TENDENCIAS DEL CIBERCRIMEN 2021 - 2022

NUEVAS AMENAZAS AL COMERCIO ELECTRÓNICO

CCIT tictac SAFE
SEGURIDAD APLICADA AL FORTALECIMIENTO EMPRESARIAL

Equipo TicTac

Dirección de desarrollo de programas:
CR (RA) Fredy Bautista García
Lorena Mesa Guzmán

Colaboradores
Ana María Fuentes - Fortinet
CrowdStrike

Diseño y diagramación:
Paula Cruz Giraldo

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.

Attribution-NonCommercial 4.0 International.

Copyright © TicTac 2021
Todos los derechos reservados. La distribución y uso de este documento sin fines comerciales está permitida sin restricciones.

TENDENCIAS DEL CIBERCRIMEN 2021 - 2022

NUEVAS AMENAZAS AL COMERCIO ELECTRÓNICO

CROWDSTRIKE FORTINET

contenido

1	Prólogo	09
2	Introducción	13
3	Comportamiento del ciberdelito en Colombia durante el 2021	15
4	**Comercio electrónico:** Aseguramiento de sitios web para proteger los datos de los usuarios	25
5	Decálogo de seguridad para las compras por internet	33
6	MDR para la ciberseguridad y ciberdefensa empresarial ¿por qué es importante?	43
7	Referencias	50

01

Prólogo

Alberto Samuel Yohai
Presidente Ejecutivo CCIT

Una de las mayores enseñanzas que nos ha dejado esta pandemia es la necesidad de proteger la información; aquí se ha demostrado que el principal reto de las empresas es cuidar la data de los usuarios, puesto que el comercio electrónico se convirtió en la principal herramienta para ofertar y comprar productos.

Por esto, la ciberseguridad se posicionó con mayor fuerza dentro de las prioridades de las compañías. Contar con un grupo especializado de profesionales que mantengan a salvo la información de todos los que utilizamos diferentes plataformas y canales de pago virtual para facilitar procesos, será de máxima prioridad para los próximos años.

Desde el Tanque de Análisis y Creatividad de las TIC (TicTac) y su programa de Seguridad Aplicada al Fortalecimiento Empresarial (SAFE) vemos con gran importancia la adopción de estrategias de ciberseguridad por parte de las compañías, que estén enfocadas a la protección del usuario, ya que, si bien hoy día se invierte en seguridad empresarial, es clave proteger a quienes utilizan diferentes canales de pago digitales.

Así como existen riesgos en el mundo físico, el comercio electrónico no está exento de presentar brechas de ciberseguridad. Es importante que las soluciones sean robustas y se comparta información de una manera coordinada para así detectar brechas de seguridad de la información, e implementar a tiempo las herramientas necesarias para contrarrestar el ciberdelito.

En este sentido, el rol que obtiene cada día mayor relevancia es el de los **Chief Information Security Officer (CISO)**, ya que su labor es prioritaria para una compañía.

02

Introducción

El 2021 se caracterizó por ser un año en el que, gracias a que los ciudadanos se han podido movilizar mucho más respecto al 2020, las compras a través de comercios electrónicos continuaron en crecimiento.

Los día sin IVA estipulados por el gobierno nacional aportan significativamente al incremento en ventas online. Solo en la primera jornada llevada a cabo el 28 de octubre, se hicieron ventas por **$9,8 billones de pesos**, así estas cifras revelan un crecimiento del **130%** frente al último día sin IVA del 2020.

Ante el uso masivo de las plataformas y sistemas de pago digitales como medio de compra, especialmente en los días sin IVA, *cyberlunes* o "*black friday*", la seguridad digital sigue siendo el principal requerimiento de los usuarios, precisamente, al finalizar noviembre de 2021, se presentaron 46.527 eventos por ciberdelitos en el país, registrando un crecimiento del 21% comparado con 2020.

El ransomware, sigue afectando a las empresas colombianas principalmente PYMES donde se registraron más de 500 casos durante los primeros 9 meses del año. Por esto, es necesario que los comercios sigan desarrollando estrategias de ciberseguridad, que brinden confianza para el consumidor a la hora de comprar por un medio virtual. De igual forma, la labor como usuario es ser mucho más previsivos, siguiendo al pie de la letra las recomendaciones que generalmente se entregan para evitar la pérdida de la información, los robos o estafas a través de engaños.

Aunque las modalidades siguen siendo las mismas, los ciberdelincuentes cada vez buscan alternativas "innovadoras" para engañar y robar, por lo que es necesario estar alerta ante cualquier sospecha. La ingeniería social, combinada con el phishing, vishing, entre otros, son los principales vectores de ataque, tanto para los ciudadanos como para las empresas. Las redes sociales, que además de permitir compra y venta de productos, también se convirtieron en un canal asociado a suplantaciones de identidad o robo de sesiones para estafar.

Velar por la información de los usuarios es una labor constante que deben tener las compañías, por esto, desde el programa SAFE hemos venido trabajando constantemente para llevar de primera mano la información más relevante y detallada frente a la ciberseguridad.

Precisamente, este último informe ha sido realizado para hacer un balance de lo que fue el cibercrimen en 2021, las tendencias para 2022, y por supuesto, mostrar un panorama centrado en herramientas para la ciberseguridad y ciberdefensa empresarial, cerrando con un análisis profundo sobre la importancia de proteger los datos de los usuarios ante las ciberestafas, teniendo en cuenta el uso constante y cada vez mayor del comercio electrónico.

03

Comportamiento del ciberdelito en Colombia durante el 2021

Escrito por: CR (RA) Fredy Bautista García

Según cifras del Cybersecurity Ventures sobre economía cibernética global, el costo del cibercrimen alcanzará en **2025** los **10.5 billones de dólares**; lo que equivale a la suma de las economías de Japón, tercera en el planeta, Alemania cuarta y Suiza la 18ª; se estima entonces que durante el **2021** los costos por daños globales del cibercrimen ascenderán a 6 trillones de dólares, lo que equivale a **648 millones de dólares** en pérdidas por hora; 11.4 millones de dólares en un minuto y cerca de 190.000 dólares por segundo.

Estos datos responden al incremento significativo de los casos de ciberataques exitosos en el mundo reflejados en los múltiples reportes de infecciones por software malicioso generalmente propagado por phishing o por navegación desprevenida de los usuarios en sitios infectados en la web. Tan solo durante el ***2021***, se reportaron ***3.806 empresas víctimas de Ransomware*** a nivel mundial y 53 grupos cibercriminales han sido identificados desde el 2019 hasta noviembre del 2021 como responsables del crecimiento de esta tipología de ataque basada en el secuestro de información para posteriores escenarios de ciber extorsión.

Dentro de los grupos cibercriminales que más datos han expuesto en la red durante el 2021, como resultado de la exfiltración de información luego de un ciberataque se encuentran: LockBit, Conti, Ragnarok, Egregor y Sodinokibi/Revil, este último grupo recientemente fue objeto de una operación internacional por parte de Europol y el FBI siendo arrestados cinco de sus integrantes en una acción conjunta internacional en la que se vieron involucrados cerca de 17 países a través de la denominada Operación Gold Dust. Con más de 7.000 infecciones a nivel global; los cibercriminales miembros de Sodinokibi/Revil llegaron a exigir 232 millones de dólares por concepto de rescates según informó en su sitio web recientemente la agencia federal de investigación.

Cifras del ciberdelito en Colombia

Al analizar el comportamiento del cibercrimen en Colombia reflejado en el número de denuncias instauradas ante el ecosistema de la Fiscalía General de la Nación, las policías judiciales del CTI y la Policía Nacional (DIJIN-SIJIN) a través del aplicativo a denunciar, al finalizar el mes de noviembre del **2021** se habían registrado **46.527 denuncias** por distintos delitos lo que equivale a un **incremento del 21% respecto al 2020**. Si se tienen en cuenta comparativamente los años 2019 y 2021, es decir sin contabilizar el año de pandemia, el incremento alcanzó un 107% acumulado entre el incremento suscitado durante el 2020 y el aumento continuo durante el 2021.

Sin duda el ciberdelito se ha convertido en la tipología criminal de mayor crecimiento en Colombia durante los últimos tres años; impulsado por aceleradores como la pandemia y el consecuente incremento del comercio electrónico cuyo crecimiento alcanzó el **59.4%** en las transacciones durante el periodo de cuanterena obligatoria y del **35%** durante el 2021 con ventas estimadas en 37 billones de pesos al finalizar el año según cifras de la Cámara de Comercio electrónico de Colombia CCCE.

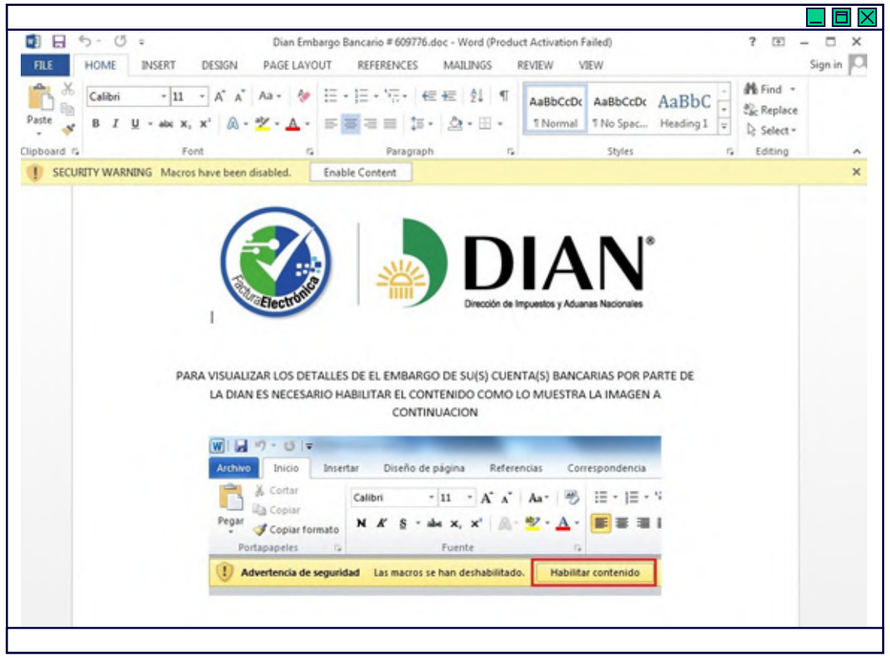
Actores del cibercrimen

Lo anterior aunado a la rápida adaptación de los cibercriminales a la nueva realidad disparó los ciberataques basados en vectores de infección como correos electrónicos que continúan suplantando a las entidades gubernamentales principalmente a la DIAN, Fiscalía General de la Nación, Ministerio de Salud, Registraduría Nacional del Estado Civil, DANE, Migración Colombia y Policía Nacional.

Precisamente al revisar los grupos cibercriminales internacionales con injerencia en Colombia destaca el grupo APT C36 que según la publicación del sitio web especializado de MITRE ATT&CK https://attack.mitre.org/groups/G0099/, es sospechoso de ciber espionaje en Sudamérica, y se encuentra activo desde 2018 teniendo como objetivo instituciones gubernamentales, corporaciones del sector financiero, industria del petróleo y grandes empresas manufactureras en Colombia.

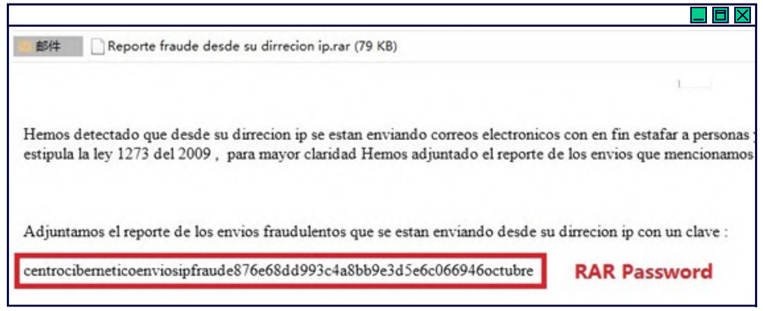
En los informes especializados se identificó que han sido suplantadas al menos (8) entidades de gobierno con la finalidad de enviar en correos fraudulentos enlaces maliciosos que redireccionan la navegación de los usuarios hacia sitios en internet, infectados previamente.

Algunos dominios maliciosos utilizados por el atacante APT C36 también se hacen pasar por sitios web del gobierno colombiano. Por ejemplo, “diangovcomuiscia.com” que suplanta al dominio oficial “muisca.dian.gov.co” perteneciente a la Dirección Nacional de Impuestos y Aduanas.



Fuente imagen: *Propia*

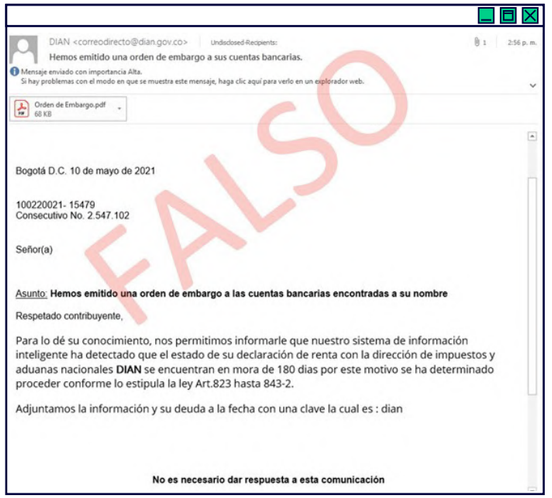
Como técnica empleada de ataque los correos electrónicos enviados traen un archivo que se cifra y almacena en el paquete comprimido. Dentro del texto del mensaje se proporciona una contraseña de descifrado para evitar la detección de seguridad en el enlace del correo electrónico, como se observa en la gráfica a continuación:



Fuente imagen: *Propia*

Todos los documentos utilizados como señuelo son MHTML[1] con macro maliciosa incrustada y el sufijo .doc para evitar la detección; en otras ocasiones el archivo adjunto es un documento .pdf “ORDEN DE EMBARGO.

A continuación, se muestra un ejemplo de documento de señuelo identificado durante mayo del 2021:



Fuente imagen: *COLCERT*

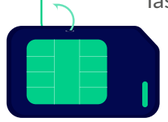
[1] MHTML o MIME HTML, es un estándar para incluir recursos que en páginas HTML usualmente están enlazados externamente, tal como los archivos de imágenes y sonido, en el mismo archivo.

Delitos con mayor crecimiento durante el 2021

La Violación de Datos Personales con 13.458 casos es el delito de mayor crecimiento en el país durante el 2021 con un **45%** de variación porcentual respecto a los casos registrados durante el 2020. Lo anterior tiene una explicación relacionada con las campañas de Phishing, mediante las cuales los cibercriminales consiguen enviar enlaces que redireccionan hacia sitios web con formularios utilizados para sustraer información personal principalmente datos bancarios, nombres y apellidos de la víctima, documento de identidad, lugar de nacimiento y demás información necesaria para adelantar trámites y generar procesos fraudulentos vinculados a solicitudes de crédito, trámites de tarjetas de crédito, fraudes en seguros o venta de datos en la internet profunda para suplantación de identidad.

La segunda modalidad de mayor crecimiento es el acceso abusivo a sistemas informáticos que presenta un total de **9.926 denuncias**, y un incremento del **18%** respecto a las cifras reportadas durante el 2020. El acceso abusivo a sistemas informáticos sigue siendo el delito generalmente asociado a las fases iniciales de un ciberataque especialmente cuando el intruso luego de realizar labores de escaneo consigue ganar acceso al sistema para luego escalar privilegios, realizar modificaciones a las configuraciones principalmente en los sistemas de defensa como antimalware, firewall y otras que presentan diferentes configuraciones de seguridad disponibles en la infraestructura del sistema comprometido.

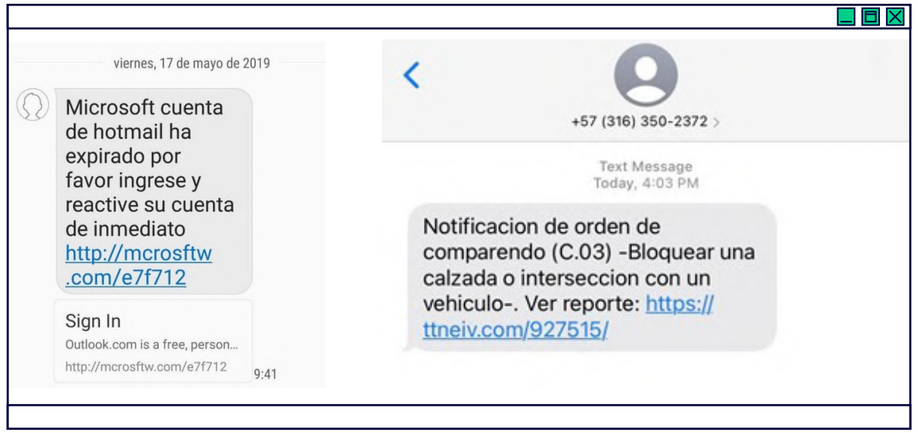
En tercer lugar, se encuentra el hurto por medios informáticos, que tuvo un incremento del **3%**. Sin embargo, se han instaurado **17.608 denuncias** desde enero hasta noviembre del 2021; siendo el delito con mayor frecuencia en el país lo que señala claramente que la motivación de los ciberataques guarda la tendencia recurrente de los últimos frente al interés económico de los cibercriminales por afectar y comprometer las cuentas bancarias de las personas y empresas afectadas sin importar el capital o tamaño de estas.



El hurto por medios informáticos igualmente conlleva vulnerar los mecanismos de seguridad para acceder a las plataformas bancarias; tales como la utilización de un factor múltiple de autenticación, el compromiso de las contraseñas de acceso y las labores previas de ingeniería social vinculadas a la modalidad de SIM SWAPPING que sigue teniendo un auge durante el 2021 y que se constituye en la principal técnica de los cibercriminales para suplantar a la víctima y apoderarse de la SIM CARD y así acceder de manera fraudulenta a los servicios de banca electrónica de la víctima suplantada.

La suplantación de sitios web igualmente con **7.654 casos** tuvo un incremento similar del **3%** respecto al año 2020, siendo el Phishing y el Smishing las principales modalidades empleadas por los Cibercriminales; en algunas ocasiones combinado con técnicas de llamadas en escenarios de ingeniería social y manipulación; particularmente con la utilización de datos que han sido comprados en los mercados ilegales por parte de los estafadores.

Durante el 2021 se detectó un incremento en el número de casos igualmente de Smishing por el uso creciente de mensajes de texto vía SMS que incorporan dentro del cuerpo del mensaje una URL acortada del sitio bancario suplantado, lo que supone un engaño para la víctima pues generalmente los usuarios desconocen las vías de confirmación respecto a la legalidad del sitio web señuelo como se observa en la gráfica a continuación.



Fuente imagen: *@ColCERT*

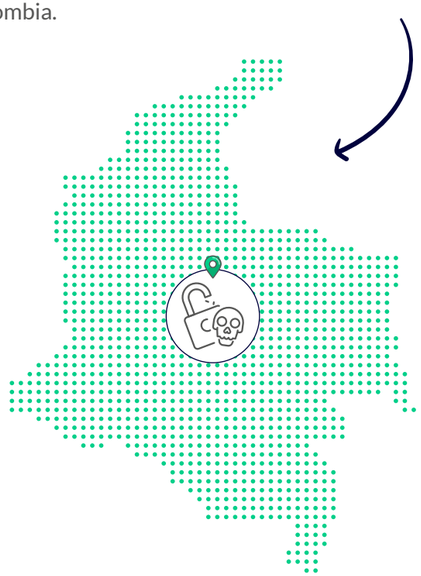
El Smishing se consolida como una variante del Phishing y seguirá marcando una tendencia al alza durante el 2022; puesto que los servicios bancarios seguirán popularizándose a través de medios de movilidad tales como aplicaciones, billeteras virtuales desarrolladas para tabletas y teléfonos celulares.

Otras modalidades delictivas como el daño informático, el uso de software malicioso, la obstaculización ilegítima de sistemas informáticos o redes de telecomunicaciones y la interceptación de datos informáticos se mantienen estables; sin embargo durante el 2021 se denunciaron cerca de 395 casos que pueden estar vinculados a la modalidad de ransomware puesto que se reportaron alteraciones, borrado y supresión de los datos afectando sistemas informáticos en ataques que además incluyeron el uso de software con fines maliciosos.

Las anteriores cifras siguen demostrando que los esfuerzos por implementar mecanismos eficientes de seguridad en las empresas pueden resultar insuficiente si la ciberseguridad no centra su atención en el usuario, pues gran parte de los vectores de infección requieren al final el click o la descarga desde un enlace fraudulento; tarea que está asociada a la voluntad del usuario hacia dónde ha sido dirigido el correo de engaño.

El anterior planteamiento supone la necesidad de fortalecer la sensibilización mediante jornadas de capacitación continuas para todos los roles de una organización así como los espacios de Ciberacademia continua mediante la implementación de plataformas de formación con cursos exigibles como requisito para la vinculación a un nuevo empleo así como procesos de formación continua para habilitar competencias que permitan a todos los empleados identificar las nuevas ciberamenazas y conocer los procedimientos para acudir a los responsables de seguridad en la organización cuando se encuentran frente a un mensaje sospechoso o se genere alguna actividad inusual en la interacción con los medios tecnológicos de la empresa.

Finalmente es muy importante seguir incentivando el uso de los canales virtuales de denuncias puesto que dentro de la estrategia para combatir el cibercrimen, los observatorios especializados de analítica del fenómeno requieren conocer las circunstancias de modo, tiempo, lugar, modalidad empleada, técnica utilizada, indicadores de compromiso y vector de infección para poder realizar las asociaciones que permitan unificar los procesos judiciales y requerir la asistencia judicial internacional en caso de que sea necesaria una prueba digital transfronteriza; así como también participar de manera propositiva en la generación de mejores prácticas para la prevención del ciber delito en Colombia.



04

Comercio Electrónico: Aseguramiento de sitios web para **proteger los datos de los usuarios**

Escrito por: Ana María Fuentes
Systems engineer de Fortinet Colombia

FORTINET

La pandemia de COVID 19 en 2021 aceleró el crecimiento de comercio electrónico un **30%** más que en 2019[2] y permitió que las empresas de venta al por menor y grandes superficies pudieran sobrevivir a esta situación.

Lo anterior aumentó la concientización acerca de la importancia del aseguramiento de datos en los sitios web para que la información personal de los usuarios compradores no se comprometiera al realizar transacciones de compra en línea. Sin embargo, según la encuesta de seguridad de aplicaciones de 2021 realizada a nivel mundial por Fortinet, a 344 profesionales de ciberseguridad, se evidenció que solo el **43%** de las Organizaciones son moderadamente a extremadamente confiadas con la postura de seguridad de sus aplicaciones web[3].

Los datos más importantes que se deben proteger en el escenario de comercio electrónico, son los relacionados con información personal de los usuarios, sus gustos, preferencias, campañas de fidelización, entre otros.

Debido a que en Colombia no existe regulación ni legislación legal para proteger datos personales en el entorno de transacciones en línea, cada una de las compañías que ofrecen servicios de e-commerce deben garantizar que sus aplicaciones web sean seguras para mejorar y aumentar la confianza del consumidor, en el uso de transacciones digitales y de esta forma acelerar sus ventas.

[2] https://forbes.co/2021/10/05/tecnologia/que-hay-detras-del-crecimiento-de-30-en-ecommerce-en-colombia-esta-docuserie-te-da-el-panorama/
[3] https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-cybersecurity-insiders-application-security-fortinet.pdf

Algunos de los desafíos más importantes para proteger aplicaciones web utilizadas para comercio electrónico son:

Detección de amenazas o brechas, ya que las empresas únicamente cuentan con herramientas de seguridad tradicionales y no tienen herramientas de ciberseguridad dedicadas a proteger sitios web y APIs.

Despliegues de aplicaciones web en nubes públicas como AWS, Azure, GCP, Oracle Cloud, entre otras, puesto que muchas compañías dan por hecho que la seguridad es un componente que viene embebido en estos servicios y realmente es una responsabilidad de cada empresa, por lo cual los datos quedan expuestos a internet.

La mayoría de las aplicaciones web se desarrollan a la medida por un equipo de desarrolladores interno o tercero quien se encarga que las aplicaciones sean funcionales, pero no se tiene en cuenta que sean seguras y se dejan en producción sin realizar ningún análisis que permita identificar vulnerabilidades y mitigarlas correctamente.

Revisemos algunos ejemplos de los ataques más frecuentes que afectan a las aplicaciones web de e-commerce:

Defacement: Ataque que altera la apariencia visual de una aplicación web impactando principalmente la reputación de una compañía, ya que los atacantes modifican la página de inicio adjuntando imágenes, videos, enlaces, incluyendo información de organizaciones que pueden ser competencia.

Inyección SQL: Ataque que inyecta código malicioso en la base de datos de la aplicación web permitiendo obtener información confidencial. Un ejemplo de este tipo de ataque ocurrió al sitio web de la compañía Tesla en 2014 permitiendo a los atacantes tener privilegios administrativos y robar datos de usuarios.

Cross Site Scripting: Permite ejecutar una secuencia de instrucciones no autorizadas en la aplicación web, facilitando su suplantación y comprometiendo los datos de sus usuarios. Un ejemplo de este tipo de ataque sucedió a British Airways en 2018, la brecha afectó 380.000 transacciones de reservas permitiendo obtener a los atacantes información detallada de tarjetas de crédito.

Bots: Automatizan solicitudes hacia aplicaciones web para manipular o interrumpir el servicio. Es importante tener en cuenta que hay bots de tráfico legítimo, pero frecuentemente los bots son maliciosos, permiten el robo de datos y la ejecución de ataques de denegación de servicio.

En su mayoría, las empresas utilizan controles de seguridad reactivos para proteger las aplicaciones web y no se realiza monitoreo continuo y en tiempo real, por lo cual, en muchas ocasiones, no se logran identificar las brechas y desafortunadamente lo que se percibe son los impactos a nivel reputacional, financieros, la perdida de disponibilidad de los sitios web y la exposición de información sensible.

A continuación, se encuentran algunas recomendaciones para proteger los datos de los consumidores o usuarios en los sitios web de comercio electrónico:

Implemente un proceso para aseguramiento de código que incluya escaneo de vulnerabilidades, hacking ético, remediación de vulnerabilidades identificadas, uso de certificados digitales para evitar interceptación de información y utilice un dominio para la publicación de sitios web.

Despliegue seguridad a nivel de red para proteger los servidores web en nubes privadas y públicas principalmente contra malware e intrusiones utilizando un Firewall de Nueva Generación.

Utilice herramientas dedicadas para protección de aplicaciones web, principalmente en nubes privadas y públicas que aseguren los sitios contra ataques conocidos y desconocidos usando machine learning para detección de comportamientos anómalos y mitigación de falsos positivos.

Incluya mitigación específica para ataques de denegación de servicio con una solución Anti-DDoS que permita diferenciar el trafico normal de sus sitios web de comercio electrónico en comparación a las solicitudes maliciosas, inclusive en días de alto consumo, como el día sin IVA.

Utilice una arquitectura con contingencia para su sitio web, de tal forma que no se altere la continuidad en sus ventas. Para esto puede utilizar un servicio de balanceo global que permita garantizar la disponibilidad del sitio web ante una falla de infraestructura u operacional.

Implemente doble autenticación para que los clientes por ejemplo introduzcan un pin adicional que deben recibir a su móvil para finalizar la compra en línea, de esta forma podrá disminuir la posibilidad de fraude.

Utilice una pasarela de pagos confiable y reconocida en el mercado para generar mayor tranquilidad y confianza a los clientes en el momento de realizar transacciones en línea.

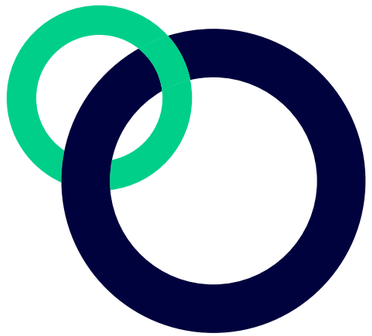
Envie mensajes de concientización de seguridad a sus clientes para evitar que sean víctimas de ataques de phishing y spam con correos de publicidad y promociones falsas.

Como complemento a las sugerencias anteriores, tenga en cuenta la importancia de contratar personal calificado con conocimientos y experiencia en ciberseguridad, así como automatizar tareas de mitigación de ataques o amenazas dirigidas hacia sitios web de comercio electrónico. Por otra parte, es importante tener en cuenta que, si el desarrollo de las aplicaciones web se realiza a través de un tercero, debe establecer y exigir un procedimiento de código seguro a nivel contractual; el cual debe evaluarse y auditarse frecuentemente.

La adopción de comercio electrónico aumentara cada día más, ya que está demostrado que permite ampliar la cobertura de ventas a nivel nacional e internacional, lo cual es óptimo para las empresas.

Asimismo, se incrementará la generación de amenazas nuevas y sofisticadas, debido a esto es importante el aseguramiento de los datos de usuarios de e-commerce, el cual es un proceso de esfuerzo y mejora continua.

Por esta razón, en Fortinet contamos con un gran equipo de trabajo en Colombia para hacer una labor consultiva que permita a nuestros clientes contar con arquitecturas integrales, soluciones y procesos de ciberseguridad que garanticen la disponibilidad, confidencialidad e integridad de la información, optimicen las operaciones propias del negocio y faciliten una mejor experiencia a los usuarios.



05

Decálogo de seguridad para las **compras por internet**

Escrito por: CR (RA) Fredy Bautista García

La temporada navideña y de cierre de año, generan un incremento en el número de transacciones en portales de comercio electrónico. Durante el 2021 y particularmente en los meses de noviembre y diciembre se desarrollaron tres jornadas de día sin IVA, que se valieron de las tiendas en línea como impulsores económicos dado el importante número de usuarios que accedieron a estos portales.

Sin embargo, los defraudadores virtuales y estafadores en internet reconocen las debilidades en algunos procesos de validación y autentificación de usuarios en las plataformas virtuales, los errores y fallos en la configuración segura de los portales, abren la oportunidad para instalar programas maliciosos mediante inyección de código donde cargan las páginas mal desarrolladas y finalmente aplican los ataques de ingeniería social para sustraer información personal de los usuarios, dando inicio a la cadena múltiples modalidades de ciberataques y defraudaciones virtuales en estas plataformas de Comercio electrónico.

Se destacan las siguientes modalidades:

1. Exigencia de pago previo y no entrega del producto adquirido.
2. Pagos de la compra mediante cheques (chequeras robadas o sin fondos).
3. Entrega de productos de baja calidad o de características distintas a las condiciones pactadas en la transacción.
4. Entrega de productos tipo dummi o piezas de imitación elaboradas en materiales como jabón o madera para simular forma y peso de un teléfono celular o una tableta, que son enviados en cajas de apariencia “original”.
5. Robo de datos bancarios en sitios infectados o mal configurados .

Para no caer en este tipo de estafas es muy importante inicialmente considerar el decálogo de seguridad para las transacciones seguras en plataformas de Comercio electrónico durante la temporada navideña y de fin de año:

1. Tenga cuidado con las falsificaciones

Los cibercriminales durante el 2020 y 2021 han **copiado los contenidos y ofertas de las principales páginas y tiendas más populares en internet** y de esta manera aumentan las posibilidades de engaño a usuarios mediante el robo de contraseñas y claves. (Phishing)

La modalidad consiste nuevamente en acceder a sitios de compra y venta a través de enlaces maliciosos en los cuales los anuncios de una promoción son acompañados de hipervínculos o enlaces que direccionan la navegación hacia la página donde se va a realizar la supuesta compra. En ocasiones estos sitios utilizan certificados de seguridad y de transferencia segura de datos bajo protocolos HTTPS y SSL con los que buscan dar una apariencia segura del sitio comprometido. Sin embargo, como ya se ha dicho en este informe es muy importante mantener el estado de alerta y poder revisar los enlaces antes de dar clic sobre ellos.

En caso de tener dudas sobre la oferta anunciada en el sitio web promocionado es necesario buscar otros canales y medios alternativos de comunicación con la empresa suplantada para poder salir de dudas y validar la legalidad de la oferta expuesta en la red.

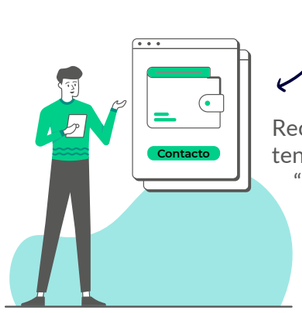
2. Redes sociales sí, pero con seguridad

En esta temporada los sitios y perfiles en plataformas de redes sociales como Instagram, Twitter y Facebook son utilizados como tiendas virtuales y marketing digital, sin embargo, también se incrementan las denuncias por casos de estafas que incluyen distintos escenarios entre ellos los siguientes:

A. Perfiles Falsos: Utilizados para la venta de productos principalmente tecnológicos como teléfonos celulares, tabletas y accesorios a muy bajo precio, en cuya oferta se pide la consignación anticipada como mínimo del 50% o 70% del valor total de la compra para el despacho de la mercancía. En muchas ocasiones estos sitios no tienen datos reales de contactos del supuesto vendedor y una vez la persona ha hecho la transferencia bancaria; el estafador no contesta o bloquea las publicaciones de la víctima para evitar que otros usuarios desprevenidos que caminan hacia la estafa puedan alertarse y salir del sitio a denunciarlo.

B. Robo de datos: Otros perfiles en redes sociales son utilizados como plataforma de envío de mensajes fraudulentos que contienen enlaces cuya navegación es dirigida a sitios falsos o suplantados utilizados por el cibercriminal para la captura de datos personales. En algunas ocasiones incluso se habilitan botones de pago con los cuales los criminales capturan los datos bancarios de la víctima.

C. Secuestro de cuentas de Instagram: En esta modalidad los cibercriminales suplantan a los administradores de las redes sociales para enviar supuestas alertas de intentos de fraude en las cuentas de redes sociales de importantes marcas y comercios electrónicos. Mediante el engaño a los responsables del manejo de las aplicaciones en las empresas se apoderan de la cuenta de correo electrónico vinculada al perfil en la red social y su contraseña para luego exigir el pago de dinero a cambio de devolver el control de administración del perfil o evitar la publicación de contenido que puede afectar gravemente la imagen y reputación de la marca. Es muy importante que los perfiles de las tiendas virtuales en internet implementen controles como el doble factor de autenticación, cuentas alternativas de correo de respaldo y token virtual de claves temporales o aleatorias.



Recuerde que, aunque la tienda online se encuentre en una red social debe siempre tener una sección específica con información: “Aviso legal”, “Política de Privacidad”, “Quiénes somos”, “Contacto”, etc.

3. Verifique las referencias y comentarios de otros compradores

Las tiendas en línea y los perfiles en redes sociales y otras plataformas de comercio electrónico permiten la identificación de los perfiles de los vendedores. Por lo anterior es muy importante que antes de realizar una compra se verifique los comentarios o se indague respecto al nivel de reputación de la tienda y del vendedor, puesto que en caso de que haya ocurrido alguna novedad en el proceso de compra o entrega del producto a adquirir, suele ser común encontrar comentarios negativos o advertencias respecto a las prácticas fraudulentas presentadas, información que ayuda a advertir o prevenir a futuros compradores. Es muy importante en estos casos indagar con los números de contacto o perfiles oficiales de las tiendas y marcas utilizadas en la publicidad del sitio web o perfil de la red social a validar.

4. Siempre utilice una conexión a Internet segura

Evite utilizar conexiones a Internet mediante redes WIFI gratuita, puesto que cibercriminales podrían simular redes públicas y dejarlas sin contraseña para la conexión en centros comerciales, restaurantes, cafés, inclusive en servicios de transporte público o terminales aéreas y terrestres que son ampliamente frecuentados durante la temporada. En el mismo sentido un atacante podría vulnerar la seguridad de estas conexiones gratuitas a internet **(man in the middle)** y apoderarse de datos sensibles como información personal y financiera del usuario que realiza una transacción de compra o de venta de productos en línea. Es necesario entonces que, al realizar una transacción electrónica, hagamos uso de una conexión segura (por ej: plan de datos) a través de un dispositivo de confianza (computador, Tablet o teléfono móvil) que haya sido previamente analizado mediante la utilización de un programa de antivirus y la utilización de otros mecanismos seguros de transmisión de información, como las conexiones privadas virtuales (VPN), que garantizan que la información que estamos intercambiando con el portal transaccional viaje segura y no pueda ser interceptada por los cibercriminales.

5. Realice siempre los pagos a través de plataformas autorizadas

Es muy importante identificar la pasarela de pago utilizada para la transacción electrónica. Se recomienda verificar que en el momento de realizar el pago el sitio web o tienda en línea ofrezca alguna plataforma de las ya ampliamente conocidas en Colombia tales como: PayU, Mercado Pago, En línea Pagos, Pagos Inteligentes, ePayco, Interpagos, Pago Digital, Recaudo Express, ev1enlinea, Dicmax, Shopify, Kushki o Mercado Pago. Estas pasarelas de pago son vigiladas por la SUPERSOCIEDADES lo que garantiza que en el caso de alguna contingencia o fraude se pueda acudir hacia las instancias de Gobierno que regulan a estas plataformas.

6. No todo lo que brilla es ORO

En Ciberseguridad existe un viejo adagio que dice que si ***"¿es gratis en internet? Entonces el producto es usted"***, por lo tanto es necesario que antes de dar clic o demostrar algún interés en una promoción que presente un producto a un precio más bajo del habitual o descuentos que pueden llegar inclusive al 80% del valor real, se identifique la legalidad de la tienda, las características del producto ofertado, los comentarios respecto al vendedor como ya lo hemos anotado, las condiciones de entrega, pero sobre todo entender que los cibercriminales buscan robar información que les pueda servir para realizar otros ataques informáticos basados en la suplantación de identidad mediante técnicas de ingeniería social.

Por lo tanto, la emoción propia de la temporada navideña no debe afectar el nivel de atención y la conciencia del riesgo que se presenta por una práctica de navegación desprevenida en la red. Es recomendable definir con anterioridad la necesidad del producto a adquirir estableciendo buenas pautas como una búsqueda de las tiendas oficiales donde se puede encontrar este producto, canales autorizados y conocer precios de referencia, información muy útil para el proceso de decisión antes de realizar la compra de manera segura en el portal o tienda de interés. Además valide antes el domicilio fiscal de la tienda, qué datos recopilan de los usuarios y con qué fin, las formas de pago que permiten y las políticas de envío.

Sospeche tiendas con precios muy por debajo del precio de mercado, o si todos los productos se venden al mismo precio, independientemente del modelo. Al final si se tiene alguna duda es mejor buscar otra alternativa.

7. Proteja siempre sus sitios Web y aplicaciones de Comercio Electrónico

Los sitios web y las aplicaciones de comercio electrónico generalmente almacenan gran número de información personal y financiera de los clientes, por lo que un ciberataque que conlleve una exposición de datos o una brecha de seguridad, puede llegar a comprometer información confidencial de los usuarios y materializar los riesgos operativos reputacionales, legales y de cumplimiento de su negocio o empresa. A continuación, algunas de las recomendaciones para mantener seguros estos sitios y aplicaciones y así prevenir o mitigar el impacto de un ciberataque sobre estas plataformas de alto volumen de tráfico y transacciones:

a. Considere siempre contratar un hosting dedicado, pues una brecha de seguridad en la configuración o actualización de los servidores de una compañía vecina no va a afectar la operación de su empresa; disponer de un hosting dedicado facilita además la seguridad, la estabilidad y la escalabilidad a futuro de su plataforma.

b. Realice siempre copias de seguridad de manera automatizada de todo el sitio con una frecuencia diaria recomendable, pues permite restaurar el portal sin mayor contratiempo.

c. Valide la actualización de las versiones de software utilizadas para la gestión de su hosting, pues ello limita el número de vulnerabilidades susceptibles de explotar por parte de un ciberatacante.

d. Identifique la calidad del soporte técnico disponible, pues facilita la solución rápida de problemas y la comunicación más fluida en caso de una incidencia cibernética.

e. Verifique que el proveedor utilice plugins de calidad, toda vez que plugin mal desarrollado puede generar una brecha de seguridad e impactar el sitio web de una manera crítica. Considere no utilizar versiones gratuitas o de terceros, pues a menudo son difíciles de mantener actualizadas o no se han validado mediante procesos de pruebas de penetración o de analítica de vulnerabilidades.

f. Utilice siempre contraseñas seguras y robustas con combinaciones alfanuméricas e incluso de símbolos, nunca vinculadas a fechas especiales o información que sea fácilmente deducible por parte de un atacante. Establezca mecanismos de recuperación de contraseñas para poder mantener el control del sitio web de Comercio electrónico.

g. Implemente mecanismos de escaneo de seguridad que ayuden a identificar actividades sospechosas o la presencia de algún código malicioso que comprometa la integridad la confidencialidad y la disponibilidad de la información del sitio web. Mantener informado respecto a las últimas alertas de seguridad ayudan a anticipar la materialización de los ciber riesgos.

h. Configure un FIREWALL que ayude a identificar las direcciones IP maliciosas que intenten conectarse a tu sitio web de e-Commerce, bloqueando amenazas comunes y habilitando una capa adicional de seguridad a su portal web.

8. Mantenga el nivel de alerta con las APPS a instalar

Los dispositivos móviles, mediante las aplicaciones descargadas facilitan, entre otros aspectos, los procesos de compras en línea, pues entrelazan las aplicaciones bancarias con los comercios electrónicos. Por lo anterior debemos seguir las mismas recomendaciones para la interacción segura con un sitio web tradicional, veamos entonces:

a. Revisa el número de descargas de la aplicación, si cuentas con pocas instalaciones reportadas por usuarios podría tratarse de una APP no oficial y por tanto debe ser sometida a un análisis cuidadoso para valorar su confianza y fiabilidad.

b. Consulta la valoración de otros usuarios respecto a la APP antes de instalarla o comprarla, pues ayuda a identificar una aplicación fraudulenta o de mala reputación.

c. Identifique el nivel de acceso a su información solicitado por la aplicación y establezca si es razonable y se justifica para el funcionamiento del servicio ofrecido por la aplicación.

d. Conozca la política de privacidad, pago, renovación, actualización y seguridad de la aplicación para evitar inconvenientes a futuro.

e. Evite siempre descargar apps de repositorios no oficiales, ya que no hay ninguna garantía de seguridad de las aplicaciones allí alojadas y cualquiera ha podido manipularlas.

Finalmente es muy importante implementar mecanismos de seguridad, como soluciones de antivirus y escaneo permanente de su dispositivo móvil, en aras de garantizar la protección de su información y contraseñas almacenadas.

9. Conozca la política de privacidad y devolución en los sitios Web

Antes de realizar una transacción para la compra en línea de algún producto es importante que los usuarios conozcan y revisen la política de privacidad y de devoluciones en los sitios web, las cuales deben estar configuradas bajo los parámetros establecidos en la ley 1480 del 2011 conocida como el Estatuto del consumidor en Colombia. Esta norma dispone que los sitios web contemplen todas las garantías para los usuarios frente a los aspectos de calidad, idoneidad y seguridad de los productos o servicios contratados o adquiridos en los portales web.

Sin lugar a duda este instrumento normativo constituye una herramienta fundamental para hacer valer los derechos y establecer las pautas para proceder en caso de que las promesas realizadas en la venta de un producto o en la adquisición de un servicio no se cumplan a satisfacción.

10. Denuncie y reporte los ciberfraudes

Ante la ocurrencia de un hecho fraudulento en Internet es importante que el usuario disponga y conozca de los mecanismos de denuncia virtual. La utilización del portal web de la Fiscalía General de la Nación y de la Policía Nacional (en particular del aplicativo A DENUNCIAR) permite los usuarios víctimas de fraude en internet reportar a las autoridades estos hechos delictivos y de esta manera dar inicio a las investigaciones para establecer los presuntos responsables, unificar los casos de estafas virtuales en la red e identificar nuevas modalidades o incluso alertar sobre la utilización de sofisticados programas maliciosos para el robo de información personal y financiera.

Las redes sociales de la Policía Nacional, también se han constituido en una importante herramienta de contacto con los ciudadanos. A través de la página web caivirtual.policia.gov.co y de las redes sociales Twitter y Facebook la cuenta oficial @Caivirtual facilita la interacción de los ciudadanos con las autoridades e implementar estrategias encaminadas hacia la prevención de los delitos y el uso seguro de internet.

06

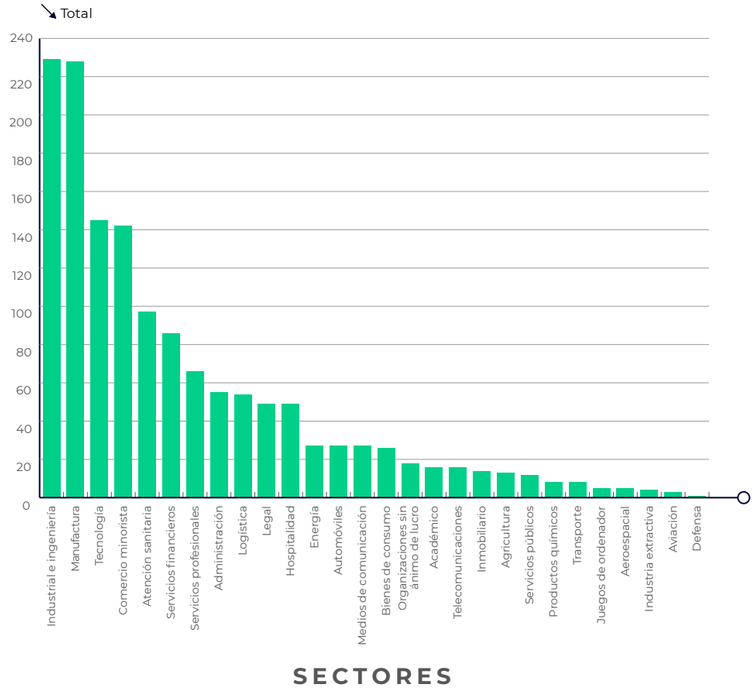
MDR para la ciberseguridad y ciberdefensa empresarial **¿por qué es importante?**

CROWDSTRIKE

Atravesamos a nivel mundial cambios para los cuales no estábamos preparados. Llegó la pandemia y tanto empresas como trabajadores, comenzaron a reinventarse, evolucionar y hacer de la tecnología y el trabajo desde casa, un espacio para darle más importancia a la ciberseguridad como eje vital de la data. Esta nueva normalidad ha implicado masivamente la proliferación de ciberataques y adversarios sin previo aviso. El descuido, la falta de conocimiento, información y herramientas son algunas de las razones por las que en este tiempo algunas organizaciones se han visto afectadas.

Aunque la mayoría de las operaciones de ransomware son oportunistas, el equipo de Inteligencia de CrowdStrike identificó que el mayor número de operaciones de extorsión de datos por ransomware durante este año se presentó en el sector industrial y de ingeniería (229 incidentes), seguido de cerca por el sector manufacturero (228 incidentes). Una alteración en las operaciones diarias afecta el núcleo del negocio si una empresa no logra satisfacer las demandas de producción como consecuencia de interrupciones en el sistema.

SECTORES AFECTADOS POR FUGAS DE DATOS



SECTORES

El ransomware es una de las amenazas de más rápido crecimiento en el ámbito de la ciberseguridad, y se prevé que los daños alcancen los 20.000 millones de dólares a nivel mundial en 2021. Defenderse de los atacantes con grandes motivaciones financieras puede ser un gran reto para organizaciones de todo tipo y tamaño. Requiere no solo tecnología, sino también un profundo conocimiento de las técnicas y motivaciones del atacante, y un equipo de expertos con la habilidad y la disciplina necesaria para detectar, comprender y responder rápidamente a las amenazas emergentes.

Desafíos para manejar el ransomware:

Las organizaciones se enfrentan a algunos desafíos comunes cuando implementan programas de seguridad de endpoints para reducir el riesgo de ransomware, lo que impulsa la demanda por servicios de MDR, tales como Falcon Complete:

1. Dificultades para manejar la tecnología.
2. Incapacidad para actuar de forma confiable y oportuna frente a las amenazas para detener las brechas.
3. Dificultades para remediar adecuadamente los incidentes.

Es por esto que una de las herramientas que pueden ayudar a evitarlo son los servicios MDR.

> *«Para el 2025, el 50% de las organizaciones estarán utilizando servicios de MDR para el monitoreo de amenazas, funciones de detección y respuesta que ofrecen capacidades de contención de amenazas.»*
>
> Investigaciones Gartner

¿Qué es MDR Detección de respuestas gestionadas en ciberseguridad y cuál es la importancia de implementarla en la ciberseguridad y la ciberdefensa empresarial?

Las vulnerabilidades por falta de madurez en la brecha de seguridad en las organizaciones han abierto la puerta a los cibercriminales; delincuentes cibernéticos que usan sistemas informáticos débiles para acceder a datos confidenciales. Incidentes que obligan a los CISO a descubrir herramientas de ciberseguridad y ciberdefensa empresarial para proteger adecuadamente la compañía, al momento de detectar riesgos en la organización, y mitigarlos y con un plan de acción efectivo.

MDR (Managed Detection and Response) es un servicio de ciberseguridad administrado que brinda a las organizaciones un monitoreo activo 24/7 y detección de amenazas basada en una inteligencia que ayuda a responder rápidamente las amenazas detectadas a tiempo.

» ¿En qué ayuda implementar MDR en su organización?

Protege su empresa de eventos de seguridad que podrían dañar su marca y los resultados.

Acelera los objetivos de seguridad y le ayuda a obtener un rápido retorno de su inversión en ciberseguridad.

Hará crecer su negocio con una solución de ciberseguridad que se adapta continuamente a las necesidades de su organización.

Una encuesta realizada por IDC US MDR, muestra que las organizaciones están buscando servicios MDR para ayudar con:

Detección más rápida de intrusiones.

Proporcionar una gestión de amenazas coherente en locales y dominios de la nube.

Acceso a la inteligencia de amenazas.

Acelerar el tiempo para detectar violaciones de seguridad a través de la búsqueda proactiva de amenazas.

Proporcionar capacidades de respuesta a incidentes.

Beneficios con MDR

» **Se elimina la complejidad del SOC**
Los servicios MDR incluyen el uso de un SOC de clase mundial que ya existe y satisface las necesidades del SOC de la organización.

» **Implementación rápida**
Con un SOC ya implementado, la implementación de los servicios MDR lleva semanas en lugar de trimestres.

» **Acceso a expertos en seguridad**
Los proveedores de servicios de MDR ya cuentan con analistas experimentados en su personal, lo que complementa su equipo de TI interno con un equipo de seguridad instantáneo.

» **Mejor detección y respuesta de amenazas**
Manejo más preciso y rápido de amenazas potenciales gracias a herramientas de monitoreo de seguridad.

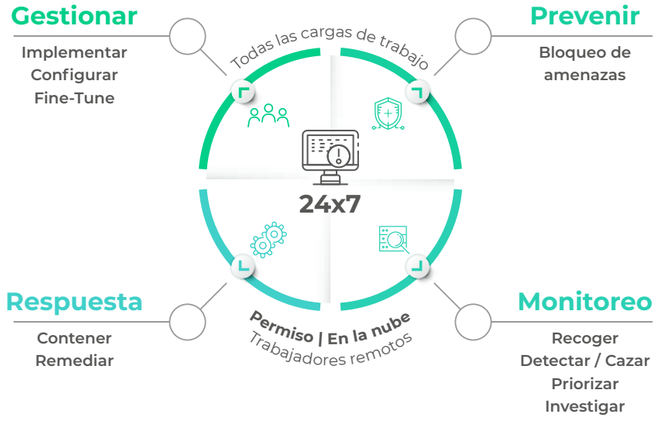
» **Mucho más rentable**
Un servicio MDR se convierte en más que un “gasto operativo mensual” que alivia la carga de implementar y mantener soluciones.

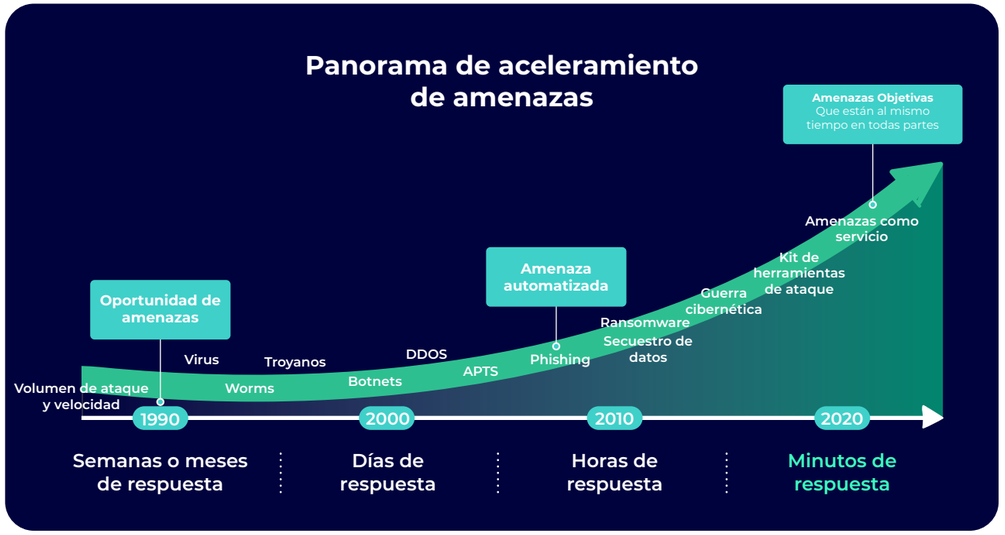
Fuente: *https://info.smartekh.com/*

Los servicios MDR más efectivos deben ofrecerle mejores resultados de seguridad al proporcionarle las herramientas y tecnologías como inteligencia de amenazas, búsqueda de amenazas, monitoreo constante 24/7, análisis avanzado, contención y eliminación de incidentes o violaciones donde se sospecha o se sabe que los datos se han filtrado o destruido. Tenga en cuenta que una oferta de MDR debería ir más allá de ofrecer orientación y recomendaciones. ¿Su organización está preparada para enfrentar sin miedo los ciberataques de cibercriminales? ¿Ya implementa MDR en su organización? Recuerde que la madurez en la brecha de seguridad en una organización es la clave para la protección completa de sus datos e información confidencial. **¡Ayúdenos a disminuir la tasa de ciberataques protegiendo su empresa!**

Conozca cómo funciona nuestro modelo MDR

Detener las infracciones requiere más que tecnología





¡Ayúdenos a disminuir la tasa de ciberataques, protegiendo su empresa!

Referencias

1. https://cybersecurityventures.com/cybersecurity-spending-2021-2025/
2. https://www.europol.europa.eu/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged
3. https://www.ccce.org.co/gestion_gremial/informe-del-comercio-electronico-en-el-segundo-trimestre-de-2021/
4. http://www.idccolombia.com.co/el-surgimiento-de-la-deteccion-y-respuesta-gestionadas-mdr/
5. https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf
6. https://blog.smartekh.com/que-es-la-deteccion-y-respuesta-gestionada-mdr
7. https://blog.netdatanetworks.com/que-es-mdr-deteccion-y-respuestas-gestionadas-en-ciberseguridad

CCIT
tictac
SAFE
SEGURIDAD APLICADA AL FORTALECIMIENTO EMPRESARIAL