CIBER - SEGURIDAD

EN REDES DE TELECOMUNICACIONES MÓVILES

CCIT tictac SAFE

Equipo TicTac

Desarrollo del proyecto:
CR (RA) Fredy Bautista García
Lorena Mesa Guzmán

Colaboradores
CrowdStrike
Carlos Robledo - BDM seguridad en la nube de
Fortinet Colombia y Ecuador

Diseño y diagramación:
Paula Cruz Giraldo
Luisa Blanco Lemus

Sobre el TicTac
El TicTac es el primer tanque de análisis y creatividad del sector TIC en Colombia, establecido por la CCIT con el fin de proponer iniciativas de política pública orientadas a la transformación digital del país, con base en la sostenibilidad y competitividad económica, la inclusión social y la eficiencia gubernamental.

CIBER - SEGURIDAD

EN REDES DE

TELECOMUNICACIONES MÓVILES

CROWDSTRIKE FORTINET

Contenido

1	Prólogo	05
2	Introducción	07
3	Comportamiento de las cifras del cibercrimen 2022	09
4	Revelando la web abierta, deep web, dark web y más	16
5	Seguridad de redes móviles para redes 4G y 5G	26
6	La ciberseguridad proactiva	33
7	Referencias	39

01

PRÓLOGO

Alberto Samuel Yohai
Presidente Ejecutivo CCIT

Los riesgos cibernéticos hacen parte de la realidad de las sociedades de la información desde hace años. Precisamente, con la masificación de las TIC, la profundización de soluciones de la Cuarta Revolución Industrial y el aumento de transacciones en entornos digitales, las organizaciones deben trabajar por seguir el paso a las exigencias de ciberseguridad a nivel global.

Por esto, la ciberseguridad juega un rol central en la economía digital y la sociedad contemporánea, pues no solo las personas están expuestas a ataques de diferentes tipos, sino también las organizaciones públicas y privadas se han convertido en un blanco atractivo para los delincuentes cibernéticos.

En ese sentido, este nuevo estudio, realizado en el marco del programa de Seguridad Aplicada al Fortalecimiento Empresarial (SAFE), enfocó sus esfuerzos en analizar las diferentes vulnerabilidades que pueden presentarse en las redes de telecomunicaciones móviles, que son usadas por millones de usuarios para hacer todo tipo de actividades, y por ende la prioridad está en tomar las medidas necesarias con el fin de identificar y evitar posibles ataques.

Los operadores móviles se enfrentan a uno de los retos más importantes de los últimos años, que es brindar mayor y mejor seguridad a su creciente número de usuarios. Cada que se desarrollan nuevos servicios y funcionalidades, los ciberatacantes buscan nuevas maneras para robar información, recursos y afectar la disponibilidad de los servicios, usando sofisticadas herramientas, que se convierten en nuevas amenazas. Por esto, vemos necesario que las soluciones de ciberseguridad para redes de telecomunicaciones móviles tengan una visión integral de en dónde estamos y para dónde vamos en materia de ciberseguridad, tanto a nivel local, como internacional.

Siendo así, nos genera mucha satisfacción ver como la cadena de valor de las tecnologías de la información y las comunicaciones en Colombia, están trabajando mancomunadamente para asegurar un ambiente que protege a los usuarios.

02

INTRODUCCIÓN

Desde que inició el programa de Seguridad Aplicada al Fortalecimiento Empresarial (SAFE) en 2019 se ha venido trabajando por apoyar a todas las empresas del país, a través de nuestros estudios, con los cuales se busca concientizar sobre la importancia de proteger la información y más aún cuando muchas compañías han decidido trabajar de forma remota. Si bien esta modalidad ha traído muchas ventajas, es evidente que requiere de mayor atención cuando de ciberseguridad se trata.

Los documentos disponibles del programa se han enfocado en temas de seguridad de la información y sus diferentes aristas. Los temas han tocado puntos desde las buenas prácticas, pasando por los entornos cotidianos, las tendencias del cibercrimen, los ataques que se han visto en las entidades de gobierno, la seguridad en dispositivos móviles hasta informes de evaluación, retos y amenaza que puede sufrir las compañías, para darle así un campo más amplio y completo a este tema de gran importancia.

Para este nuevo estudio, se analizarán las redes de telecomunicaciones móviles, que también son objeto de ataque, sin duda, los operadores de este tipo de redes se han tenido que enfrentar al desafío constante de brindarle seguridad y confianza a sus usuarios cumpliendo al mismo tiempo con las obligación que los rige de proteger la seguridad pública.

Cada vez que se amplía el abanico de productos y servicios más avanzados, también se incrementa el número de posibilidades para nuevas amenazas, por ello, la labor de los operadores está en tener las soluciones necesarias y contar con una visión más amplia para hacerle frente a los ciberdelincuentes.

Este nuevo estudio se enfocará en las diferentes alternativas y buenas prácticas que hay disponibles para proteger las redes de telecomunicaciones móviles. Finalmente se entregará el estado actual de las tendencias del cibercrimen a cierre del tercer trimestre de 2022 y las recomendaciones que desde la experiencia de nuestros aliados se deben tener presentes para seguir combatiendo este flagelo.

03

COMPORTAMIENTO DE LAS CIFRAS DEL CIBERCRIMEN

3T 2022

Escrito por: CR (RA) Fredy Bautista García

La cifra de Ciberdelitos denunciados en Colombia durante el 2022 ha crecido un 20.5% respecto al 2021.

Según el reporte de la National Cyber Security Index (NCSI) , Colombia ocupa el lugar 65 en el ranking global que mide el nivel de seguridad cibernética de un país, su preparación para prevenir amenazas cibernéticas y su capacidad para gestionar incidentes cibernéticos, delitos y crisis a gran escala.

Los indicadores del estudio demuestran la necesidad de seguir fortaleciendo las medidas implementadas tras la publicación en 2020 de la Política Nacional de Confianza y Seguridad Digital cuyo plan establece acciones para analizar la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías a fin de preparar al país para enfrentar los desafíos de la cuarta revolución industrial (4RI). La implementación de las acciones de esta Política definió actividades hasta el año 2022.

Fuente propia

54.121 DENUNCIAS
01 enero 2022 - 31 octubre 2022

42.998 DENUNCIAS
01 enero 2021 - 31 ocubre 2021

Pese a los esfuerzos y avances logrados en Colombia, los ciberdelitos siguen creciendo y así lo demuestran las cifras del Centro Cibernético Policial, que indican que el número de casos denunciados en lo corrido del año asciende a 54.121 reportes realizados por las víctimas ante el SPOA de la Fiscalía General de Nación y los canales de denuncia de la Policía Nacional .

Los registros superan en 11.223 casos respecto al 2021, cuando transcurridos diez meses del año se habían presentado 42.998 denuncias. Esta variación porcentual equivalente al 20.5% señala el crecimiento constante que se ha venido observando desde el inicio de la pandemia en marzo del 2020.

Análisis de los Delitos Más Denunciados

La motivación de los Cibercriminales basada en la rápida monetización de los ciberataques guarda una relación directa con los tipos penales (delitos) más denunciados. Es así como el Hurto por Medios Informáticos; en sus distintas modalidades sigue siendo el delito de mayor incidencia en el registro total de casos. Las cifras indican que en el periodo de tiempo evaluado (Enero-Octubre) se han presentado 20.787 denuncias; equivalentes a un 24% más que durante el 2021, cuando se habían registrado 15.618 casos.

El hurto por medios informáticos involucra la materialización de varias conductas informáticas previas tales como el robo de las credenciales de acceso a sistemas de banca virtual y móvil generalmente mediante ingeniería social e incluso la instalación de malware bancario a través del envío de correos malintencionados. Más información se encuentra disponible en el sitio Web de C2USER.

Si bien es cierto el número de Ciber fraudes denunciados es muy bajo respecto al total de transacciones de banca digital (alrededor de 700 millones de transacciones en Internet en 2021, según cifras de la SFC)[1], es importante explorar nuevos mecanismos de difusión y prevención basados en sensibilización y concienciación de los usuarios y del fortalecimiento de los sistemas de autenticación y accesos a servicios.

[1] Cifra presentada por el Superintendente Financiero, Jorge Castaño Gutiérrez, durante el 12° Congreso de Acceso a Servicios Financieros y Medios de Pago de Asobancaria en 2021.

El Ransomware sigue creciendo en Colombia

Las denuncias por el delito de Obstaculización ilegítima de sistema informático o red de telecomunicaciones crecieron 28%, al ser denunciados 318 casos (90 más respecto a 2021) en los cuales se impidió total o parcialmente el acceso a un sistema o red, característica propia en la ejecución de un ciberataque de Ransomware.

Estas cifras guardan una relación directa con el incremento de las denuncias presentadas por el delito de Violación de datos personales que registró 11.243 casos (250 más que en 2021). Es importante señalar que la fase extorsiva de un Ciberataque de Ransomware conlleva la obtención y posterior divulgación no autorizada de los datos extraídos de manera ilícita en una organización bajo ataque.

La regulación en materia de protección de datos fijada por la SIC (Superintendencia de Industria y Comercio) conlleva la obligación de reportar los incidentes de seguridad informática que involucren la fuga de datos personales en los primeros quince días hábiles después de identificado o notificado el incidente, lo que supone la urgencia de reporte y denuncia.

Fuente propia

El comportamiento global del Ransomware registró un aumento interanual del 105 %, y ha subido un 232 % desde 2019.

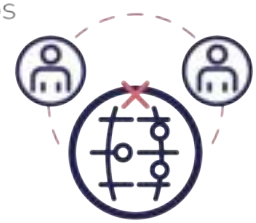
La intrusión informática como fase inicial de un Ciberataque mayor

El incremento del 39% en el número de denuncias por el delito de acceso abusivo a sistema informático refleja la creciente dinámica y actividad de los ciberataques en Colombia. En 2021 se habían registrado 7.026 casos en comparación con la cifra de 11.611 hechos denunciados en 2022 es decir una variación absoluta de 4585 casos más durante el periodo evaluado.

Existe consenso desde el abordaje jurídico-informático; respecto a la necesidad que tienen los atacantes de ganar el acceso a un sistema informático o red con el fin de desplegar otras actividades como el escalamiento de privilegios, o la dispersión de un malware.

Lo anterior permite suponer entonces que los 11 mil casos registrados como Acceso Abusivo a Sistema Informático pueden estar relacionados con otras afectaciones a la disponibilidad, confidencialidad e integridad de la información y los datos, no contempladas en el total de cifras en estudio, pues podría tratarse de accesos a dispositivos (servidores, móviles, equipos de cómputo, redes) en fases iniciales de la cadena de un Ciberataque: (Reconocimiento + Preparación). Gráfica Fases de un Ciberataque tomada del sitio Web del INCIBE.

Los atacantes suelen valerse de los accesos a los sistemas para dar paso a las fases de distribución y explotación de ciberamenazas, como ocurre en los despliegues realizados durante los ataque de troyanos bancarios o dispersión de malware (Ransomware).



Phishing o pesca de usuarios se mantiene estable

Las cifras de denuncias instauradas por infracción a la ley 1273/2009 en cuanto al delito de Suplantación de sitios web para capturar Datos personales se mantiene estable respecto al año 2021, la estadística dispone señala un leve incremento de 102 casos.

Durante el 2022 se han reportado 4.768 casos vinculados al diseño programación o envío de enlaces maliciosos con los cuales los cibercriminales consiguen redireccionar la navegación de los usuarios hacia sitios previamente preparados con malware o formularios para capturar datos personales.

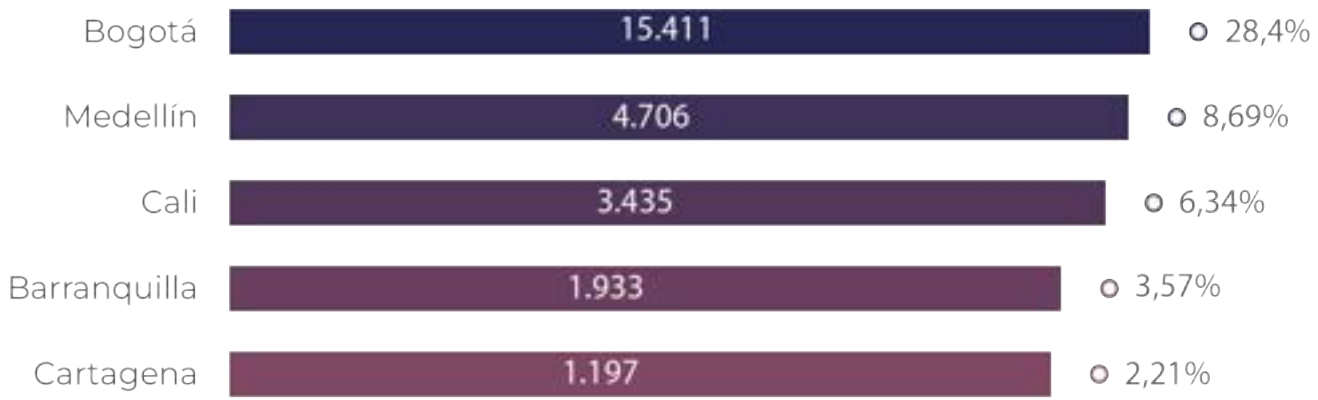
Sin embargo, es importante reconocer que la principal vía para la infección de los equipos posteriormente afectados sigue siendo el envío de correos spam de manera masiva con los cuales se busca engañar al usuario y robar principalmente las credenciales bancarias para la posterior suplantación ante las plataformas o aplicaciones de banca móvil o digital.

Las modalidades siguen migrando hacia el Spear Phishing y Smishing ataques más personalizados que generan una mayor tasa de éxito pues el estudio previo de las víctimas aumenta la probabilidad de interacción del usuario con el enlace fraudulento o contenido del correo malicioso.

Gráficas Smishing Fuente ColCERT

Cibercrimen, una problemática nacional

El reporte de denuncias por cibercrimen durante el 2022 señaló una distribución directamente relacionada con los índices de penetración o acceso a servicios de internet a nivel país; de tal manera que las ciudades con mayor interacción y acceso a internet y a servicios de banca virtual y comercio electrónico registran un mayor número de denuncias que aquellas áreas del país en las cuales se dificultan la conectividad y demás servicios de acceso a las tecnologías.



Fuente: Reporte de denuncias por cibercrimen 2022

Otras ciudades como Bucaramanga, Ibagué, Villavicencio y Pereira reportan porcentajes que oscilan entre el 1,91% y el 1.40% del total de denuncias registrando en promedio cerca de mil casos cada una durante el periodo en estudio. El Centro Cibernético de la Policía Nacional reportó durante el mismo periodo 179 capturas de personas involucradas en infracciones a la ley 1273 de 2009.

REVELANDO LA WEB ABIERTA, DEEP WEB, DARK WEB Y MÁS

Cómo identificar amenazas externas, proteger su marca y mitigar el riesgo

CROWDSTRIKE

El ciberdelito es desenfrenado. Internet está llena de foros turbios, mercados y comunidades donde los malos actores se congregan y las economías digitales clandestinas prosperan. Los adversarios buscan robar sus datos, explotar su marca y estafar a sus clientes. Hay que tener visibilidad de los rincones oscuros de la Web para identificar amenazas, enderezar posibles incidentes y minimizar el riesgo de sus activos críticos. Pero la mayoría de las organizaciones simplemente no tienen el tiempo, el presupuesto o el conocimiento para navegar por los rincones ocultos de Internet.

El costo total promedio de una violación de datos es de 3.86 millones de dólares. [1]

[1] Seguridad de IBM Costo de un informe sobre la brecha de datos 2020

LOS CIBERCRIMINALES SE ESTÁN EMBOLSANDO MILES DE MILLONES

El crimen cibernético es un gran negocio. Todo, desde credenciales robadas hasta números de tarjetas bancarias, datos confidenciales de clientes y propiedad intelectual, está disponible para la venta en áreas ocultas de Internet. Los adversarios de hoy disfrutan de una sólida economía clandestina y tienen un vasto ecosistema a su disposición.

Los malos actores pueden sacarle provecho a los kits de herramientas de código abierto y de ransomware, malware y phishing bajo demanda para realizar campañas y cometer delitos fácilmente. Los ciberdelincuentes pueden comprar y vender datos robados en innumerables mercados delictivos. Y los adversarios pueden incluso encontrar información confidencial, como credenciales de acceso en sitios abiertos y repositorios de códigos públicos como GitHub si saben dónde buscarlo. [2]

El delito cibernético puede perjudicar su negocio, afectar los resultados de su empresa, empañar su marca y dar lugar a severas multas regulatorias y costosos acuerdos legales. Los analistas de la industria de la seguridad estiman que los daños por delitos cibernéticos globales anuales alcanzarán los 6 billones de dólares en 2021.[3] Y según los informes de la industria, el costo total promedio de una violación de datos es de 3.86 millones de dólares, qu incluye costos directos, como los gastos forenses, e indirectos, como la pérdida de ingresos debido al daño a la reputación.[4]

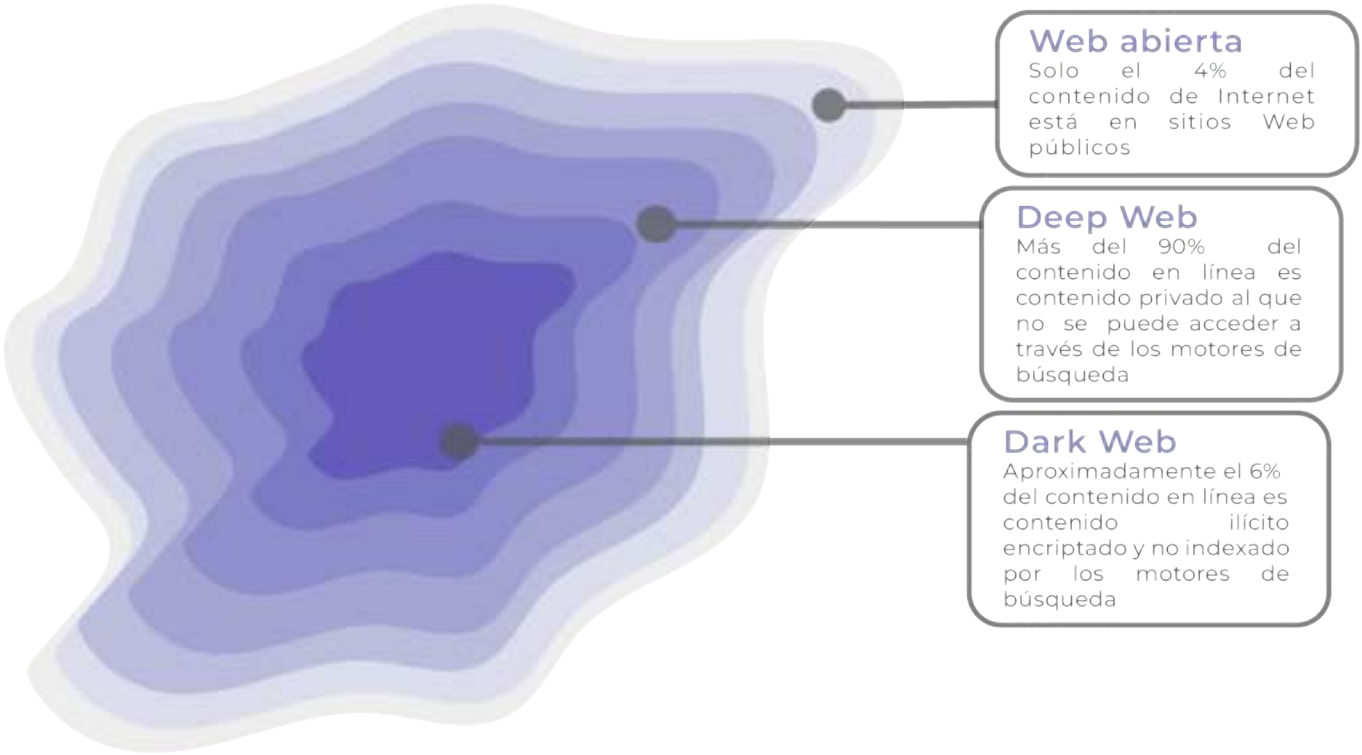
[2] Los desarrolladores a menudo codifican claves de API y datos personales en aplicaciones.
[3] Cybersecurity Ventures, noviembre de 2020
[4] Informe sobre el costo de la seguridad de IBM con una brecha de datos 2020

LAS AMENAZAS EXTERNAS SON EXTENSAS

Una amplia variedad de malos actores acecha en la deep y dark Web, y se esconden a plena vista en la Web abierta en blogs y sitios de redes sociales. Y para empeorar las cosas, adversarios operan más allá de la Web, utilizando plataformas de mensajería, aplicaciones móviles maliciosas y otras herramientas para llevar a cabo actividades ilícitas. Los ciberdelincuentes organizados, los actores patrocinados por el estado y los hacktivistas siempre encuentran nuevas formas de evadir la detección y causar estragos. Cada minuto de cada día su organización está expuesta a miles de agentes de amenazas que buscan oportunidades para explotar su marca, robar sus datos y engañar a sus clientes.

Táctica	Ejemplos de
Hacerse pasar por su marca en correos electrónicos, mensajes SMS, sitios de redes sociales, aplicaciones móviles y sitios web	› Ataques de phishing que recopilan credenciales y otros datos confidenciales de consumidores desprevenidos › Esquemas de falsificación que venden productos falsificados con su marca › Estafas en la cadena de suministro que engañan a los proveedores para que cometan fraude o robo
Robar y revender información y datos confidenciales de la empresa	› Credenciales (como nombre de usuario, contraseñas y claves API) para sistemas de TI y aplicaciones críticas para el negocio › Documentos internos, propiedad intelectual, datos confidenciales de los empleados y comunicaciones › Datos del cliente que incluyen información de identificación personal (IIP) e información de salud protegida (PHI) › Tarjetas de crédito corporativas, números SWIFT y números de pasaporte
Ejecutar fraudes en el sector minorista	› Tarjetas de regalo, códigos de cupón y puntos de fidelidad falsos
Compra y venta de malware, herramientas y servicios de piratería	› Keyloggers, ladrones de contraseñas y herramientas de pirateo de redes sociales › Kits de explotación, generadores de malware y troyanos › Servicios de cifrado, spam y deepfake

WEB ABIERTA, DEEP WEB y DARK WEB ¿CUÁL ES LA DIFERENCIA?



La web abierta incluye cualquier contenido que esté indexado por los motores de búsqueda y aparezca en los resultados de búsqueda en Google, Bing, etc.

La deep Web contiene una gran cantidad de contenido privado que no está indexado ni es accesible a través de un motor de búsqueda. Incluye todo lo que requiera credenciales de inicio de sesión e incluye contenido que bloquea explícitamente la indexación de los rastreadores de web.

Solo se puede acceder a la deep Web mediante un navegador especial como Tor (The Onion Router) o I2P. Es la parte más vulnerable de Internet y el hogar de información robada, bienes ilegales y una miríada de foros delictivos y actividades sospechosas.

UN ENFOQUE PROACTIVO ES SU MEJOR DEFENSA CONTRA LAS AMENAZAS EXTERNAS

Los malos actores pueden dañar la reputación de su empresa y costarle dinero. Usted debe adoptar un enfoque proactivo para identificar y mitigar las amenazas externas, pero tomar el pulso de manera regular en la vasta y dinámica red subterránea es una propuesta desalentadora que está fuera del alcance de la mayoría de las empresas.

Pocas organizaciones tienen el presupuesto necesario y las personas adecuadas para diseñar, implementar y administrar un motor de recopilación de datos escalable a nivel masivo. Y pocos saben cómo navegar por la parte más oscura de Internet.

Monitorear los rincones ocultos de la Web es una tarea importante:

Mantener el ritmo del cambio es un trabajo de tiempo completo. El ecosistema criminal está en constante evolución - siempre hay nuevos sitios, foros y actores a los que realizar un seguimiento.

Las credenciales de los sitios ilícitos son difíciles de obtener. El acceso a sitios ilícitos puede ser difícil porque algunos solo permiten el acceso por invitación.

Hay que ser inteligente y discreto. Si los malos actores saben que están siendo observados (o monitoreados por un bot), le van a bloquear.

Usted debe capturar y preservar continuamente datos de inteligencia por procesar. La actividad maliciosa puede ser transitoria. Los sitios pueden desaparecer en días o incluso horas, y los delincuentes con frecuencia eliminan las publicaciones incriminatorias, por lo que usted debe recopilar datos mientras sea posible hacerlo.

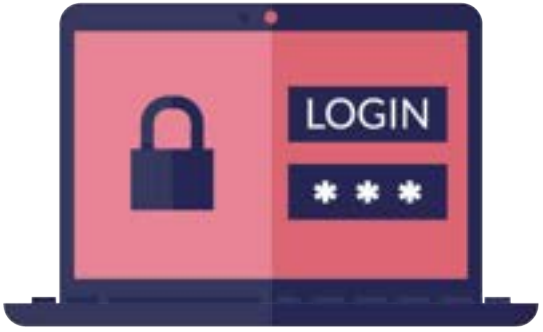
Si su empresa es como la mayoría, simplemente no tendrá el tiempo, el conocimiento o los medios para monitorear los rincones ocultos de Internet en busca de actividad maliciosa. CrowdStrike puede ayudar brindándole la experiencia, la tecnología y los profesionales dedicados para ayudarle a mantenerse un paso por delante de los delincuentes.

CROWDSTRIKE FALCON X RECON: RIESGO DIGITAL RECONOCIMIENTO PARA LA WEB ABIERTA, DEEP WEB, DARK WEB Y MÁS

CrowdStrike Falcon X Recon expone la actividad potencialmente maliciosa de la Web abierta, deep Web, dark Web y más, lo que le ayuda a aumentar la visibilidad, proteger su marca y reducir el riesgo. La solución recopila datos de manera proactiva y monitorea la actividad de millones de páginas Web restringidas, foros criminales, marketplaces, sitios de pegado, sitios de filtraciones, plataformas de redes sociales y plataformas de mensajería, lo que brinda información valiosa sobre el comportamiento sospechoso asociado con su marca.

Con Falcon X Recon, usted puede realizar consultas en tiempo real para descubrir fraudes, brechas de datos, campañas de phishing y otras amenazas cibernéticas. Además, la solución monitorea continuamente los sitios subrepticios en busca de actividad maliciosa, proporcionando una notificación automática de los riesgos potenciales.

Falcon X Recon se basa en la plataforma CrowdStrike Falcon® nativa en la nube para ofrecer la máxima simplicidad y rentabilidad. Con Falcon X Recon no hay nada que implementar o administrar, por lo que usted puede concentrar su valioso tiempo y sus recursos en identificar amenazas y proteger su negocio. La solución CrowdStrike® está respaldada por un equipo de profesionales experimentados dedicados a ayudarle a mejorar el conocimiento de la situación.



RECOPILAR

Falcon X Recon recopila, a escala, datos de inteligencia no procesados, extrayendo automáticamente datos de millones de páginas Web ocultas y miles de sitios restringidos donde los delincuentes se encuentran, compran y venden. La solución recopila datos de foros restringidos, marketplaces, tiendas de aplicaciones, sitios de pegado y más.

Con Falcon X Recon usted puede volar bajo el radar, recopilando datos de inteligencia en tiempo real de sitios ilícitos sin ser detectado. La solución captura y conserva datos para que los agentes de amenazas no puedan cubrir sus huellas eliminando publicaciones o sitios. Usted puede usar Falcon X Recon para identificar amenazas inminentes, interrumpir la acción de adversarios, y para tomar el pulso a la charla y la actividad delictivas. También puede usarlo para rastrear y examinar datos históricos para identificar tendencias y patrones de comportamiento.

INVESTIGAR

Falcon X Recon facilita la detección e investigación de amenazas externas a su empresa. La solución proporciona asistentes fáciles de usar, con criterios de búsqueda predefinidos como marcas, ejecutivos, dominios, vulnerabilidades y direcciones de correo electrónico. Usted puede realizar consultas ad hoc en tiempo real o monitorear continuamente la red clandestina, utilizando reglas personalizadas para filtrar de manera eficiente los datos de inteligencia sin procesar.

Falcon X Recon muestra los resultados de la investigación en tarjetas concisas y fáciles de entender. Usted puede ver las publicaciones originales del agente de amenazas, junto con el contexto sobre el agente y el sitio. Las publicaciones en idiomas extranjeros, incluida la jerga de los hackers, se pueden traducir instantáneamente al inglés. (La traducción automática admite 18 idiomas extranjeros).

NOTIFICAR

Falcon X Recon proporciona notificaciones automáticas de actividad sospechosa. Usted puede configurar reglas personalizadas para marcar comportamientos potencialmente maliciosos o delictivos. Puede categorizar y priorizar alertas, definir con qué frecuencia se generan (inmediata, diaria o semanalmente) y qué personas y equipos las van a recibir. Puede enviar alertas a los equipos de operaciones y seguridad de TI, así como a otras partes de la organización que necesiten conocer la pérdida de datos confidenciales, las estafas y el abuso, como los departamentos de marketing, jurídico, recursos humanos y fraude.

¿POR QUÉ FALCON X RECON?

Falcon X Recon proporciona una visión en profundidad de la Web subterránea, lo que le ayuda a identificar e investigar las amenazas externas a su negocio con una velocidad y cobertura incomparables. La solución CrowdStrike de alto rendimiento y escalabilidad masiva:

Recopila continuamente datos de más de 1 millón de fuentes únicas, mantiene más de 8 mil millones de páginas, mensajes y archivos, y extrae datos 24 veces más rápido que las soluciones de la competencia.

Otorga visibilidad de los datos históricos de la actividad del adversario.

Brinda más de 44 millones de indicadores de afectación.

Utiliza honeypots y honeynets repartidos por todo el mundo para atraer a los adversarios e identificar botnets, ataques DDoS y otras amenazas en línea para su empresa.

+8 MIL MILLONES

Archivos, publicaciones, etc.

+1 MILLÓN

Fuentes únicas

8 AÑOS

Datos históricos

+44 MILLONES

de indicadores de afectación

24X

Extracción más rápida

SEGURIDAD DE REDES MÓVILES PARA REDES 4G Y 5G

El papel cambiante de la seguridad en las redes y servicios móviles

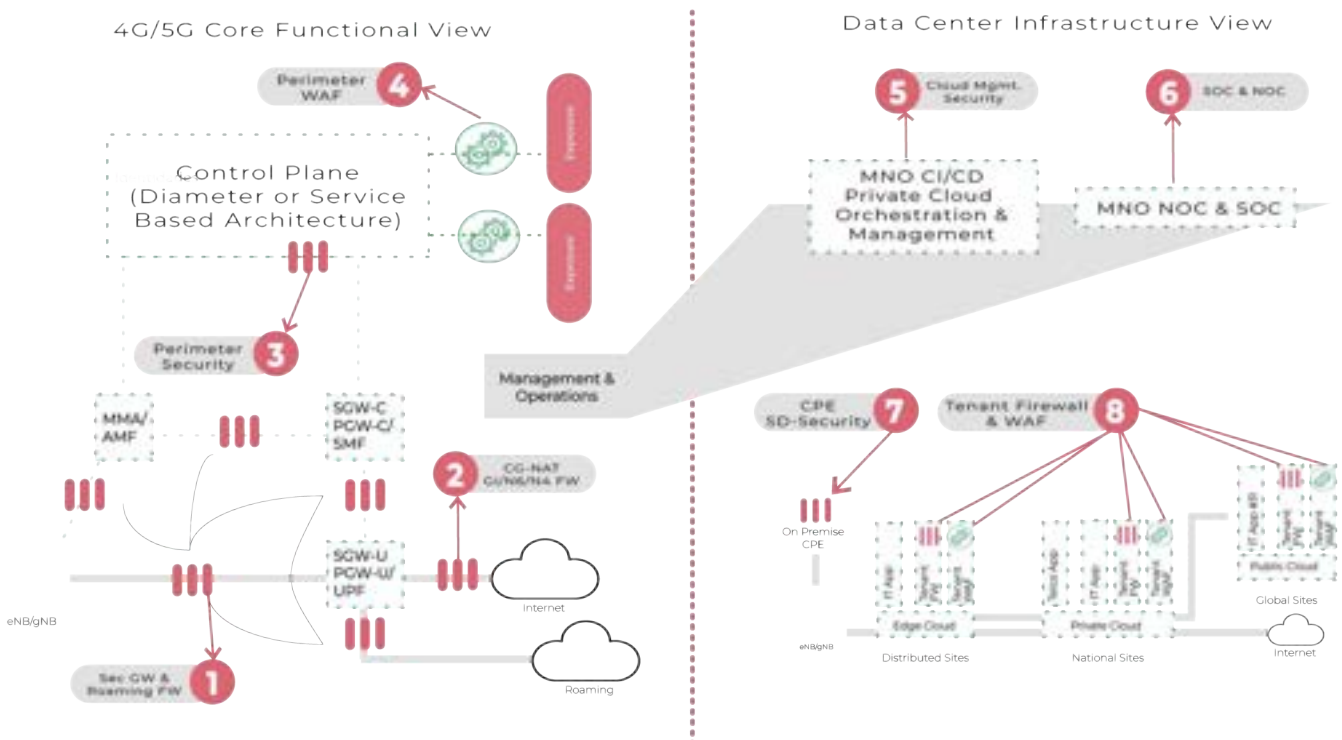
Escrito por: Carlos Robledo - BDM seguridad en la nube de Fortinet Colombia y Ecuador

FORTINET

La evolución de la tecnología en las redes móviles 4G y la introducción de la tecnología 5G ofrecen a los operadores de redes móviles (Mobile Network Operators, MNO) la oportunidad de realizar un cambio radical en los segmentos mercado a los que pueden dirigirse, el alcance de los servicios y el valor que ofrecen. Estas nuevas capacidades y servicios son fundamentales para permitir la innovación en cualquier industria, desde el sector manufacturero y de energía hasta el transporte, la logística y el cuidado de la salud.

La red 5G ofrece movilidad acompañada de una baja latencia, un alto rendimiento y una escalabilidad masiva, que en conjunto hacen posible la innovación, la automatización, la eficiencia y la seguridad. Las líneas de producción autoadaptables, el mantenimiento predictivo, la cirugía a distancia, las ciudades inteligentes y la administración del tráfico en tiempo real asistida por la IA son algunos de los casos de uso favorecidos por la 5G.

Las ventajas de la red 5G, que cambiarán el mundo, solo se pueden aprovechar si cuentan con la protección adecuada. La innovación digital que se produce en las redes móviles crea una función doble para la seguridad en entornos móviles. Ofrece seguridad de infraestructura móvil interna y seguridad y monetización de casos de uso externos.



Fortinet protege la innovación y permite el crecimiento

Fortinet ofrece un conjunto general de soluciones y herramientas de seguridad que permiten la visibilidad y el control de la seguridad de extremo a extremo para infraestructuras móviles 4G y 5G, además de hacer posible la seguridad y la monetización de los casos de uso de la industria. Este enfoque facilita tanto la integración como la incorporación mientras mantiene las operaciones y los esfuerzos de administración al mínimo, ya que la misma plataforma se utiliza constantemente en todo el ecosistema 5G.

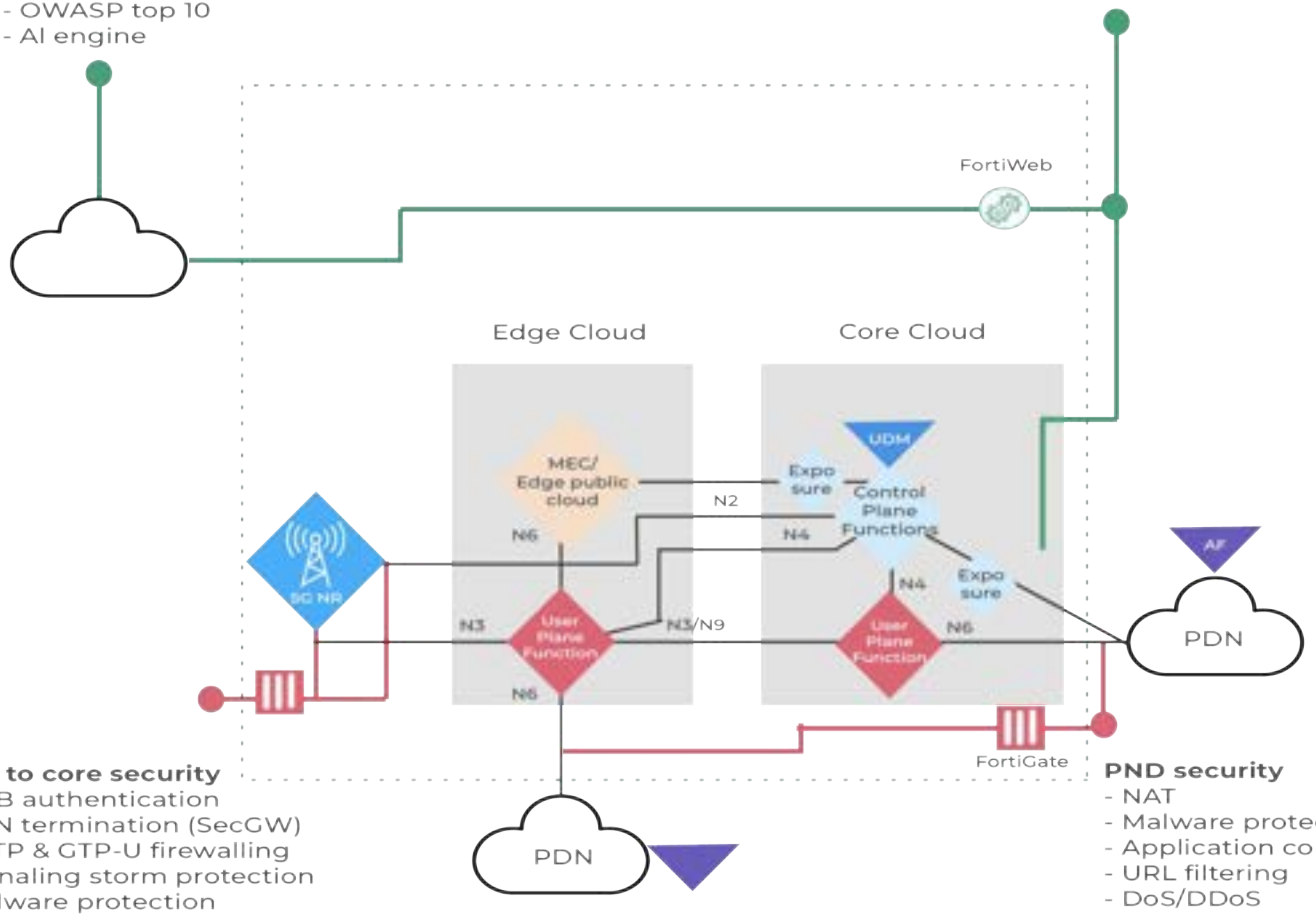
Entre los productos y servicios se encuentran el Firewall de próxima generación FortiGate (NGFW) y el Firewall de aplicación web (WAF) FortiWeb. En conjunto, permiten a los operadores de redes móviles impulsar de forma segura la innovación en tecnología, servicios y casos de uso para los segmentos de consumidores y empresas por igual.

Redes privadas 5G: Una oportunidad evidente

Las redes móviles que no son públicas, también conocidas como redes móviles privadas, ofrecen las ventajas de la tecnología 5G según las necesidades específicas de cada empresa, sus casos de uso, privacidad y control. Los puertos marítimos, aeropuertos, plantas de producción, compañías logísticas y productores de gas y petróleo pueden configurar una red móvil 5G privada acorde a su tamaño, infraestructura de OT e IoT, sus aplicaciones industriales, socios, etc. Existen distintas arquitecturas para la implementación de redes móviles privadas, que varían según las necesidades de cada empresa o industria y sus casos de uso, además de las distintas regulaciones y asignación por país. Garantizar su seguridad es una prioridad dada la importancia y criticidad de sus casos de uso.

API security
- OpenAPI 3.0 verification
- HTTP/2 support
- JASON & XML protocol comformance
- Schema validation
- Signature enforcement
- API GW functionality

Application security
- OWASP top 10
- AI engine



RAN to core security
- gNB authentication
- VPN termination (SecGW)
- SCTP & GTP-U firewalling
- Signaling storm protection
- Malware protection

PND security
- NAT
- Malware protection
- Application control
- URL filtering
- DoS/DDoS

Fortinet ofrece una plataforma de seguridad común para las distintas necesidades de las redes móviles privadas

Para ganar participación de mercado e ingresos, un operador de redes móviles (mobile network operator, MNO) debe proporcionar un conjunto de arquitecturas y servicios flexibles y seguros para satisfacer las distintas necesidades de diversas industrias con respecto a la red 5G privada. Entre ellas se pueden incluir consideraciones como costos, administración, privacidad de los datos, KPI de seguridad, etc.

Las plataformas FortiGate y FortiWeb de Fortinet ofrecen un conjunto común de herramientas avanzadas para la visibilidad y el control de la seguridad en una gran variedad de arquitecturas de red y casos de uso 5G. Esto permite a los MNO cumplir con los requisitos de seguridad, ya sea como parte de una oferta de red privada 5G, o bien como un conjunto de servicios de seguridad administrados. Algunas de estas ofertas son:

- Proteger los puntos expuestos en las arquitecturas de redes privadas (RAN, PDN y API).
- Proteger la red privada de las tormentas de señalización de la IoT y de conexiones anómalas.
- Seguridad para la computación en los bordes del acceso múltiple (Multi-access Edge Computing, MEC) contra amenazas y ataques al nivel de la aplicación.
- Proteger el ecosistema de API de la red privada frente a los ataques.
- Servicios de seguridad que generan ingresos para la empresa a través de la red móvil privada 5G.

La compatibilidad con la multitenencia nativa de Fortinet ofrece la mayor eficacia y rentabilidad como plataforma común para prestar servicios de seguridad en los segmentos privados de 5G, desde la RAN y hacia la nube Telco.

SEGURIDAD DE LA NUBE TELCO

Los operadores de redes móviles (MNO) confían en sus bases y capacidades tecnológicas para suministrar el alcance y la profunidad de sus servicios inalámbricos. Dado que los entornos comerciales, competitivos y tecnológicos se encuentran en medio de una rápida transformación digital, los MNO deben seguir el ritmo de las modernas tecnologías y arquitecturas para conservar su posición e impulsar la innovación y el crecimiento.

Hace falta una evolución fundamental, la evolución hacia el modelo de la nube Telco, para impulsar la eficiencia y la agilidad, ofrecer un mayor valor al cliente e impulsar el crecimiento.

A medida que las organizaciones contemplan incorporar servicios inalámbricos de computación de borde para fomentar la proliferación de la IoT, los trabajadores remotos y la innovación digital general, la red 5G permite que los MNO aporten valor más allá de la conectividad a los sectores verticales de una empresa. La nube Telco amplía todos los dominios operativos para ofrecer servicios ágiles y rentables a través de redes RAN y Core 4G y 5G, nubes privadas y públicas, y ubicaciones de computación en el borde de acceso múltiple. Esto aumenta la complejidad y amplía la superficie de ataque. Por lo tanto, los MNO deben implementar soluciones de seguridad sólidas para hacer frente a estos desafíos:

SEGURIDAD PARA LA NUBE TELCO

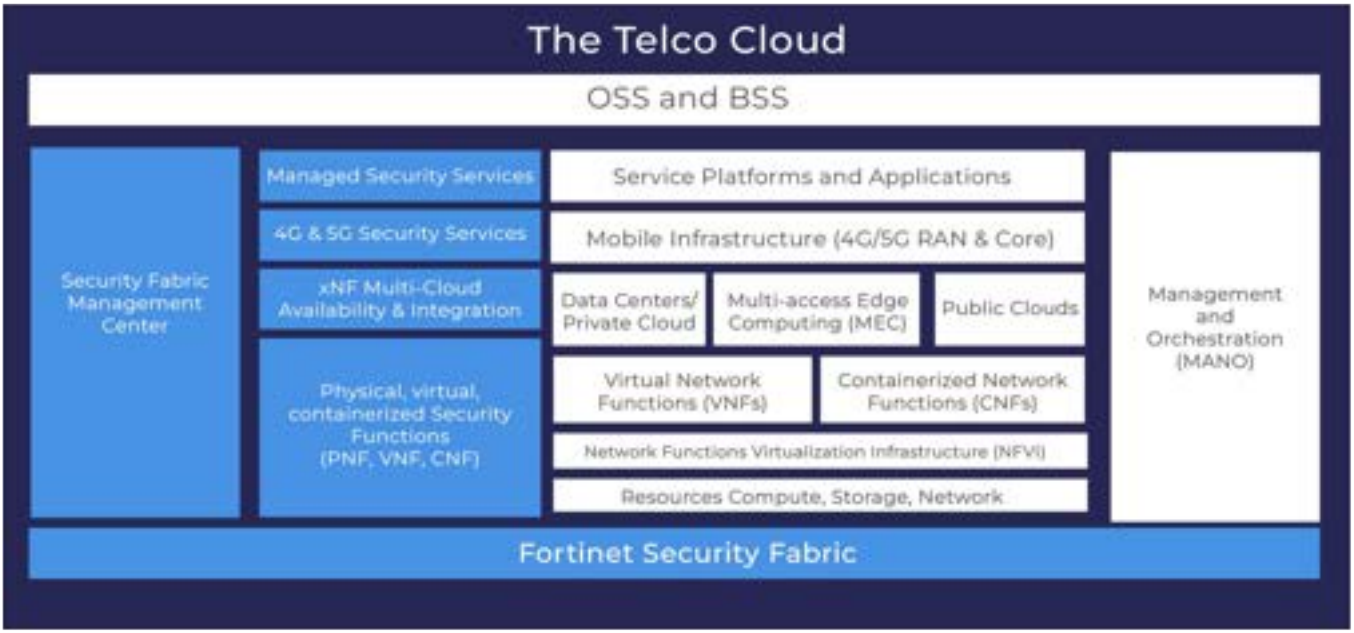
Garantizar que las tecnologías, aplicaciones y servicios que conforman la plataforma de servicios de la nube Telco estén correctamente protegidos para poder así garantizar la disponibilidad y la continuidad del servicio.

SEGURIDAD DESDE LA NUBE TELCO

La nube Telco como una plataforma de servicios, que permite suministrar y prestar servicios de seguridad a clientes internos y externos.

El Fortinet Security Fabric: La base de la seguridad en la nube Telco

Fortinet Security Fabric y la nube Telco utilizan las mismas bases tecnológicas. Entre ellas se encuentran la función de red virtualizada (VNF) de seguridad, las redes definidas por software (SDN), la función de red nativa de la nube (CNF), las API abiertas y las operaciones de seguridad (SecOps). Las mismas se implementan con compatibilidad con los requisitos específicos de los MNO, como la escalabilidad masiva, eficiencia, alto rendimiento y muy baja latencia. Al igual que la nube Telco, los componentes de Security Fabric se integran internamente para formar una plataforma de servicios de seguridad automatizada y perfecta que se integra externamente a las tecnologías, los componentes y las arquitecturas de la nube Telco para convertirse en una parte indivisible de la propia nube Telco.



LA CIBERSEGURIDAD PROACTIVA

Un nuevo enfoque para la gestión de las Ciberamenazas

HUAWEI

La capacidad de los cibercriminales para encontrar y aprovechar brechas de seguridad, evadir detecciones y ocultar actividades maliciosas se ha vuelto cada vez más sofisticada; casi de forma paralela al potencial que tienen las empresas en aprovechar nuevas infraestructuras para digitalizar servicios, ofrecer agilidad, posibilitar la transformación digital y, en consecuencia, aportar mayor valor a las organizaciones.

Este desafío continuo obliga a los directores de tecnología y responsables de seguridad informática a desarrollar un nuevo enfoque basado en la Ciberseguridad proactiva, que incluya herramientas de inteligencia de detección de amenazas y un cuidadoso entrenamiento tanto para el personal de TI y empleados de todas las áreas de la organización.

Los operadores de redes móviles enfrentan el permanente desafío de brindar a los usuarios una experiencia móvil segura, cumpliendo al mismo tiempo con las obligaciones de proteger la seguridad pública. A medida que se desarrollan servicios más avanzados y complejos, también aumenta la lista de posibles amenazas y el alcance de los daños que pueden causar. Las estafas y los ataques son cada vez más sofisticados y por ser su objetivo las comunicaciones en general y no sólo las de un dispositivo móvil, las soluciones deben tener una visión integral.

Huawei ha adoptado para sus redes 5G el mecanismo de control de seguridad promovido por la patronal mundial de tecnológicas, GSMA. Se trata de un Esquema de Garantía de Seguridad de Equipos de Red (Nesas, por sus siglas en inglés), un mecanismo de evaluación en ciberseguridad estandarizado, definido conjuntamente por la GSMA y la 3GPP (Asociaciones de Tercera Generación).

La seguridad de los usuarios entonces se puede abordar desde cuatro importantes pilares:

Uso de los dispositivos móviles

La privacidad y los datos

La seguridad pública

La seguridad de las redes y la integridad de los dispositivos

Uso de los dispositivos Móviles

Este pilar busca promover el uso seguro de los servicios móviles a través de medidas proactivas para la protección del usuario, de actividades ilegales y perjudiciales vinculadas al uso de teléfonos móviles o facilitadas por estos:

- Robo de equipos terminales móviles
- Empoderamiento del usuario
- Dispositivos falsificados
- Registros nacionales de usuarios

Un ejemplo de cómo se puede fortalecer la seguridad y prevenir el robo de terminales es el Sistema de Verificación de Dispositivos (IMEI Device Check) que GSMA pone a disposición de los usuarios a través de la página web del Regulador, y que además permite verificar de manera gratuita si un dispositivo móvil ha sido reportado como robado en algún lugar del mundo. De este modo, cualquier persona puede comprobar la legitimidad del equipo antes de efectuar su compra. Interrumpiendo así el circuito de demanda de equipos robados.

El segundo pilar está enfocado a la protección de los datos y la privacidad, al respecto la GSMA estableció nueve principios que se abordaran a continuación.

Los datos y la privacidad

La privacidad de los usuarios se ve afectada por una serie de factores, a menudo controlados por múltiples partes involucradas, tales como el proveedor de servicios o aplicaciones, el operador de servicios de telecomunicaciones móviles, el fabricante del equipo y el sistema operativo u otro proveedor de software.

El objetivo principal de la protección de la privacidad es generar confianza en que los datos privados están protegidos de forma adecuada y conforme con las reglamentaciones y requerimientos de privacidad aplicables. Para ello, todas las partes involucradas deben adoptar una estrategia coherente, con neutralidad tecnológica y congruencia a través de todos los servicios, sectores y geografías.

Al respecto, GSMA desarrolló un conjunto de Principios de Privacidad Móvil que describen la forma en que se debería respetar y proteger la privacidad del consumidor móvil al utilizar aplicaciones y servicios que tienen acceso, utilizan o recolectan sus datos personales. Estos principios no reemplazan ni sustituyen la legislación aplicable, pero se basan en los preceptos de privacidad y protección de datos reconocidos y aceptados internacionalmente.

A continuación, se describen los nueve principios de la GSMA, que además buscan generar un equilibrio entre proteger la privacidad de una persona y garantizarle un trato justo, a la vez que se permite a las entidades alcanzar sus objetivos comerciales, sociales y de política pública, veamos entonces:

1. Mínima recolección de datos:

Solo se debe recolectar la mínima cantidad de información personal necesaria para cumplir con los fines comerciales legítimos y para proporcionar, suministrar, mantener o desarrollar aplicaciones o servicios. La información personal no se debe mantener más tiempo que el necesario para los fines comerciales legítimos o para cumplir con las obligaciones legales correspondientes, y luego debe ser eliminada o se deben anonimizar dichos datos personales.

2. Opciones y control de usuarios:

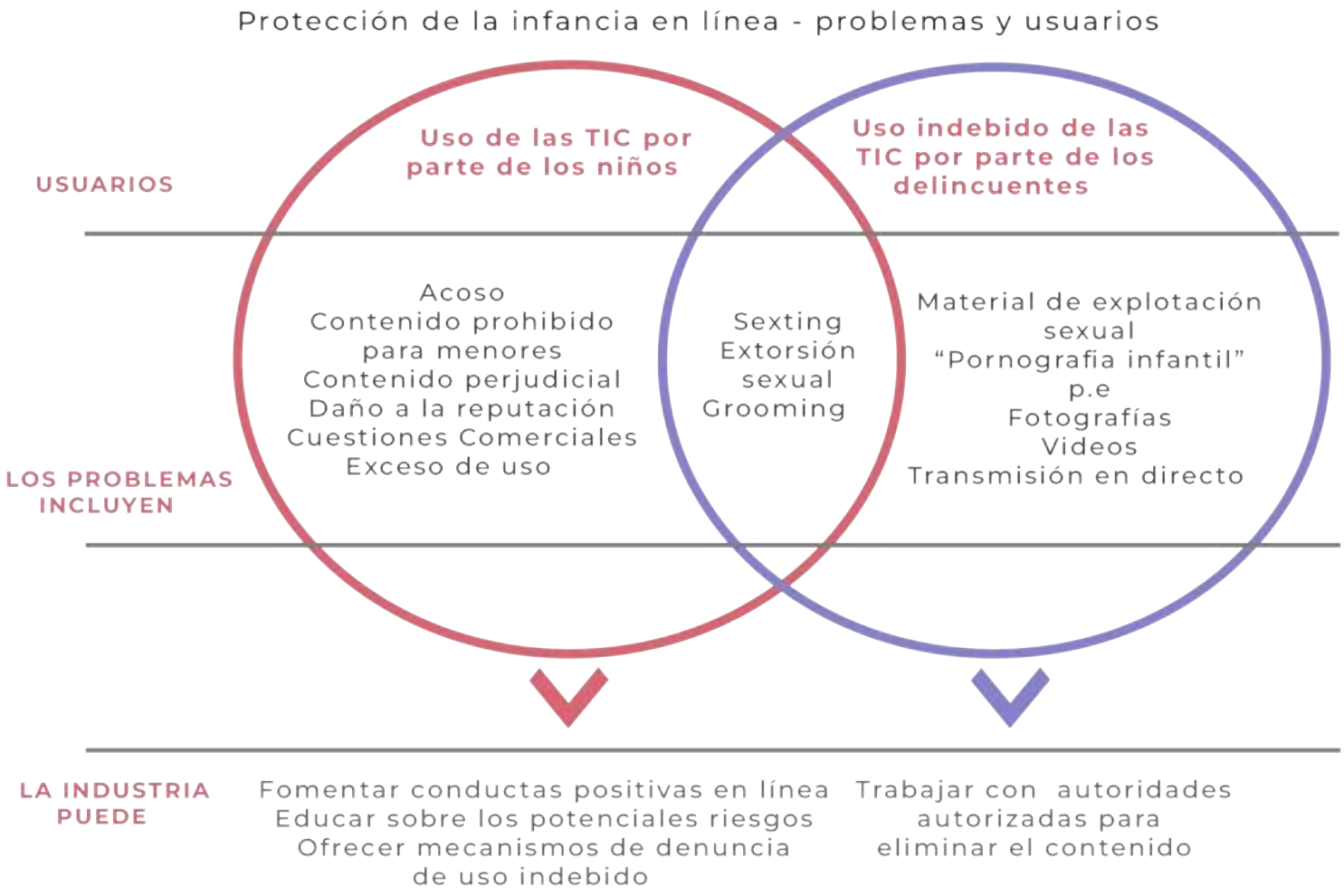
Los usuarios deben tener la oportunidad de ejercer la OPT elección y el control de su información personal.

3. Apertura transparencia y notificación:

Las personas responsables deben ser abiertas y honestas con los usuarios y asegurarse de que se les suministre información clara, en forma prominente y oportuna, sobre su identidad y las prácticas de privacidad de datos. Se debe suministrar información al usuario respecto de las personas que recolectan su información personal, el propósito de una aplicación o servicio como también respecto del acceso, recolección, distribución, divulgación y uso posterior de la información personal del usuario, incluyendo a quién se puede divulgar su información personal, permitiendo así a los usuarios tomar decisiones informadas sobre si utilizar o no una aplicación o servicio móvil.

4. Protección de los niños, niñas y adolescentes:

Las aplicaciones o servicios dirigidos a niños y adolescentes deben garantizar que la recolección, el acceso y el uso de información sea apropiado, en todo tipo de circunstancias, y compatible con las leyes nacionales.



Gráfica tomada de Protección de la infancia en línea – problemas y usuarios GSMA

5. Seguridad de la información personal:

La información personal se debe proteger utilizando garantías razonables y adecuadas a la sensibilidad de la información.

6. Propósito y uso:

El acceso, recolección, distribución, divulgación y uso posterior de la información personal del usuario estarán limitados a fines comerciales legítimos, tales como la provisión de aplicaciones o servicios solicitados por el mismo usuario o, de lo contrario, a cumplir con las obligaciones legales correspondientes.

7. Respeto a los derechos de los usuarios:

Se debe suministrar información a los usuarios respecto de sus derechos al uso de su información personal y una forma sencilla de ejercerlos.

8. Responsabilidad y ejecución:

Todas las personas a cargo son responsables de asegurar el cumplimiento de estos principios.

9. Educación:

El usuario debe recibir información sobre las cuestiones de privacidad y seguridad y las formas de administrar y proteger su privacidad.

Seguridad Pública

La seguridad pública implica que los ciudadanos de una misma región puedan convivir en armonía, cada uno respetando los derechos individuales del otro. El Estado es el garante de la seguridad pública y el máximo responsable a la hora de evitar las alteraciones del orden social.

Sin embargo los preceptos y estándares desde GSMA señalan que cualquier interrupción en las redes de comunicaciones, los servicios de red o el internet (tales como redes sociales, motores de búsqueda o sitios de noticias) tiene el potencial de afectar la seguridad pública y restringir el acceso a servicios vitales de emergencia, pagos y salud.

Por ejemplo, una restricción de los servicios de telecomunicaciones puede limitar la capacidad del usuario móvil de ponerse en contacto con los servicios de emergencia a través de números como el '112' o el '123' y puede interferir en el funcionamiento de las alarmas móviles conectadas o dispositivos médicos personales. Por estos motivos, las restricciones de servicios deben ser mínimas y se deben considerar los efectos colaterales negativos para todos los usuarios. Tal es el caso del uso de inhibidores de señal de telefonía móvil (Jammers) que pueden llegar a interferir la señal de los usuarios.

Seguridad de las redes e integridad de los dispositivos

La mayoría de los servicios en redes móviles presentan los mismos desafíos de seguridad que enfrentan tantos otros servicios que dependen de la conectividad. Por lo tanto, es importante garantizar la disponibilidad, la identidad, la integridad y la privacidad:

Disponibilidad

Asegurar una conectividad constante entre los terminales y sus respectivos servicios

Identidad

Autenticar los terminales, servicios y usuarios

Integridad

Asegurar que la integridad del sistema puede ser verificada y monitoreada

Privacidad

Reducir el potencial acceso a información por parte de personas no autorizadas

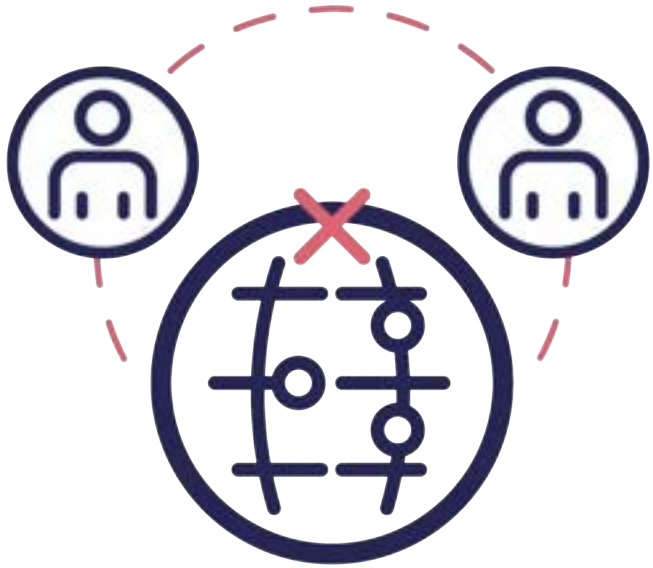
OBJETO DE LA PROTECCIÓN	DESCRIPCIÓN DE LA AMENAZA	POSIBLE ATAQUE
INTEGRIDAD: Evitar la alteración de los datos	Adulteración no autorizada	Ataque por interceptación 
CONFIDENCIALIDAD: Mantener la privacidad de los datos	Acceso no autorizada	Escuchas 
DISPONIBILIDAD: Mantener la disponibilidad de la red y los datos para los usuarios legitimos	Destrucción, robo, eliminación o pérdida de datos o redes no disponibles	Denegación de servicio 

1. Principales problemas de Seguridad en las redes:

Según los resultados de la encuesta realizada a expertos de la industria por la Cloud Security Alliance (CSA) para recopilar opiniones profesionales sobre los mayores problemas de seguridad dentro de la computación en la nube; la violación de datos, la falta de estrategia de seguridad, la gestión de identidad y el secuestro de datos, representan los principales retos en materia de aseguramiento y protección de datos corporativos en la nube. Veamos entonces:

- Violaciones de datos
- Configuración incorrecta y control inadecuado de cambios
- Falta de arquitectura y estrategia de seguridad en la nube
- Identidad insuficiente, credencial, acceso y gestión de claves
- Secuestro de cuentas
- Amenazas internas
- Interfaces y API inseguras
- Plano de control débil
- Fallos en la meta estructura y la estructura de aplicaciones
- Visibilidad limitada del uso de la nube
- Abuso y mal uso de los servicios en la nube

El anterior panorama de amenazas y problemas de seguridad hace que las medidas tradicionales de defensa pasiva sean menos eficaces. Esto redundará en largos tiempos de detección de amenazas y de respuesta. Las organizaciones deben enforcarse en soluciones que permitan una detección más inteligente de amenazas, optimizar la respuesta a estas y mejorar la eficiencia y costos en las operaciones y mantenimiento de la seguridad de las redes empresariales y la infraestructura de telecomunicaciones.



2. Implementación de Modelos de Seguridad Zero Trust:

Confianza Cero es un modelo de seguridad de red basado en un proceso estricto de verificación de identidad. Este marco de seguridad impone que solo los usuarios y dispositivos autenticados y autorizados puedan acceder a las aplicaciones y a los datos. Al mismo tiempo, protege esas aplicaciones y usuarios frente a amenazas avanzadas de Internet.

- Los usuarios, los dispositivos, los datos y las aplicaciones se están trasladando fuera del perímetro de la empresa y de la zona de control.
- Los nuevos procesos empresariales, impulsados por la transformación digital, incrementan el riesgo a la exposición.
- El enfoque "confiar, pero verificar" ya no es una opción, dado que las amenazas avanzadas ahora acceden al perímetro de la empresa.
- Los perímetros tradicionales son complejos, incrementan el riesgo y ya no son adecuados para los modelos de negocio actuales.

La Ciberseguridad Proactiva incorpora soluciones de seguridad de big data y anti-APT con capacidad de mitigar el riesgo que representan las amenazas persistentes avanzadas (APT)[1] a través de las cuales los ciberdelincuentes han incorporado tácticas, técnicas y procedimientos que utilizan malware personalizado, vulnerabilidades de día cero o tecnologías de evasión avanzadas para romper las defensas tradicionales, como firewall, sistemas de prevención de intrusiones y dispositivos antivirus.

Una solución de defensa de APT y seguridad de big data robusta utiliza un sistema de big data para recolectar información de toda la red, y realizar análisis de correlación multidimensional de datos masivos, basados en un algoritmo de detección de inteligencia que permite identificar con precisión los ataques de APT y prevenir de manera efectiva que estos comprometan los activos de información central.

[1] Según la Guía de Glosario de términos de ciberseguridad del INCIBE define una APT como un tipo de ataque informático que se caracteriza por realizarse con sigilo, permaneciendo activo y oculto durante mucho tiempo, utilizando diferentes formas de ataque.

Las soluciones de nueva generación incorporan el aprendizaje automático para la detección de amenazas, dándole un plus a la capa de defensa proactiva que requieren las organizaciones. Los algoritmos de aprendizaje automático ayudan a las empresas a detectar con mayor rapidez parámetros, que se salen de los patrones normales y que puede esconder potenciales ataques (ofuscar el vector de ataque).

A partir del análisis de estos datos, los propios sistemas de aprendizaje automático son capaces de establecer protocolos de seguridad, que llevan asociadas determinadas acciones en función del tipo de intromisión en redes empresariales e infraestructuras de telecomunicaciones.

La Ciberseguridad proactiva permite igualmente fortalecer el aseguramiento de las redes y para ello es importante que las organizaciones consideren incorporar en sus capacidades de defensa proactiva, así como las oportunidades que brindan los firewalls de nueva generación NGFW, los cuales permiten la aceleración de procesamiento de servicios de cifrado/descifrado de patrones y mejoran en gran medida el rendimiento de los firewalls, la detección de seguridad y los servicios IPSec[2]. Además de ello proporcionan servicios de VPN, prevención de intrusiones, antivirus, prevención de fugas de datos, gestión de ancho de banda, anti-DDoS, filtrado de URL y funciones antispam; elevando de manera significativa la seguridad en las fronteras de la organización.

Por otra parte, la frecuencia de los ataques DDoS orientados a generar la indisponibilidad de los sistemas y redes empresariales se ha incrementado gracias al modelo de oferta de servicios de cibercrimen (Crime as a Service) y las motivaciones económicas con origen extorsivo, posicionan esta ciber amenaza casi al nivel de los ataques de Ransomware.

La Ciberseguridad proactiva debe proveer a los responsables de la estrategia empresarial soluciones, que permitan adaptar rápidamente capacidades de analítica de big data, que faciliten el modelado de los diferentes tipos de tráfico de red para responder a los ataques en cuestión de segundos y ofrecer protección integral contra ataques volumétricos y de aplicaciones en tiempo real.

[2] IPsec es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado. Fuente INCIBE

Consideraciones finales

Un ciberataque genera importantes pérdidas financieras principalmente asociadas a la interrupción de la productividad en una empresa, los gastos de recuperación de incidentes, los gastos por reemplazo de sistemas de información/datos, las pérdidas asociadas a ventajas competitivas, gastos por falta de conformidad legal (Cibercompliance) y la pérdida de reputación.

Por ejemplo, el costo promedio asociado a un ataque de ransomware en una empresa mediana/grande fue de 1.85 millones de dólares en 2021, incluidos tiempo de inactividad, y costos de la red y de dispositivos, entre otros. El rescate promedio pagado por las organizaciones fue de 170.400 dólares y sólo el 65% de los datos se restauraron después del pago, lo que supone riesgos mayores por incumplimiento a normas de LA/FT y protección de datos personales.

Entonces, el impacto económico negativo para una organización que ha sufrido un Ciberataque debe ser considerado por la alta dirección al momento de definir su estrategia de seguridad (Valor en Riesgo). También debe cuantificar el impacto del mismo y el costo para recuperarse, en relación con la inversión en implementación de una estrategia de ciberseguridad sólida ajustada al negocio de la empresa.

“El tema de la ciberseguridad hoy, muchas veces visto como un costo, ante estas potenciales pérdidas, necesita ser visto como una inversión”

Marcelo Motta
Director de Ciberseguridad y Protección de Datos de Huawei América Latina.

Por lo tanto, hay que transformar el modelo eminentemente reactivo en uno proactivo. En ese sentido, aunque tenemos exceso de información sobre amenazas, hay que realizar importantes esfuerzo por convertirla en conocimiento que permita anticipar la acción y la respuesta inmediata a los desafíos crecientes de los Ciberataques.

Referencias

Referencias
Referencias

1. https://c2usercisoslab.com/2022/05/26/malware-bancario/
2. https://www.crowdstrike.com/products/threat-intelligence/falcon-x-recon/
3. https://www.fiscalia.gov.co/colombia/adenunciar/
4. https://adenunciar.policia.gov.co/Adenunciar/Login.aspx?ReturnUrl=%2fadenunciar%2f
5. https://www.sic.gov.co/tema/proteccion-de-datos-personales
6. https://cloudsecurityalliance.org/research/topics/top-threats/
7. https://www.gsma.com/latinamerica/wp-content/uploads/2017/06/Seguridad-privacidad-y-proteccio%CC%81n-del-ecosistema-mo%CC%81vil.pdf
8. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf


CCIT
tictac
SAFE