SEGUROS

Principales
riesgos digitales y cómo prevenirlos

INTRODUCCIÓN

La tecnología ha facilitado la vida de múltiples formas, actualmente existen teléfonos, computadores, redes interconectadas y diversos avances que han logrado mejorar la calidad de vida. Por ejemplo, la manera en la que interactúas, aprendes, te cuidas y trabajas es mediada por la tecnología, esta permite tener todo a la mano, de manera fácil e inmediata, y a un solo clic resolver o dar respuesta a diversas situaciones.

Sin embargo, no todo es positivo a la hora de usar la tecnología, existen algunos riesgos a los que estamos expuestos independientemente del momento de vida en el que nos encontremos. Estos se pueden materializar por múltiples razones, entre ellas: falta de conciencia del entorno digital y sus riesgos, hábitos inadecuados, exposición excesiva de información en internet, desconocimiento de las herramientas de seguridad e incluso falta de precaución; lo cual facilita que personas malintencionadas puedan valerse de su conocimiento y las vulnerabilidades identificadas para actuar.

Por eso, conocer los riesgos existentes, las formas en que se materializan y a su vez, contar con las herramientas suficientes para estar protegidos, nos permitirá saber cómo actuar en caso de que haya algún indicio de riesgo y así evitar su materialización, es decir, evitar que te sucedan a ti o a alguien cercano.

En este documento encontrarás los principales riesgos digitales agrupados por categorías, con su respectiva descripción, población impactada, formas de exponerse a ellos y recomendaciones generales que nos ayuden a prevenirlos.

Clasificación de los riesgos digitales

Los riesgos digitales pueden afectarte de múltiples formas, por ejemplo, al perder acceso total o parcial a la información, al dañarse tus dispositivos, e incluso podrían afectar tus finanzas debido a la necesidad de recuperar la información o reparar los dispositivos.

También, hay casos en los que personas malintencionadas acceden a tus cuentas bancarias o realizan compras con tus tarjetas.

Es muy importante que tengas en cuenta que estos riesgos no solo te pueden afectar en el ámbito personal, sino también en el laboral, generando así, impactos negativos en la seguridad de la información de las compañías.

A su vez, y aunque no lo dimensiones, algunos de estos riesgos pueden afectar tu salud física y mental, impactar negativamente tus relaciones interpersonales, afectar tu comportamiento, emociones e incluso tu reputación.

Existen diversas formas de clasificar los riesgos digitales, a continuación, los encontrarás agrupados en **cuatro grandes categorías:**

- ***Riesgos de conducta***
- ***Riesgos de contacto***
- ***Riesgos de contenido***
- ***Riesgos técnicos***

RIESGOS DE CONDUCTA

Implican un comportamiento que puede poner en riesgo la integridad de la persona.

1. Ciber inducción al daño físico

Son retos o juegos en línea, donde se incita a las personas a realizar una serie de tareas peligrosas, como ataques violentos y daño auto infringido, lo que puede generar impactos emocionales y en algunos casos hasta el suicidio.

Algunos ejemplos son 'El juego de la Ballena Azul' o 'Momo', donde les plantean una serie de retos por cumplir, algunos de los cuales pueden resultar peligrosos, o incluso mortales. El principal medio por el que se viralizan son las redes sociales.

- **Principal público impactado:** Niños, niñas y adolescentes.

- **Cómo nos exponemos:** Al no tener consciencia sobre los riesgos y cuando se hace uso de internet sin el acompañamiento necesario de padres y cuidadores, quienes no validan el contenido al que se están exponiendo, ni garantizan que la interacción en la web se haga de manera segura.

- **Buenas prácticas:**

  - Explica a los niños aquellos riesgos a los que se exponen cuando navegan en internet.
  - Saca los dispositivos electrónicos de los cuartos de los niños y define sitios comunes del hogar para navegar.
  - No permitas que los menores de edad tengan cuentas propias en redes sociales sin cumplir la edad mínima recomendada para ello.
  - Haz seguimiento constante a las actividades de los niños mediante herramientas de Control Parental.
  - Antes de participar en un reto, reflexiona frente a sus posibles consecuencias.

2. Ciberbullying o ciberacoso

Es la acción repetida e intencional de agredir de manera individual o colectiva a una persona, haciendo uso de dispositivos digitales (teléfonos celulares, computadores, tablets, entre otros). Algunas de las formas principales de este tipo de ataques son el hostigamiento, los insultos, la exclusión y la difamación; así como el hecho de compartir o publicar contenido negativo, perjudicial, falso, o cruel sobre otra persona. En todas ellas, se busca afectar la imagen personal y la autoestima de alguien más, provocando humillación o vergüenza.

- **Principal público impactado:** Niños, niñas y adolescentes.

- **Cómo nos exponemos:** La exposición puede ocurrir incluso sin el conocimiento de la persona, puede darse en cualquier momento y desde cualquier lugar, basta con la intención del agresor de utilizar cualquier información -falsa o verdadera- para agredir a la víctima. El ciberacoso puede ocurrir mediante mensajes de texto, aplicaciones, redes sociales, correo electrónico, foros o juegos.

- **Buenas prácticas:**

  - Habla con tus hijos sobre los riesgos a los que se exponen en internet y hazles saber que es importante que te cuenten si se presenta una situación que les genere miedo o confusión.

  - Si en algún momento eres victima de este delito no respondas o tomes represalias. Informa a las autoridades y reporta el perfil del agresor.

  - La tolerancia y el respeto por los demás son fundamentales, niégate a participar de estas forma de violencia.

  - Reporta los malos comportamientos de otros. Denuncia frente a las autoridades competentes.

    aquí te contamos cómo hacerlo

  - Piensa dos veces antes de publicar, enviar mensajes y compartir información, pues una vez lo haces pierdes el control de esta.

3. Ciberadicción

También conocida como trastorno de adicción a internet, se define como el uso abusivo de este, a través de diferentes dispositivos electrónicos, con impactos en la vida diaria. Es decir, es la pérdida de control frente al uso racional de internet. Está asociada con la conexión compulsiva, o FOMO (Fear Of Missing Out), que es el miedo a perderse algo o a la exclusión digital.

- **Principal público impactado:** Niños, niñas y adolescentes.
- **Cómo nos exponemos:** La exposición puede ocurrir:
  - Por falta de hábitos saludables en el consumo de tecnología, que llevan a un uso desmedido de la misma.
  - Por la falta de interacción social de manera presencial.
- **Buenas prácticas:**
  - Acuerda un horario concreto y moderado de conexión a internet, así como el uso de videojuegos en la red.
  - Planea las tareas a realizar en internet, antes de conectarse y tratar de mantener la atención en ellas hasta su terminación.
  - Diversifica las actividades cotidianas tratando de dedicarle a cada una el tiempo necesario.
  - Cultiva las relaciones personales y familiares.
  - Respeta las horas de sueño y descanso, así como los espacios de alimentación y de interacción en familia.

4. Ciberestrés o ciberfatiga

Se refiere a los efectos negativos por el uso de las nuevas tecnologías y los cambios constantes que enfrentan. En gran medida por la gran cantidad de tiempo de exposición al entorno digital, pero también por la dificultad de adaptarse a un cambio tecnológico constante.[1]

- **Principal público impactado:** Adultos.
- **Cómo nos exponemos:**
  - Cuando hay rechazo al cambio y/o la adaptación.
  - Con la exposición prolongada al entorno digital en jornadas extendidas de trabajo o de estudio.
  - Cuando damos privilegio al uso de dispositivos sobre los vínculos interpersonales presenciales.
- **Buenas prácticas:**
  - Solicita acompañamiento o realiza autoestudio frente a nuevas plataformas tecnológicas.
  - Privilegia la interacción social de manera presencial creando un balance adecuado entre vida online con vida offline.
  - Ten hábitos saludables de consumo digital.
  - Define y respeta tiempos de descanso.

5. Ciberpirámides

La ciberpirámide, se basa en el esquema de la estafa piramidal, cuyo propósito es captar la atención de las personas y que éstas recomienden y refieran a otros con el objetivo de generar beneficios adicionales a los participantes iniciales.

[1] https://www.riesgozero.info/sectores-de-actividad/administracion-comunicacion-y-servicios/la-columna-del-experto-riesgos-digitales-el-nuevo-topico-de-la-agenda-preventiva/

- **Principal público impactado:** Adultos.
- **Cómo nos exponemos:**
    - Confiando en quienes ofrecen rendimientos exorbitantes y en corto tiempo.
    - Cuando se invierte en negocios, en los cuales no hay claridad de dónde salen los recursos que prometen, ni justificación válida para las ganancias.
- **Buenas prácticas:**
    - Sospecha ante ofertas de rendimientos muy altos en el retorno de la inversión.
    - Sospecha cuando el negocio planteado involucre el reclutamiento de otras personas para la sostenibilidad de este.
    - Consulta siempre antes de entregar tus recursos: verifica con las autoridades y entes reguladores, si en verdad se trata de una empresa o persona autorizada para captar recursos del público en forma masiva.

6. Nomofobia

Consiste en el miedo irracional a no disponer del teléfono móvil, bien sea porque se ha dejado en casa, se ha descargado, está fuera de cobertura, ha agotado el saldo, se lo han robado o simplemente sufre un daño.

La nomofobia no está considerada todavía como una patología o un trastorno del comportamiento, pero lo cierto es que es consecuencia de una adicción, de un uso desmedido de los dispositivos móviles.

- **Principal público impactado:** Adolescentes y adultos.
- **Cómo nos exponemos:**
  - Cuando hacemos un uso indiscriminado del dispositivo.
- **Buenas prácticas:**
  - Establece hábitos saludables de navegación, definiendo o acordando espacios y momentos libres de dispositivos, por ejemplo, a la hora de comer, de dormir o relacionarse desde la presencialidad.
  - Diversifica las actividades cotidianas tratando de dedicarle a cada una el tiempo necesario.
  - Cultiva a diario las relaciones personales y familiares.

7. Phubbing

Combinación de las palabras phone (teléfono) y snubbing (hacer un desprecio), este término hace referencia al hecho de ignorar a alguien al estar prestando atención al teléfono celular.

- **Principal público impactado:** Niños, niñas, adolescentes y adultos.
- **Cómo nos exponemos:**
  - Al usar de forma desmedida los dispositivos tecnológicos ignorando la presencia del otro.
- **Buenas prácticas:**
  - Guarda el dispositivo cuando estés compartiendo espacios con otras personas, así evitarás mirarlo y usarlo constantemente.
  - Dales prioridad a las relaciones offline sobre las online.
  - Define momentos y espacios libres de tecnología.
  - Desactiva las notificaciones que no sean prioritarias, para evitar distracciones.

8. Suplantación de identidad digital o Spoofing

Es el acto deliberado en el que una persona se hace pasar por otra en internet para llevar a cabo actividades maliciosas, afectando la reputación o materializando fraudes. Se puede perder el control de las cuentas de redes sociales, correo y líneas telefónicas, lo que muchas veces impide tener acceso a las alertas y notificaciones de actividades realizadas por terceros en nuestras cuentas financieras y digitales.

- **Principal público impactado:** Adolescentes y adultos.
- **Cómo nos exponemos:**
  - Al entregar información personal a través de llamadas o correos electrónicos de remitentes aparentemente oficiales.
  - Ingresando a páginas web fraudulentas.
  - Utilizando contraseñas inseguras.
  - Cuando no contamos con una configuración segura de cuentas digitales y dispositivos.
  - Al autenticarnos en sitios web utilizando conexiones a internet públicas.
- **Buenas prácticas:**
  - Mantente atento a la correspondencia, notificaciones y alertas para identificar cualquier actividad anormal.
  - Usa contraseñas seguras y cámbialas con frecuencia.

Conoce aquí cómo hacerlo

  - No ingreses información personal en computadoras ubicadas en espacios públicos o estando conectado a redes públicas.
  - No respondas emails ni otros mensajes que te pidan información personal.

- Activa el doble factor de autenticación que proporcionan las entidades bancarias, las plataformas de correo electrónico y otros servicios digitales para fortalecer la seguridad de tus cuentas digitales.

Conoce aquí cómo hacerlo

9. Vamping

El vamping, viene de las palabras inglesas vampire (vampiro, un ser fantástico que está activo por la noche) y texting (enviar mensajes de texto a través de aparatos electrónicos). Se trata del fenómeno por el cual las personas, utilizan aparatos electrónicos durante la noche, reduciendo las horas necesarias de sueño para lograr un buen descanso que permita realizar las actividades cotidianas de una forma óptima.

- **Principal público impactado:** Niños, niñas, adolescentes y adultos.
- **Cómo nos exponemos:**
  - Con la disponibilidad de dispositivos electrónicos en el lugar de descanso y uso desmedido del mismo, la luz azul que emiten las pantallas impide la función de la melatonina en el cuerpo, hormona que regula el ciclo del sueño. Esto deriva en problemas de insomnio.[2]
- **Buenas prácticas:**
  - Retira los dispositivos digitales de las habitaciones al momento de dormir. Puedes usar relojes despertadores comunes y corrientes, para no tener que usar las alarmas de los teléfonos.
  - Los padres deben acompañar con normas y límites a los niños y adolescentes mientras aprenden a usar teléfonos, computadores y tabletas digitales de forma moderada, usando herramientas de control parental.
  - Ten buenos hábitos digitales, cuidando el equilibrio entre la vida online y offline.

[2] https://cronicaglobal.elespanol.com/cronica-directo/vamping-riesgos-movil-antes-dormir_233493_102.html

- Es importante la alfabetización digital del padre de familia. En muchos casos los padres desconocen lo que sus hijos hacen porque no tienen habilidades para utilizar un Smartphone o un computador, lo que evita que puedan evaluar y acompañar el uso que sus hijos hacen de los mismos y de la web.

RIESGOS DE CONTACTO

Este tipo de riesgos implican la interacción directa con un desconocido que se acerca de forma malintencionada.

1. Grooming

Conocido también como engaño pederasta, consiste en el engaño (la mayoría de las veces luego de ganarse su confianza) de un adulto hacia un menor de edad haciendo uso de canales digitales, como las redes sociales o las aplicaciones de mensajería instantánea.

El abusador crea un perfil falso buscando captar la atención de los niños, niñas y adolescentes, para establecer una relación íntima y posteriormente solicitarle fotos y videos con contenido sexual, que luego podría utilizar para chantajearle, con el propósito de obtener más material con contenido erótico o abusar sexualmente de él.

- **Principal público impactado:** Niños, niñas, adolescentes
- **Cómo se exponen:**
  - Cuando los menores de edad navegan en redes sociales o plataformas online, sin el acompañamiento adecuado de un adulto.
  - Siendo usuarios de redes sociales sin tener la edad apropiada.
  - Aceptando como contactos a personas desconocidas.
  - Por desconocimiento de los riesgos a los que están expuestos en la web, cómo funcionan y cómo pueden protegerse.

- **Buenas prácticas:**

    - Habla con tus hijos sobre los riesgos a los que se exponen en internet y hazles saber que es importante que te cuenten si se presenta una situación que les genere miedo o confusión.

    - Establece acuerdos y hábitos para el entorno digital, como el tiempo máximo que pueden navegar en el día y con quién pueden interactuar.

    - Dialoga con los niños sobre el uso consciente que deben hacer de las cámaras de sus dispositivos y, en lo posible, mantenla desactivada.

    - Utiliza las herramientas de control parental que están disponibles en la web.

2. Phishing

Es el método utilizado por los delincuentes cibernéticos para estafar y obtener información confidencial o financiera como contraseñas, datos de tarjetas de crédito, entre otros, utilizando técnicas de **ingeniería social.**

El phisher o estafador se hace pasar por otra persona o por empresas confiables y reconocidas, en comunicados electrónicos como correos, mensajería instantánea como WhatsApp, redes sociales, mensajes de texto (SMS/MMS, en este caso, llamado Smishing), que llevan a sitios web fraudulentos en los que capturan la información de quien ingresa.

- **Principal público impactado:** Adultos.

- **Cómo nos exponemos:** Por la falta de conciencia frente a este tipo de riesgos asociados al uso de correo electrónico, mensajes de texto o la navegación web sin las precauciones adecuadas.

- **Buenas prácticas:**

  - No respondas a correos electrónicos sospechosos o cuyo remitente es desconocido. Verifica la autenticidad y veracidad del comunicado antes de compartir información o ingresar a enlaces sospechosos.

  - Usa contraseñas seguras y recuerda que son confidenciales y que nunca, por ningún motivo, debes compartirlas. Activa el doble factor de autenticación que proporcionan la mayoría de las plataformas de correo electrónico y cuentas digitales para fortalecer el ingreso a ellas.

Navega seguro y aprende cómo estar protegido para aprovecharlo al máximo. ***Haz clic aquí***

  - Recuerda que las entidades financieras o gubernamentales no solicitan datos como claves o números de cuentas y tarjetas por este medio.

  - Comprueba la URL (dirección web) de los sitios que visitas. En muchos casos de phishing, la dirección web parece legítima, pero en realidad es sutilmente diferente a la original.

  - Mantén actualizado tu navegador y otras aplicaciones, pues con esto disminuyen posibles brechas de seguridad

3. Vishing

Es una modalidad de estafa en la que los ciberdelincuentes aplican técnicas de ingeniería social a través de llamadas telefónicas, con el fin de manipular a las personas para que realicen acciones involuntarias con la intención de acceder a información personal y financiera y obtener un beneficio económico.

Uno de los ataques más frecuentes de esta modalidad es la llamada telefónica en la que se hacen pasar por un familiar en una situación de urgencia y juegan con las emociones de las personas. Este estafador empieza a contar una historia como si estuviera pasando un momento muy crítico en la que necesita de alguna cantidad de dinero para solventarlo.

En esta modalidad los delincuentes también buscan obtener información como: Detalles de la tarjeta de crédito (incluidos los datos de vencimiento y los códigos de seguridad), números de cuenta y su contraseña, fecha de cumpleaños y número de pasaporte.

- **Principal público impactado:** Niños, niñas, adolescentes y adultos.
- **Cómo nos exponemos:**
  - Al contestar llamadas de números desconocidos sin precaución y proceder a entregar información.
  - Al exponer información personal y de contacto en redes sociales o sitios web.
- **Buenas prácticas:**
  - Ante una llamada de un número desconocido o con una situación atípica, no reveles información sensible como: direcciones físicas, correo electrónico, información de tarjetas débito/crédito o cuentas bancarias.
  - Conserva la calma y revisa la situación antes de actuar, indaga un poco más, solicita información que te permita verificar la veracidad de la información.
  - Cuando se trate de ofertas o solicitudes asociadas a productos financieros, comunícate directamente con la entidad para confirmarlas.

    Recuerda que las entidades oficiales no te pedirán que proporciones verbalmente ningún número de identificación personal, contraseña bancaria o datos de cuentas y tarjetas.

RIESGOS DE CONTENIDO

Son aquellos derivados del mal uso que se da al contenido que se consulta o se comparte en el entorno digital.

1. Deepfakes

Los deepfakes (mentiras profundas) son imágenes, videos o audios en las que se reemplaza la cara o voz de una persona por otra, utilizando inteligencia artificial. Tales videos de falsificación pueden ser creados, por ejemplo, sobre un actor o personaje del espectáculo para que aparezca en el video falso con contenido sexual, escenas de películas o series con otros protagonistas dando información falsa o solicitando información con fines de estafas.

- **Principal público impactado:** Adolescentes y adultos.
- **Cómo nos exponemos:**
  - Dejando pública información como fotos o videos.
- **Buenas prácticas:**
  - Evita compartir videos virales en los que se comprometa la buena imagen de otras personas.
  - Verifica la veracidad y autenticidad de este tipo de contenido en una fuente confiable.
  - Configura la privacidad de tus cuentas de redes sociales y asegúrate de que tus contactos hacen parte de tu círculo de confianza o son personas conocidas. **Conoce cómo configurar tus cuentas de forma segura.**

Haz clic aquí

2. Fake news o noticias falsas

Son noticias falsas que circulan a gran velocidad por redes sociales y medios de comunicación como: prensa, radio, televisión y cuyo objetivo es la desinformación, estafar o hacer alguna broma.

- **Principal público impactado:** Adolescentes y adultos.
- **Cómo nos exponemos:**
  - Cuando accedemos a millones de contenidos sin verificar su procedencia. La rapidez con la que se propaga hoy en día la información y la falta de criterio a la hora de compartir todo lo que nos llega sin antes verificar su fuente, incrementa el impacto que puede generar la desinformación
- **Buenas prácticas:**
  - No compartas ni creas en información que no haya sido confirmada por medios confiables.
  - Lee la información completa, no te quedes solamente con el título y analiza la coherencia antes de sacar conclusiones o compartir.
  - Revisa las fechas, debido a que en muchas ocasiones estas noticias falsas se valen de información o de hechos ocurridos varios años atrás.
  - Duda si la información es muy sorprendente, no cita fuentes oficiales, no se puede corroborar por otros medios, o es recibida de manera anónima; pues tiene alta probabilidad de ser una noticia falsa o inexacta.[3]

[3] https://mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/125614:Cinco-claves-para-no-caer-en-las-fake-news

3. Oversharing:

Es la sobre exposición de información en las redes sociales, donde se comparte información personal como: edad, nombre completo, número de celular, profesión, gustos, intereses, lugares favoritos, personas cercanas. Esto supone información de fácil acceso y aprovechable por personas malintencionadas poniendo en riesgo la seguridad de la persona y de quienes la rodean.

- **Principal público impactado:** Niños, niñas, adolescentes y adultos.

- **Cómo nos exponemos:** Publicando o compartiendo de manera excesiva datos, hábitos e intereses propios o de terceros, incluso enviando la ubicación en tiempo real.

- **Buenas prácticas:**

    - No compartas en tus redes sociales información personal en exceso que pueda ser utilizada con malas intenciones.

    - Evita indicar tu ubicación en tiempo real.

    - Piensa en el impacto de lo que publicas.

    Configura adecuadamente la privacidad de tus redes.
    Conoce cómo configurar tus cuentas de forma segura.

    Haz clic aquí

    - Respeta la intimidad de otros, solicita su autorización a la hora de publicar contenido que los incluya.

4. Sextorsión

Se da a partir de la práctica del sexting, conocido también como sexteo, y se refiere a la producción, envío y/o recepción de mensajes con contenido sexual por medio de internet. Este fenómeno implica la exposición de la propia expresión sexual en medios digitales. Aunque el intercambio de imágenes, mensajes o videos se lleve a cabo dentro de un marco supuesto de confianza y privacidad, siempre estará la posibilidad de que ese material sea compartido a otros o se pierda el dispositivo en el cual se encontraba almacenada, y pueda convertirse en insumo de chantaje con amenazas sobre compartir esta información, o de agresión sexual, conocidos como sextorsión.

- **Principal público impactado:** Adolescentes y adultos.
- **Cómo nos exponemos:**
  - Enviando contenido erótico o sexual donde se vea el rostro o características que permitan identificarte. Recuerda: una vez se comparten videos o fotografías se pierde por completo el control sobre ellas.
  - Al tener contenido sexual en tus dispositivos. Los celulares y computadores pueden ser robados o puedes perderlos y una tercera persona puede tener acceso a este tipo de contenido.
  - Usando contraseñas débiles. Es probable que intenten acceder a tus cuentas digitales en busca de contenido sexual para extorsionarte.
  - Al no contar con soluciones de seguridad en tus dispositivos, estás más expuesto a que programas maliciosos puedan acceder a tu información.

- **Buenas prácticas:**

  - Evita la producción, envío y/o recepción de mensajes con contenido sexual por medio de internet. Sé consciente y promueve el cuidado de la privacidad.

  - Usar contraseñas seguras y cambiarlas con frecuencia.

Conoce aquí cómo hacerlo

  - Configura las opciones de privacidad y seguridad (configurar correctamente los dispositivos y aplicaciones).
Conoce como hacerlo en las diferentes cuentas digitales.

Haz clic aquí

  - Si vas a realizar videos o tomar fotos con contenido sexual evita que aparezca tu rostro o alguna característica particular como tatuajes, cicatrices, lunares, que permita identificarte. Evita también detalles que permitan identificar el lugar donde las realizaste.

  - Si conservas fotos o videos íntimos en tus dispositivos, protégelos con mecanismos de cifrado y autenticación como una contraseña o pin de seguridad para dificultar el acceso por parte de terceros.

  - Desactiva el almacenamiento automático de las fotografías. Muchas aplicaciones guardan automáticamente todas las imágenes del teléfono en la nube y esto podría ser un problema si alguien más tiene acceso a estos espacios privados.

5. Shareting

Su origen viene de la combinación de las palabras sharing (compartir) y parenting (crianza). Es el uso habitual de las redes sociales por parte de los padres, como medio para compartir noticias o imágenes de sus hijos.[4]

[4] https://www.pantallasamigas.net/sharenting-riesgos-consejos/

- **Principal público impactado:** Niños, niñas y adolescentes.

- **Cómo nos exponemos:**

  - Al desconocer los ajustes de privacidad de las redes sociales y no tenerlas configuradas de manera segura.

  - Publicando o compartiendo fotos de los menores desnudos o en ropa interior: independientemente si están en una bañera, en la playa o recién nacidos.

  - Dando indicios de hábitos y ubicación frecuente de los menores.

- **Buenas prácticas:**

  - Asegúrate de que tus hijos estén siempre vestidos en las fotos que compartas.

  - Lee y entiende las políticas de privacidad de las redes sociales a las que se suben las fotografías.

  - Recuerda y ten siempre presente cómo se sentirían los niños si en un futuro se tuvieran que enfrentar a una imagen suya que subieron sus padres a Internet.

  - No compartas ubicaciones en tiempo real del sitio en el que se encuentren los niños.

  - Si envías imágenes o vídeos a través de mensajería instantánea (como WhatsApp), asegúrate de que las personas a las que envías dicho contenido, son de confianza y no lo compartirán sin tu autorización

Configura adecuadamente la privacidad de tus redes.
Conoce cómo configurar tus cuentas de forma segura.

Haz clic aquí

6. Doxing

Doxing, (viene de la abreviación informal DOCS – de documentos), técnicamente es un conjunto de estrategias destinadas a recopilar información de un objetivo, ya sea una persona u organización, a través de métodos que incluyen búsquedas en bases de datos de acceso público, redes sociales, Ingeniería social y vulneración de sistemas.

Sin embargo, la práctica no se queda simplemente en almacenar estos datos, sino que se utiliza este tipo de información privada como una forma de acoso por Internet, amenazando y extorsionando con hacer público lo que se ha descubierto sobre la víctima.

- **Principal público impactado:** Adultos.

- **Cómo nos exponemos: Con la huella digital que dejamos al navegar en internet,** pues normalmente, el doxing se aprovecha de esta, cuando dejamos comentarios y al interactuar y registrarnos en páginas web donde, a partir de esos datos, van recabando para encontrar información nuestra, como el lugar de residencia, el nombre de los amigos más cercanos, las aficiones, las opiniones políticas, o incluso confesiones y vídeos comprometedores.

- **Buenas prácticas:**

  - Configura adecuadamente la seguridad y privacidad de los perfiles sociales y demás cuentas digitales.
    Conoce cómo configurar tus cuentas de forma segura.

    Haz clic aquí

  - Evita compartir datos privados y sensibles en redes sociales.

- Haz un rastreo en internet con tu nombre, apellidos o número telefónico para identificar configuraciones de privacidad inadecuadas en cuentas digitales y toma medidas correctivas.
- Protege tu huella digital. ***Escúchalo aquí***
- Activa la alertas de google sobre la privacidad de tus datos.

7. Carding

Es el nombre que recibe el uso ilegitimo de la información financiera, o la estafa que realizan los cibercriminales vendiendo la información de las tarjetas de crédito, débito, o datos financieros extraídos de las victimas mediante otras técnicas como el Vishing.

Es una de las modalidades más usada de acuerdo a las estadísticas de fraude. Luego de obtener la información de la persona se hacen compras, especialmente de tiquetes aéreos, suscripciones a servicios, transporte y hasta pago de impuestos.

- **Principal público impactado:** Adultos.
- **Cómo nos exponemos:**
  - Entrando a páginas que no sean seguras. Los estafadores utilizan páginas de internet donde se hacen pasar por instituciones legítimas como bancos, universidades, hoteles o tiendas en línea, solicitando al usuario el ingreso de sus datos.
  - Entregando información personal a través de llamadas telefónicas. Los estafadores hacen una llamada haciéndose pasar por una entidad financiera o franquicia de tarjetas de crédito y se ofrecen muy amablemente a cambiar la tarjeta por una nueva y con mejores beneficios. Para este tipo de casos, jamás debes entregar la tarjeta de crédito o permitir que se la lleven; tú mismo debes encargarte de destruirla.
  - Al no contar con programas de protección (antivirus / antimalware) en nuestros computadores, donde a través de virus que se instalan pueden acceder a nuestra información.

- **Buenas prácticas:**

  - No pierdas de vista la tarjeta de crédito cuando estés realizando pagos o transacciones, ya que pueden tomar tus datos para hacer uso de ellos de manera fraudulenta en el futuro.

  - Al realizar compras en línea, debes verificar que la dirección del sitio comience con el protocolo de seguridad "https" y al inicio de la barra de dirección esté el ícono de un candado cerrado.

  - Evita utilizar redes o computadoras públicas para acceder a tus cuentas o hacer transacciones.

  - Haz uso de las E-cards de algunos bancos, con las que se generan tarjetas de crédito de un solo uso o una sola transacción sin necesidad de usar los datos de tu tarjeta física.

  - Conoce otras recomendaciones ***Haz clic aquí***

RIESGOS TÉCNICOS

Son aquellos que afectan la información que tenemos almacenada en nuestros dispositivos, o a los dispositivos como tal valiéndose de una brecha o vulnerabilidad en la seguridad.

1. Sim swapping

También conocida como 'SIM Duplicada' o secuestro de línea telefónica, es una modalidad que consiste en la suplantación del titular por parte del delincuente ante las empresas de telecomunicaciones, aprovechando: la falta de protocolos de verificación, que el titular de la línea se encuentra de viaje o no puede atender llamadas, y reportan la línea por pérdida o robo de teléfono.

Luego, sincronizan las redes sociales y productos financieros vinculados al número telefónico para validar accesos que les permitan generar transacciones fraudulentas. Es decir, el fraude se centra en explotar la capacidad de un operador de telefonía móvil para transferir sin obstáculos un número de teléfono a una nueva SIM. Lo que buscan los delincuentes por lo general es acceder a los códigos de verificación que empresas, plataformas y entidades bancarias suelen enviarnos a nuestros dispositivos móviles.

- **Principal público impactado:** Adultos.
- **Cómo nos exponemos:**
  - Cuando perdemos o nos hurtan el celular.
  - Cuando compartes públicamente o en redes sociales periodos de ausencia como viajes al extranjero, donde posiblemente no puedes usar la línea telefónica y, por tanto, no te darás cuenta del evento de forma oportuna.
- **Buenas prácticas:**
  - Si por algún motivo tu celular deja de recibir señal de telefonía, procede a referenciarte con otras personas que tengan el mismo operador. Si eres el único afectado contacta a tu proveedor del servicio para verificar la causa. Si han pedido alguna reposición de SIM Card en tu nombre, procede inmediatamente a bloquear tus cuentas bancarias y tarjetas de crédito.
  - No divulgues tu información privada o periodos de ausencia en redes sociales.
  - Evita al máximo enviar mensajes de texto SMS con información financiera o privada, ya que estos no están cifrados.
  - Mantén activo y actualizado tu antivirus.
  - Activa el doble factor de autenticación de las plataformas tecnológicas de los bancos y de las cuentas de correo electrónico en las que recibes normalmente notificaciones bancarias.

2. Malware

Es cualquier tipo de software malicioso que trata de infectar tus dispositivos. Los cibercriminales lo utilizan con múltiples finalidades, tales como extraer información personal o contraseñas, datos financieros o evitar que los propietarios accedan a su dispositivo.

- **Principal público impactado:** Niños, niñas, adolescentes y adultos.
- **Cómo nos exponemos:**
  - Al no contar con software antimalware en nuestros dispositivos.
  - Teniendo el software desactualizado.
  - Al abrir vínculos o descargar adjuntos de correos maliciosos (Phishing).
  - Conectando memorias USB desconocidas a los dispositivos.
- **Buenas prácticas:**
  - Mantén actualizado el sistema operativo y las aplicaciones de tus dispositivos.
  - Mantén un antivirus/ antimalware activo y actualizado en los dispositivos.
  - Ten precaución con los correos sospechosos o de remitentes desconocidos con sentido de urgencia que te incitan a abrir un archivo adjunto o ingresar a un vínculo.
  - No descargues información o software de sitios web desconocidos y evita dar clic a publicidades emergentes mientras navegas en internet.
  - Mantén respaldo de la información en la nube.

3. Ransomware: secuestro o robo de información

Es un tipo de programa informático malicioso que impide a los usuarios acceder a su sistema operativo o a sus archivos y que exige el pago económico de un rescate para poder acceder de nuevo a ellos. El ransomware tiene la capacidad de bloquear la pantalla de un computador o cifrar archivos importantes predeterminados con una contraseña; por lo general el rescate se exige en criptomonedas.

- **Principal público impactado:** Adolescentes y adultos.

- **Cómo nos exponemos:** al navegar en la web y abrir vínculos malintencionados o fraudulentos en correos electrónicos, Facebook, Twitter y otras redes sociales, o en los chats de mensajería instantánea. También es muy frecuente que este tipo de virus informático venga adjunto en un correo electrónico.

- **Buenas prácticas:**

  - Realiza copias de seguridad en la nube o en dispositivos extraíbles como USB o discos externos (Backup).

  - Mantén actualizados los sistemas operativos y programas informáticos para evitar brechas de seguridad.

  - Ten instalado antivirus / antimalware y mantenlo actualizado.

  - Evita navegar por sitios web desconocidos o poco confiables.

  - Evita descargar archivos adjuntos de correos sospechosos o de remitentes desconocidos.

Conocer los riesgos digitales, entender cómo funcionan, cómo nos exponemos a ellos y cómo prevenirlos es fundamental para protegernos en el entorno digital. Recuerda que en la cadena de seguridad eres el eslabón más importante. Unos hábitos digitales adecuados y las herramientas en las que te apoyes para cuidar tu seguridad en la web son fundamentales para estar allí.

Aprende, empodérate y disfruta del entorno digital y todas las posibilidades que te ofrece.

¡Aprende más con el
Centro de Protección Digital SURA!

Conócenos aquí