es cierto que dispone de material para ejercer la amenaza.
- No ceder al chantaje en ningún caso.
- Pedir ayuda.
- Revisar el equipo con un programa antimalware.
- Modificar todas las contraseñas de acceso.
- Aumentar las opciones de privacidad en tus perfiles de las redes sociales.
- Buscar y guardar las pruebas del chantaje: capturas de pantalla, conversaciones...

CIBERBULLYING O CIBERACOSO

ACOSO Y ABUSO SEXUAL ONLINE

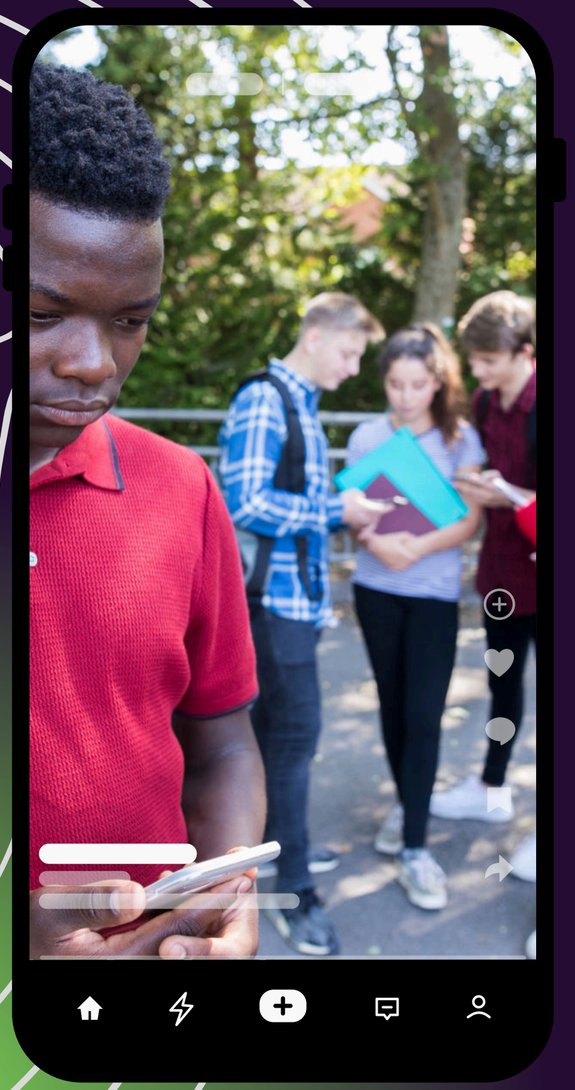
Acoso (atormentar, amenazar, hostigar, humillar o molestar) un menor a otro menor usando las tecnologías de la información y la comunicación.

CONSECUENCIAS

Puede mantenerse durante las 24 horas del día, ya que el acceso a los distintos dispositivos se puede realizar en cualquier momento y desde cualquier lugar, por lo que el perjuicio para la víctima puede ser considerablemente mayor que el bullying. Entre estos encontramos:

- Problemas de salud mental como ansiedad, depresión y baja autoestima.
- Aislamiento social
- Rendimiento académico deficiente.
- En casos extremos, puede llevar a pensamientos y autolesiones suicidas.

CIBERBULLYING O CIBERACOSO



PROTECCIÓN

- No difundas imágenes comprometidas, ni tuyas ni de otras personas.
- No proporciones datos.
- No apoyes actos que supongan ciberacoso.

NO HAGAS A OTROS LO QUE NO QUIERES QUE TE HAGAN

QUÉ HACER

- Denuncia la situación.
- Ayuda a prevenir.
- Conoce los protocolos de actuación.

SEXTING

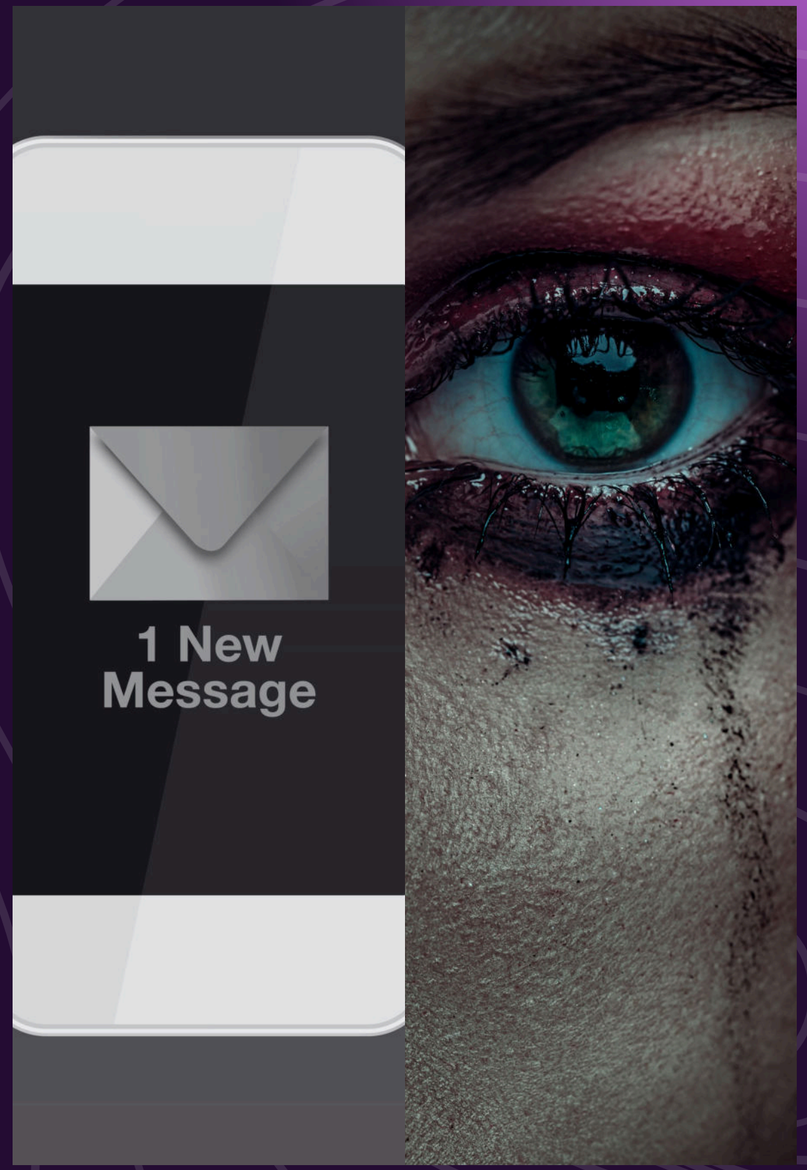
EXTORSIÓN O CHANTAJE. SEXTORSIÓN

Enviar o recibir mensajes, fotos o videos íntimos a través del celular o internet. Puede ser una forma de comunicación privada, pero también implica riesgos si el contenido se difunde sin consentimiento.

CONSECUENCIAS

- Ansiedad, tristeza o vergüenza.
- Pérdida de confianza en uno mismo o en los demás.
- Aislamiento social o miedo a ser juzgado.
- En casos graves, puede provocar depresión o pensamientos negativos.

SI TE PASA, PIDE AYUDA. NO ESTÁS SOLO/A.



SEXTING

PROTECCIÓN

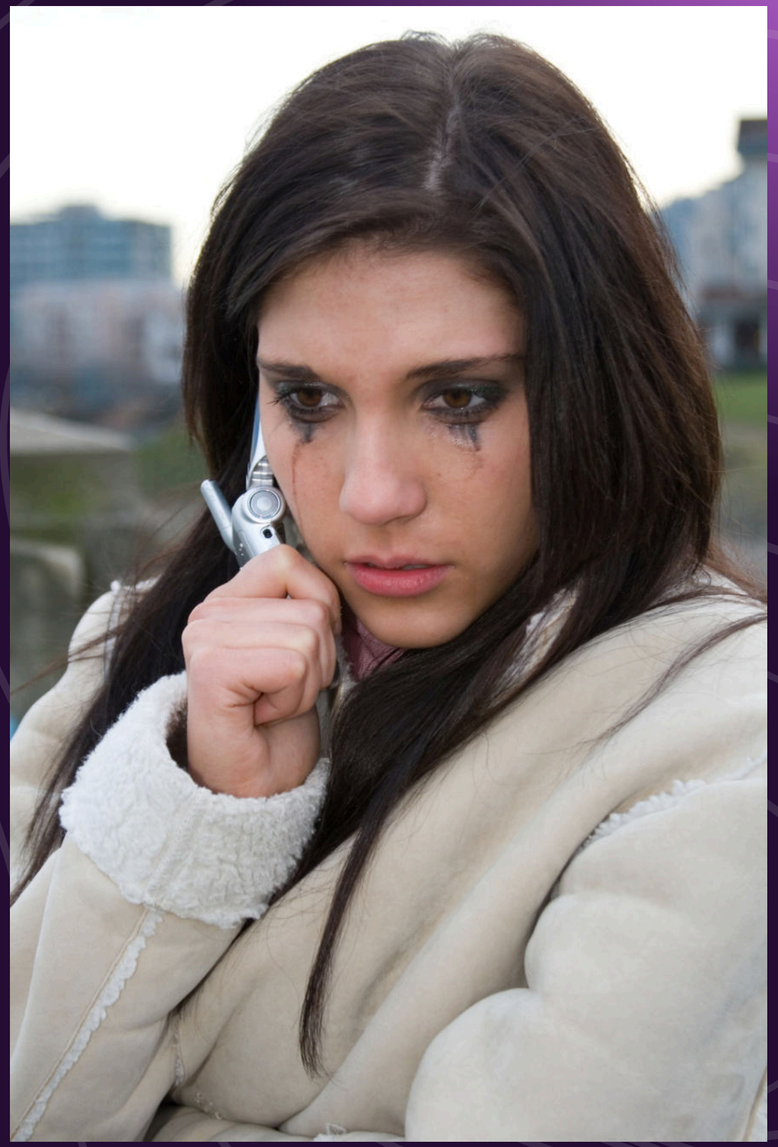
- Piensa antes de enviar. Lo que compartes, puede quedar guardado.
- No muestres tu rostro ni detalles que te identifiquen.
- Reflexiona sobre las posibles consecuencias.
- Habla con personas que respeten tu privacidad.

NADIE PUEDE PRESIONARTE PARA MANDAR ALGO QUE NO QUIERES.

QUÉ HACER

- No te culpes. La responsabilidad es de quien difunde, no tuya.
- Guarda las pruebas: pantallazos, mensajes, enlaces.
- Bloquea y denuncia al agresor en la plataforma o ante la policía.
- Busca apoyo: habla con un adulto de confianza, orientador o línea de ayuda

DIFUNDIR SIN PERMISO ES VIOLENCIA DIGITAL.



PHISING

ESTAFA, ENGAÑO.

El phishing son mensajes o webs fraudulentas que buscan robar tus datos o dinero. Solicitan datos haciendose pasar por una empresa o entidad pública con la excusa de comprobarlos o actualizarlos. Pueden hacerlo a través de un mensaje, una llamada, una ventana emergente o un email.

CONSECUENCIAS

- Pérdida de dinero o identidad.
- Que realicen un fraude o robo en tu nombre.
- Sentimiento de culpa o vergüenza. ansiedad y estrés.
- Insomnio y dificultad para concentrarte.
- Pérdida de confianza en servicios online y en relaciones digitales.

NO CONFÍES SIN COMPROBAR.

PHISING

PROTECCIÓN

- No abras enlaces ni archivos adjuntos de mensajes sospechosos.
- Comprueba la dirección del remitente y la URL (sin hacer clic).
- Activa la verificación en dos pasos y usa contraseñas únicas y seguras.
- Nunca facilites códigos SMS, contraseñas o datos bancarios por chat o email.
- No respondas a ninguna solicitud de datos. Las entidades no los piden.
- Si no estas seguro de algo, pregunta antes de dar información.

QUÉ HACER

- Desconecta o cierra la web/mensaje inmediatamente.
- No introduzcas más datos; cambia contraseñas (especialmente las relacionadas).
- Si diste datos bancarios, contacta al banco y bloquea tarjetas/operaciones.
- Guarda capturas y reenvía el mensaje a la entidad legítima para verificar.
- Denuncia en la plataforma, al banco y —si hay perjuicio económico— a la policía.

SUPLANTACIÓN DE IDENTIDAD

APROPIACIÓN DE UNA IDENTIDAD DIGITAL

Uso de tus datos (fotos, nombre, cuentas) para hacerse pasar por ti.
Pueden abrir cuentas, pedir dinero o difundir información falsa en tu nombre.

CONSECUENCIAS

- Estrés, ansiedad y sensación de pérdida de control.
- Vergüenza o miedo a que te juzguen por acciones que no hiciste.
- Pérdida de reputación o problemas en el trabajo/estudios.
- Problemas económicos si hay fraude con tarjetas o créditos.
- Imagen distorsionada de uno mismo en Internet.
- Ser víctica de burlas, insultos o amenzas.

TUS DATOS VALEN: PROTÉGELOS COMO TU DINERO

SUPLANTACIÓN DE IDENTIDAD

PROTECCIÓN

- No compartas contraseñas ni códigos de verificación.
- Activa la verificación en dos pasos en tus cuentas.
- Revisa la configuración de privacidad y elimina datos personales innecesarios.
- Evitan que miren cuando tecleas alguna contraseña
- Mantén actualizados antivirus y contraseñas únicas por servicio.
- Cierra sesión y no almacenes las contraseñas en ordenadores compartidos.

QUÉ HACER

- Cambia las contraseñas de inmediato y cierra sesiones en dispositivos desconocidos.
- Contacta a la plataforma (red social, email, banco) para denunciar la cuenta falsa y solicitar su eliminación.
- Si hay uso de tus datos bancarios o financiero, avisa al banco y bloquea tarjetas.
- Guarda pruebas (capturas, URLs) y denuncia a las autoridades si hay fraude o daños.
- Informa a amigos y familiares para evitar que confíen en mensajes enviados por el suplantador.
- Busca apoyo si te sientes ansioso/a o afectado/a emocionalmente.

CIBERADICCIÓN

CONEXIÓN COMPULSIVA

Cuando el uso de internet, móviles o redes domina tu tiempo y afecta tu vida diaria, hablamos de ciberadicción. Existe una necesidad por tener que conectarse con frecuencia.

CONSECUENCIAS

- Insomnio, fatiga y problemas de atención.
- Aislamiento social o relaciones superficiales.
- Ansiedad, irritabilidad y bajón del estado de ánimo al intentar dejarlo.
- Rendimiento escolar/laboral afectado y pérdida de hobbies reales.
- Mal humor o nerviosismo cuando no se puede conectar.
- Probelmas alimenticios.

PUEDE PASAR DESAPERCIBIDA: FÍJATE EN HÁBITOS, SUEÑO Y RELACIONES.

CIBERADICCIÓN

PROTECCIÓN

- Establece límites de tiempo por app y pausas programadas.
- Apaga las notificaciones no esenciales; usa modos “no molestar”.
- Delega el móvil fuera de la habitación al dormir.
- Mantén actividades alternativas: deporte, hobbies, encuentros presenciales.

QUÉ HACER

- Reconoce el problema: registra el tiempo real que pasas en pantalla.
- Activa límites de uso o apps que bloqueen temporariamente.
- Habla con familiares o amigos para que te acompañen en reducirlo.
- Sustituye tiempo de pantalla por actividades concretas (paseo, deporte, lectura).
- Si interfiere en estudio, trabajo o estado de ánimo, consulta a un profesional.

APAGA LA PANTALLA. ENCIENDE TU VIDA.

TIPOS DE AMENAZAS CIBERNETICAS

- ***Malware***
  Programas maliciosos que dañan tu dispositivo, roban datos o controlan tu equipo.
- ***Hackeo***
  Alguien consigue acceder a tus cuentas o dispositivos sin permiso para ver, borrar o usar tu información.
- ***Ransomware***
  Malware que cifra tus archivos y pide un rescate para recuperarlos.
- ***SIM swapping***
  Un atacante toma el control de tu número de teléfono y recibe códigos de verificación.
- ***Scareware***
  Llamadas o ventanas que dicen que tu equipo está infectado y piden acceso remoto o pago.

MEDIDAS DE PROTECCIÓN

Hackeo

- Usa **contraseñas únicas y fuertes;** activa la **verificación en dos pasos**.
- Mantén el sistema y las apps **actualizadas**.
- No instales aplicaciones de fuentes no oficiales.

Malware

- Instala y actualiza un **antivirus/antimalware** confiable.
- No abras archivos adjuntos de remitentes desconocidos.
- Evita descargar software pirata.

Ransonware

- Haz **copias de seguridad** periódicas en discos externos o en la nube.
- Mantén **todo actualizado** y evita enlaces/adjuntos sospechosos.

Swapping

- No compartas códigos SMS; usa **apps de autenticación** cuando sea posible.
- Ponte un **PIN/contraseña** con tu operador y alerta al proveedor si hay transferencias de SIM.

Scareware

- Nunca aceptes acceso remoto a desconocidos; busca **soporte oficial**.
- Cierra ventanas emergentes y no llames números que aparezcan en pop-ups.

LA SEGURIDAD NO ES UN PRODUCTO, ES UN PROCESO CONTINUO

Muchas gracias por la atención.