RECOMENDACIONES DE SEGURIDAD EN LA RED

Existe una gran cantidad de riesgos a los que te encuentras expuesto mientras estás en internet, por lo que a continuación te resumimos gráficamente algunos de los principales riesgos y recomendaciones:

PROBLEMA	DESCRIPCIÓN	RECOMENDACIÓN
 PHISHING	Emails o sitios web engañosos tratando de robar tu información personal y datos (contraseñas o tarjetas de crédito).	Verificar el remitente, no clickear en enlaces sospechosos y nunca compartir información sensible vía email.
	**CONTRASEÑAS DÉBILES** Contraseñas fáciles de adivinar o reusando la misma para múltiples cuentas	Crear contraseñas únicas y complejas (mezcla de caracteres) y usar una herramienta de administración de contraseñas
	**MALWARE Y VIRUS** Programas maliciosos que infectan, roban datos o causan daño.	Usar antivirus, mantener los sistemas operativos y aplicaciones actualizadas, y hacer descargas únicamente desde fuentes confiables.

¿QUÉ TIPOS DE AMENAZAS PUEDES ENCONTRAR EN LA RED?

Las principales y más comunes amenazas que puedes encontrar son:

Programas maliciosos (malware)

El término malware (del inglés malicious software) es un nombre general para cualquier programa de computadora creado con malas intenciones. Su objetivo es molestar, dañar o robar información de tu computadora, tablet o teléfono. Es como si alguien creara un virus para tu dispositivo.

Existen muchos tipos de malware, como los virus, gusanos, los troyanos, el spyware y el adware, entre otros.

Spyware

El spyware es un tipo de malware que se esconde en tu dispositivo para espiarte sin que te des cuenta. Su nombre viene del inglés spy (espía). Su principal meta es robar tu información personal, como tus hábitos de navegación, las contraseñas que escribes o tus datos bancarios.

Este programa puede ser muy astuto y hasta puede cambiar la configuración de tu dispositivo. Por ejemplo, puede hacer que tu internet sea más lento o cambiar la página de inicio de tu navegador sin que tú lo autorices. También existen programas como los keyloggers (registradores de teclas) que son un tipo de spyware que registra todo lo que escribes en el teclado y a veces son instalados por los mismos dueños de los dispositivos con el fin de monitorear su uso.

Spam

El spam se refiere a todos esos mensajes no deseados que recibes sin haberlos solicitado. Aunque el más común es el correo electrónico, también puede aparecer en otras formas, como mensajes de texto, en foros de internet, en las redes sociales, o incluso en los comentarios de blogs.

Phishing

El phishing es una técnica de estafa digital que se utiliza para robar información personal. Los estafadores se hacen pasar por una empresa o entidad en la que confías, como un banco o un servicio de streaming. Suelen enviarte un correo electrónico o un mensaje para que hagas clic en un enlace falso que te dirige a una página web idéntica a la original. Una vez allí, te piden que ingreses tus datos personales, como contraseñas o números de tarjeta de crédito, y así roban tu información.

Pharming

El pharming es una estafa más avanzada que el phishing. En lugar de usar un correo para engañarte, este ataque te desvía automáticamente a una página web falsa, incluso si escribes la dirección correcta en tu navegador. Esto lo logran modificando la configuración de tu conexión a internet o a través de programas maliciosos que ya están en tu computadora. La idea es que te confíes al ver la dirección correcta y caigas

en la trampa, creyendo que estás en la página real, cuando en realidad estás en una página fraudulenta.

RECOMENDACIONES DE SEGURIDAD

Es importante que prevengas el riesgo siguiendo las siguientes recomendaciones de uso responsable y seguro del servicio:

Contenido ilegal

Nunca alojes ni compartas contenido de pornografía infantil. Esto está prohibido por la ley, tanto a nivel nacional como internacional. Si ves o encuentras este tipo de material, denúncialo inmediatamente a las autoridades.

Evite Alojar, publicar o trasmitir información, mensajes, gráficos, dibujos, archivos de sonido, imágenes, fotografías, grabaciones o software que en forma indirecta o directa se encuentren actividades sexuales con menores de edad, en los términos de la legislación internacional o nacional, tales como la Ley 679 de 2001 y el Decreto 1524 de 2002 o aquella que la aclare, modifique o adicione o todas las leyes que lo prohíban.

Protección contra virus y programas maliciosos

Para mantener tu equipo seguro, sigue estos consejos:

Para mantener tu equipo seguro, sigue estos consejos:

- **Instala un buen programa de seguridad.** Usa un antivirus de una marca reconocida y de confianza para protegerte contra virus, programas espía y otros peligros de internet. Además, **usa siempre un firewall** para bloquear posibles ataques.
- **Actualiza tu sistema operativo y navegador.** Asegúrate de que tu computadora, celular y navegador web tengan siempre las últimas actualizaciones de seguridad. Estas actualizaciones corrigen fallos que los ciberdelincuentes pueden aprovechar.
- **Ten cuidado al navegar.** Evita entrar a páginas web extrañas o descargar programas de lugares que no te den confianza. Muchos programas gratuitos de intercambio de archivos (P2P) pueden venir con software espía oculto.
- **Deshabilita funciones innecesarias.** Si no las usas, es mejor desactivar funciones como las ventanas emergentes (pop-ups), Java, o la reproducción

automática de videos. Esto reduce las puertas de entrada para los programas maliciosos.

Seguridad en el correo electrónico

El correo electrónico es una de las herramientas más comunes para los ataques, así que ten mucho cuidado:

- **Protege tu dirección de correo.** No la publiques en sitios web poco confiables, ya que podrías recibir mucho correo no deseado (spam).
- **No compartas tu cuenta.** Si alguien usa tu correo para algo ilegal, la responsabilidad será tuya.
- **No envíes información personal por correo.** Evita compartir datos sensibles como contraseñas, números de tarjeta o información personal.
- **Desconfía de los correos de alerta.** Si recibes un correo de tu banco o de otra entidad pidiendo que ingreses datos, no respondas. Los bancos nunca te pedirán tu información personal por correo.
- **No hagas clic en enlaces sospechosos.** Si recibes un correo con un enlace que te parece dudoso, no lo abras. Es mejor escribir la dirección web directamente en tu navegador.
- **No reenvíes correos cadena.** Estos mensajes saturan la red y pueden contener información oculta en los encabezados que los ciberdelincuentes pueden usar.

Prevención de estafas (Phishing) y robo de información (Ingeniería social)

La "ingeniería social" es el arte de engañar a las personas para que revelen información.

- **Nunca compartas información confidencial.** No hables de temas personales o de trabajo con extraños, ya que esa información podría usarse en tu contra.
- **Ten cuidado con las llamadas o mensajes de texto.** No confíes en llamadas o mensajes que te pidan información bancaria o personal, incluso si dicen ser de una entidad conocida. Siempre valida la información directamente con la empresa.
- **Revisa la seguridad de los sitios web.** Antes de ingresar tus datos en una página, verifica que la dirección web comience con **https://** y que tenga un candado al lado. Esto indica que la conexión es segura.

Protección de contraseñas

Tus contraseñas son tu primera línea de defensa:

- **Tus contraseñas son personales, no las compartas.** No las divulgues a nadie. Si alguien más usa tu cuenta, debe usar su propio perfil.
- **Cámbialas seguido.** Lo ideal es cambiarlas al menos cada 30 días, siguiendo las recomendaciones de dificultad de cada aplicación.
- **Crea contraseñas fuertes.** Usa contraseñas que sean fáciles de recordar para ti pero difíciles de adivinar para otros.
- **Combina letras, números y símbolos.** Una buena contraseña debe tener al menos 10 caracteres y combinar mayúsculas, minúsculas, números y símbolos especiales (como !, ? o *).
- **Nunca envíes tus contraseñas por correo.** Un correo electrónico no es un medio seguro para compartir información tan sensible.

RECURSO TÉCNICO Y LOGÍSTICO DE SEGURIDAD EN LA RED

En cumplimiento de la resolución 3067 de 2011, Articulo 2.3 de seguridad en la red, CADCOM LTDA. dispone de mecanismos avanzados de Seguridad Perimetral. CADCOM LTDA. protege e identifica de manera temprana eventos e incidentes que atentan contra la confidencialidad, disponibilidad e integridad de la información y todos sus servicios son gestionados y monitoreados por el Centro de Operaciones y Monitoreo.

Para proteger las plataformas de los servicios de Internet, CADCOM LTDA. ha implementado configuraciones de seguridad base en los diferentes equipos de red, lo que comúnmente se llama líneas base de seguridad, además del establecimiento de medidas de seguridad a través de elementos de control y protección como:

Autenticación: CADCOM LTDA. cuenta con sistemas de autenticación y autorización para controlar el acceso a los diferentes servicios de la red, al igual que controles de autenticación para los usuarios (equipos terminales de acceso del cliente) -Recomendaciones UIT X.805 y UIT X.811-. Para el cumplimiento, CADCOM LTDA. tiene implementadas plataformas de autenticación de equipos terminales mediante la validación de la direcciones MAC (Media Access Control) y listas de direcciones IP fija asignadas por el personal técnico correspondiente, además dispone de procesos y políticas de seguridad mediante contraseñas y direcciones IP autorizadas para el acceso conocido únicamente por el personal técnico encargado para evitar la violación y alteración de los datos en los equipos terminales y en los equipos de transporte de la red.

Firewall: Adicionalmente CADCOM LTDA. cuenta con soluciones de cortafuegos y con una arquitectura de alta disponibilidad que garantiza la protección de los datos y la seguridad de la información que crean, distribuyen, trasmiten nuestros usuarios a través de la red de internet de CADCOM LTDA.

Acceso: Para prevenir la utilización no autorizada de un recurso, de acuerdo con las recomendaciones UIT X.805 y UIT X.812, cada equipo terminal debe ser registrado en al menos 2 equipos que hacen parte la red CORE en los filtros de listas de acceso, quienes autentican el dispositivo en cuestión y permiten su paso por la red de Internet de CADCOM LTDA.

Seguridad a nivel del CPE: Los dispositivos de conexión final ubicados en las premisas de los clientes de la red de internet de CADCOM LTDA cuentan con elementos bases para la autenticación y autorización, con ello permiten hacer una conexión a Internet de manera más segura.

Antivirus: Tanto las estaciones de trabajo como los servidores de procesamiento interno de información en CADCOM LTDA. están protegidos a través de sistemas anti-códigos maliciosos.

Antispam: Todos los servidores de correo poseen antispam que reduce el nivel de correo basura o no solicitado hacia los clientes, descongestionando los buzones y el tráfico en la red. CADCOM LTDA. continuamente evalúa el número de paquetes en la red desde direcciones IP específicas para ayudar a proteger a los usuarios ante correos o peticiones sospechosamente masivas por un periodo de tiempo.

Principio de Disponibilidad: (Recomendación X.805: Garantizar que las circunstancias de la red no impidan el acceso autorizado a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones). CADCOM LTDA. cuenta con un esquema de operación redundante en puntos críticos de la red principalmente en la red CORE, contando con al menos dos proveedores de capacidad (carriers) en salida hacia Internet, equipos de red de contingencia y archivos de configuración y de información guardados en copias de seguridad, listos para ser restablecidos en el menor tiempo posible en caso de falla de alguno de los elementos que componen la red de transporte de datos.

Filtrado de URLs: Para el bloqueo de sitios con contenido de pornografía infantil, CADCOM LTDA. utiliza servidores DNS para realizar el filtrado de estos sitios. El grupo administrador solicita mensualmente al MINTIC el listado de URL reportados que todos los proveedores de redes y servicios de telecomunicaciones tenemos la

obligación de bloquear. Una vez se detecta que ha sido publicado un nuevo listado, se descarga y se le aplica una migración para crear un archivo en texto con formato de zonas DNS basándonos en su domino. Una vez se tiene el listado depurado se procede a generar un requerimiento a través de un cambio estándar en lo servidores DNS y plataforma de resolución empleados por CADCOM Ltda., posteriormente, se documenta el cambio que queda como resultado del aprovisionamiento y se reinician los servicios de resolución de nombres.

En síntesis, el usuario solicita la página y se crea una consulta DNS con el fin de conseguir la dirección IP del URL reportado. Las direcciones IP de cada uno de los URL son propagadas vía protocolo BGP hacía los enrutadores de CADCOM Ltda., con el fin de que se informe que cualquier petición de consulta hacía los URL señaladas se resuelvan y dichas direcciones IP sean re-direccionadas a la plataforma de filtrado con el fin de que se revise si en la petición de consulta concuerdan tanto la dirección IP resuelta como el URL reportado. Si hay concordancia y está dentro del listado reportado por el MINTIC, automática se re-direcciona a una página que da información del bloqueo del sitio y su motivo al estar accediendo a una página de contenido de pornografía infantil. Si no hay concordancia en la plataforma de filtrado, el paso a seguir es re-direccionar la consulta hacía los enrutadores de Cadcom Ltda. para que salga a Internet y el URL pueda ser consultado.

Conforme con lo anterior es importante llamar la atención frente a la imposibilidad técnica y jurídica que tiene CADCOM Ltda. cuando estamos frente al bloqueo de dominios de alto tráfico, pues si se aprovisiona una URL con esta característica el servidor DNS, hará que la dirección IP correspondiente sea redireccionada a la plataforma de bloqueos y, por ejemplo si estamos frente a una URL relacionada con Facebook, se bloquearan contenidos que no necesariamente son de pornografía infantil; dichos bloqueos se propagarán a todas las consultas que tengan concordancia con dicha IP y con las URL identificadas, generando así bloqueos generalizados y afectando el rendimiento de la plataforma de filtrados debido a que Facebook es una página que tiene millones de consultas masivas a diario y la plataforma no tiene la capacidad de manejar un tráfico de tal magnitud, además que, de bloquear este tipo de páginas, se terminaría atentando contra la intimidad, la libertad de expresión y principios como la neutralidad de la red y la inviolabilidad de las comunicaciones de los usuarios, pues no serán bloqueados de manera selectiva los contenidos relacionados con pornografía infantil. Algo similar ocurre cuando se insta a CADCOM ltda. a bloquear contenidos acompañados del protocolo HTTPS, pues este

es un protocolo seguro que para lograr el bloqueo de contenidos particulares es necesario implementar el bloqueo completo del dominio.

En tal virtud, el bloqueo de contenidos que adelanta de manera particular CADCOM Ltda. responde a las obligaciones legales vigentes y con el objetivo principal de denegar el acceso a los sitios que contengan o promuevan la pornografía infantil en Internet a través imágenes, textos, documentos y/o archivos audiovisuales. Se sugiere instalar además sistemas parentales.

Conforme lo dispone el artículo 5.1.2.3.1 de la Resolución CRC 5050 del 2016, modificada por la Resolución CRC 5569 del 2018, CADCOM LTDA. dispone e implementa una Política de Seguridad de la Información de acuerdo con los criterios regulatorios y estándares internacionales vigentes.

Con el fin de asegurar el Principio de Confidencialidad e Integridad de datos y que la información de los usuarios no se pondrá a disposición de entidades o personas no autorizadas (Recomendaciones UIT X.805, X.814 y X.815), CADCOM LTDA. tiene definido una Política de Tratamiento de Datos Personales, que garantiza que la información no será compartida en ninguna circunstancia, a excepción de disposición de un ente con una orden Judicial bajo una búsqueda selectiva.

La red de Internet de CADCOM LTDA. está completamente segmentada, por lo que reduce la probabilidad de que el tráfico sea interceptado por otro dispositivo de la red sin autorización; además, cuenta con mecanismos de cifrado (encriptación) en los dispositivos de transporte, que reducen la posibilidad de que la información de usuario de extremo transportada, procesada o almacenada por una aplicación de red, sufra la modificación, la supresión, la creación y la reactuación sin autorización.