Estudio trimestral de ciberseguridad

Ataques a **entidades de gobierno**

CCIT tictac SAFE
SEGURIDAD APLICADA AL FORTALECIMIENTO EMPRESARIAL

Equipo TicTac

Dirección de desarrollo de programas:
Ana Milena Bula Páez

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

Colaboradores
CrowdStrike
César Romero - Architect Systems Engineer- Fortinet

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 2022
Todos los derechos reservados. La distribución y uso de este documento sin fines comerciales está permitida sin restricciones.

Estudio trimestral de ciberseguridad

Ataques a **entidades de gobierno**

CROWDSTRIKE FORTINET

Contenido

1	Prólogo	09
2	Introducción	13
3	Comportamiento del cibercrimen 2022 1T	15
4	Ataques dirigidos a entidades gubernamentales: La gran amenaza del 2022	23
5	Predicciones 2022 - ¿Cómo responder a un Incidente Informático?	31
6	Aproximación a un marco de ciberseguridad: Breve análisis	47
7	Referencias	57

01

Prólogo

Ataques cibernéticos a entidades oficiales:

Un reto más para el 2022

Alberto Samuel Yohai
Presidente Ejecutivo CCIT

Durante los últimos meses se han conocido numerosos casos de ciberataques a entidades oficiales a nivel global y nacional. El año 2021 puso en evidencia la capacidad de defensa de empresas y organizaciones públicas en materia de ciberseguridad, sin embargo, la eficiencia de sus sistemas de seguridad se ha visto perjudicada y es lo que hemos podido evidenciar en algunos de los ciberataques más famosos del 2021 y lo que van en este 2022.

Se podría considerar que el aumento de estos ataques se debe a la sofisticación de las técnicas empleadas. Con la intensificación de los ataques, hubo un gran aumento en la cantidad de dinero de rescate exigido por los atacantes a las víctimas, especialmente debido al incremento en el valor de la moneda virtual *bitcoin*; por esta razón, los rescates pagados por las empresas gigantes a los atacantes alcanzaron decenas de millones de dólares.

El robo de la información se ha convertido en un negocio rentable y esto lo han experimentado inclusive las organizaciones más grandes del mundo; a medida en la que empresas hagan el pago a los ciberdelincuentes va a seguir creciendo este sistema criminal. En Colombia ocurren muchas situaciones de este tipo, de hecho entidades como el Senado, la Presidencia y Fuerzas Militares, han sido víctimas de ataques.

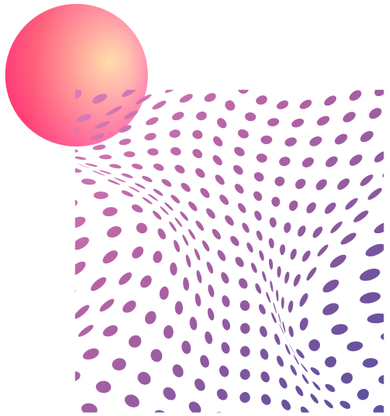
Entre los más recientes está el caso del Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima), la Aeronáutica Civil y el Departamento Administrativo Nacional de Estadística de Colombia (DANE), quienes reportaron *ransomware*, afectación a servidores internos y ataques informáticos a información sensible y confidencial.

Por eso, es importante resaltar que el gobierno nacional ha hecho grandes esfuerzos para avanzar en materia de ciberseguridad, destacándose el reciente **Decreto de ciberseguridad** que busca fortalecer la gobernanza de la seguridad digital; la identificación de infraestructuras críticas cibernéticas y servicios esenciales; la gestión de riesgos y la respuesta a incidentes de Seguridad Digital. Además, establece la inminente cooperación y coordinación de los CSIRT sectoriales y la Plataforma de Notificación y Seguimiento de Ciberincidentes.

Vemos con buenos ojos los avances en esta materia, pero es necesario que las entidades sigan avanzando en los modelos de madurez de ciberseguridad, estableciendo campañas y fortaleciendo la figura de los CISOs como una estrategia que permita alinear los objetivos de prevención y control en las organizaciones.

02

Introducción



En el año 2021 se presentaron 41 billones de intentos de ataques cibernéticos en el mundo y siete billones en Colombia. Los cibercrímenes generan cada vez más rentabilidad para los atacantes y en este sentido, si no existen herramientas para contrarrestarlos y estar protegidos, seguirá creciendo la curva de ciberataques para empresas y entidades de gobierno.

De acuerdo con el último informe presentado por la Fiscalía General de la Nación, en Colombia en el año 2021 el número de ataques cibernéticos aumentó en un 30%, comparado con el año anterior. Si bien, las compañías y entidades oficiales han venido trabajando fuertemente en estrategias tendientes a robustecer las medidas de ciberseguridad, estas no han sido suficientes, ya que casos como el secuestro de información o la afectación de datos a entidades mediante *Ransomware* o ataques de día cero sin filtración de datos, aún continúan presentándose y han ocasionado grandes pérdidas económicas para las organizaciones ya que éstas han tenido que efectuar cuantiosos pagos frente a este tipo extorsiones a los cibercriminales.

Recordemos que la ciberseguridad tiene que ser parte del escenario estratégico organizacional, por ello no es suficiente velar por el fortalecimiento y la actualización de los sistemas, hacer copias de seguridad y cerrar las brechas que se generan a partir de las vulnerabilidades, sino que de igual manera resulta primordial adoptar un enfoque proactivo en el sentido de evaluar las posibles amenazas contra la seguridad de las entidades, así como tomar las precauciones necesarias en materia de cooperación con las instituciones locales e internacionales para evitar que la información de carácter sensible y confidencial caiga en manos equivocadas.

A través de este estudio, los invitamos a que conozcan las cifras más recientes de tendencias del cibercrimen en el primer trimestre del año. Así mismo, gracias a nuestros aliados, tanto empresas como entidades de gobierno podrán identificar la manera adecuada en la que se debe reaccionar frente a un ataque informático, y qué hacer cuando se detecta.

Finalmente, analizaremos el contexto para el 2022 en materia de ciberseguridad para empresas y entidades oficiales, y cómo estas deben estar preparadas para enfrentar una nueva ola de ataques.

03

Comportamiento del Cibercrimen 2022 1T

Escrito por: CR (RA) Fredy Bautista García

Un nuevo panorama se ha identificado en 2022, y ha sido el incremento y sofisticación de Ciberataques a entidades del estado que podrían estar siendo objeto de campañas dirigidas con la finalidad de propagar y difundir programas maliciosos. Han sido públicos los **Ciberataques a entidades estatales** como el Departamento Administrativo Nacional de Estadísticas (DANE), el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (INVIMA), el Departamento Nacional de Planeación (DNP) entre otros, que hacen parte del ya extenso inventario de afectaciones a sitios públicos (dominio gov.co).

El nivel de criticidad y características de los ataques puede variar, sin embargo, las modalidades más comunes se encuentran asociadas a la infección de malware con distintos alcances, sin embargo la motivación es la obtención ilícita de ganancias, bien sea por el robo de credenciales, el secuestro de información (Ransomware), la exfiltración y fuga de información de credenciales de seguridad con fines de exposición en internet y la venta de datos en la DarkNet (aunque cada vez es más frecuente la venta de datos en internet superficial).

Por ejemplo, desde el 2018 se han detectado campañas de difusión de malware contra entidades estatales atribuidas a grupos cibercriminales como Blind Eagle o APT C36 presunto grupo de espionaje muy activo en algunos países de la región, y que ha sido señalado como responsable de ataques principalmente a instituciones del gobierno colombiano, así como a importantes corporaciones en el sector financiero y la industria petrolera.

La problemática ha evolucionado; como lo refleja el hallazgo de **193 sitios web**, de entidades públicas colombianas, que han sido infectados y sustraídos los datos de usuarios gubernamentales o usuarios públicos de servicios públicos gubernamentales; que finalmente fueron dispuestos para su distribución y venta en la internet profunda y expuestos en foros de Dark web.

Fuente: https://darktracer.com/news

El programa malicioso utilizado en esta ocasión por los ciber atacantes es Redline Stealer que recopila credenciales de cuentas guardadas en navegadores web, detectado por primera vez en la web oscura en marzo del 2020. Luego de sustraídas las contraseñas son expuestas para la venta en los mercados ilegales de Internet.

Al respecto globalmente se han conocido cerca de 142 mil sitios infectados y adicionalmente en febrero de 2022, fue revelada una filtración de más de 12 millones de credenciales de usuarios afectados en 49.880 sitios gubernamentales a nivel mundial.

En Colombia entre las entidades con alertas de datos exfiltrados se encuentran la Dirección de Impuestos y Aduanas Nacionales (DIAN), la Comisión Nacional del Servicio Civil (CNSC), el Instituto Colombiano para la Evaluación de la Educación (ICFES), la Unidad del Servicio de Empleo, la Agencia Nacional de Contratación Pública, el ICETEX, COLPENSIONES, la Secretaría de Hacienda del Distrito de Bogotá, Migración Colombia, el Fondo Nacional del Ahorro y la Alcaldía de Medellín.

Ranking de Sitios de dominio gubernamental con mayor exposición de credenciales de usuarios comprometidas:

No.	Dominio.gov.co comprometido	Credenciales expuestas
66	muisca.dian.gov.co	3,318
226	simo.cnsc.gov.co	1,122
277	www2.icfesinteractivo.gov.co	933
328	personas.serviciodeempleo.gov.co	766
446	www.icetex.gov.co	555
461	evaluarparaavanzar311.icfes.gov.co	539
500	sede.colpensiones.gov.co	499
512	oficinavirtual.shd.gov.co	489
573	community.secop.gov.co	434
605	servidorpublico.sigep.gov.co	414
629	miseguridadsocial.gov.co	404
682	epagos.registraduria.gov.co	373

No.	Dominio.gov.co comprometido	Credenciales expuestas
703	www.colpensiones.gov.co:8070	359
744	jovenesenaccion.dps.gov.co	339
813	www.positivaenlinea.gov.co	307
837	web.sispro.gov.co	296
893	visibles.migracioncolombia.gov.co	273
910	www.fna.gov.co:8081	265
937	snrbotondepago.gov.co	254
943	webazure.dian.gov.co	252
1077	solicitudes.icetex.gov.co	213
1200	www.medellin.gov.co	192
1244	ecenso.dane.gov.co	182
1297	www.funcionpublica.gov.co	176

Fuente: *Informe completo disponible en https://bit.ly/35AeMcz*

Recientemente el Instituto Nacional de Vigilancia de Medicamentos y Alimentos- Invima fue víctima de un ataque cibernético contra su plataforma tecnológica, según lo informó la entidad el impacto del ciberataque comprometió un 80% de los servicios generando indisponibilidad de información, sistemas, página web, correos electrónicos y otros aplicativos institucionales.

En efecto se trató del Ransomware BlackByte[1] cuyos indicadores de compromiso fueron publicados por el FBI en una alerta generada el 11 de febrero del 2022, justamente 5 días después que la entidad viera comprometidos el 80 % de la información almacenada en los servidores, luego de 53 días la entidad restableció los servicios. Más información acerca del Ransomware Black byte se encuentra disponible en el sitio de la Agencia de Ciberseguridad en Infraestructura Crítica de los EE. UU. en el siguiente enlace: https://www.cisa.gov/uscert/ncas/current-activity/2022/02/15/fbi-and-usss-release-advisory-blackbyte-ransomware

El caso del Invima confirma la tendencia identificada por SAFE, en la cual actualmente se presenta una disminución gradual y sostenida de los Ciberataques de afectación baja, y las técnicas más especializadas de los atacantes se enfocan ahora hacia organizaciones más grandes entre las que se cuentan las entidades públicas, pues el nivel de preparación de los responsables de enfrentar la problemática no es proporcional a la cantidad y riesgos de las amenazas identificadas.

Además, el grado de madurez con respecto a la ciberseguridad en el sector público en Colombia es muy variable; podría señalarse que algunas entidades del sector defensa, sector energético y de hidrocarburos cuentan con estrategias de largo alcance bien formuladas y en ejecución, pero en el nivel descentralizado, no ocurre lo mismo y las brechas de seguridad generadas por errores de configuración y obsolescencia tecnología son muy frecuentes.

Otro factor para considerar es la posibilidad de mejorar la obtención de ganancias ilícitas derivadas de la monetización por la venta de datos[2] en foros de internet.

[1] https://www.ic3.gov/Media/News/2022/220211.pdf
[2] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Veamos entonces el comportamiento del cibercrimen en Colombia durante el primer trimestre del 2021:

En lo corrido del año respecto a las infracciones a la Ley 1273 de 2009 (Ley de Delitos Informáticos en Colombia) se presentó una disminución del -23.1% en el número de denuncias por ciberdelitos, en comparación a las reportadas durante el 2021.

En el primer trimestre del 2022 se registraron en Colombia **9.226** denuncias por ciberdelitos; cerca de **3 mil casos menos** que el año anterior, cuando ya se habían reportado **12.012** casos de afectación a la integridad, confidencialidad y disponibilidad de los datos y sistemas de información en el mismo periodo de tiempo 1T 2021.

Los tres delitos con mayor impacto en relación directa con el número de ocurrencia de incidentes de ciberseguridad siguen siendo en su orden los siguientes:

El Hurto por medios informáticos con **3.574** casos en 2022 frente a 3.981 casos presentados en el 1T 2021. Casos recurrentes de robo de credenciales bancarias para luego suplantar a los usuarios y transferir los activos de las cuentas afectadas.

La **Violación de datos personales** con **1.947** casos registran una disminución del 39% dada la diferencia con el 2021 cuando fueron reportados 3.204 casos.

Y la **suplantación de sitios WEB** generalmente relacionados con casos de phishing que registro 914 casos en 1T 2022 en comparación a 1545 casos en 1T del 2021.

Otra de las tendencias identificadas en 2022, han sido los ciberataques especializados a empresas proveedoras de servicios o actores de la **cadena de suministros tecnológicos.** Los actores maliciosos saben que a través de ataques dirigidos a vendedores y proveedores podrían comprometer a sus clientes si se valen de recursos tecnológicos compartidos.

Muchas empresas trabajan con docenas de proveedores, desde suministro de materiales de producción hasta la externalización de trabajo y tecnología. Debido a ello, es muy importante proteger la cadena de suministro y asegurar que las empresas proveedoras de tecnología se encuentren debidamente aseguradas.

Finalmente uno de los factores a considerar durante el 2022; es el proceso electoral que actualmente se desarrolla en Colombia, para todos es bien conocido el incremento en el número de actividad maliciosa, que podría generar un mayor número de alertas a la Registraduría Nacional del Estado civil, particularmente en los aplicativos y plataformas tecnológicas a través de las cuales se informa a los votantes; los sitios de votación la notificación como jurados de mesa e incluso los reportes preliminares de resultados basados en el preconteo en los puestos de votación.

Con el fin de poder hacer frente a estas amenazas el Gobierno nacional ha expedido recientemente normativas que facilitan la implementación de buenas prácticas orientadas a la adopción de planes de Ciberseguridad al interior de las entidades públicas del País.

04

Ataques dirigidos a entidades gubernamentales:

La gran amenaza del 2022

CROWDSTRIKE

Nos enfrentamos a una nueva ola de ataques dirigidos, más rápidos y precisos.

Durante el 2021, los adversarios especializados en ataques dirigidos aprovecharon el caos ocasionado por la pandemia para desarrollar nuevas tácticas, adaptadas a los cambios del mundo y las nuevas oportunidades operativas que presenta. Entre los destacados por su adaptabilidad están adversarios rusos, chinos, iraníes y norcoreanos.

Adversarios rusos: Enfocaron sus ataques en proveedores de servicios IT y en la nube, debido al auge del teletrabajo.

Adversarios chinos: Aumentaron la militarización de vulnerabilidades para facilitar los esfuerzos de acceso inicial a sus objetivos.

Adversarios iraníes: Usaron ransomware para camuflar sus actividades dirigidas como si se tratara de cibercrimen común.

Adversarios norcoreanos: Centraron sus esfuerzos en atacar entidades de criptomoneda para mantener sus ingresos durante la crisis económica de la pandemia.

Por si fuera poco, estos ataques dirigidos son cada vez más rápidos, lo que dificulta su detección y respuesta. El equipo de CrowdStrike midió los tiempos de infiltración —es decir, el tiempo que le toma a un adversario moverse lateralmente de un host a otro dentro del mismo entorno afectado— y descubrió que el promedio es de apenas 1 hora y 38 minutos.

Esto significa que los adversarios tienen un alto nivel de sofisticación en sus ataques y tienen la preparación necesaria para moverse rápidamente de un punto a otro una vez que logran una brecha. Si no está listo, el equipo de seguridad tiene poco tiempo para reaccionar y evitar que los datos sean comprometidos.

El tiempo promedio de infiltración es de apenas 1 hora y 38 minutos.

¿Qué pueden esperar los gobiernos para el 2022 en materia de ciberseguridad?

1 Aumento en las "operaciones sombra"

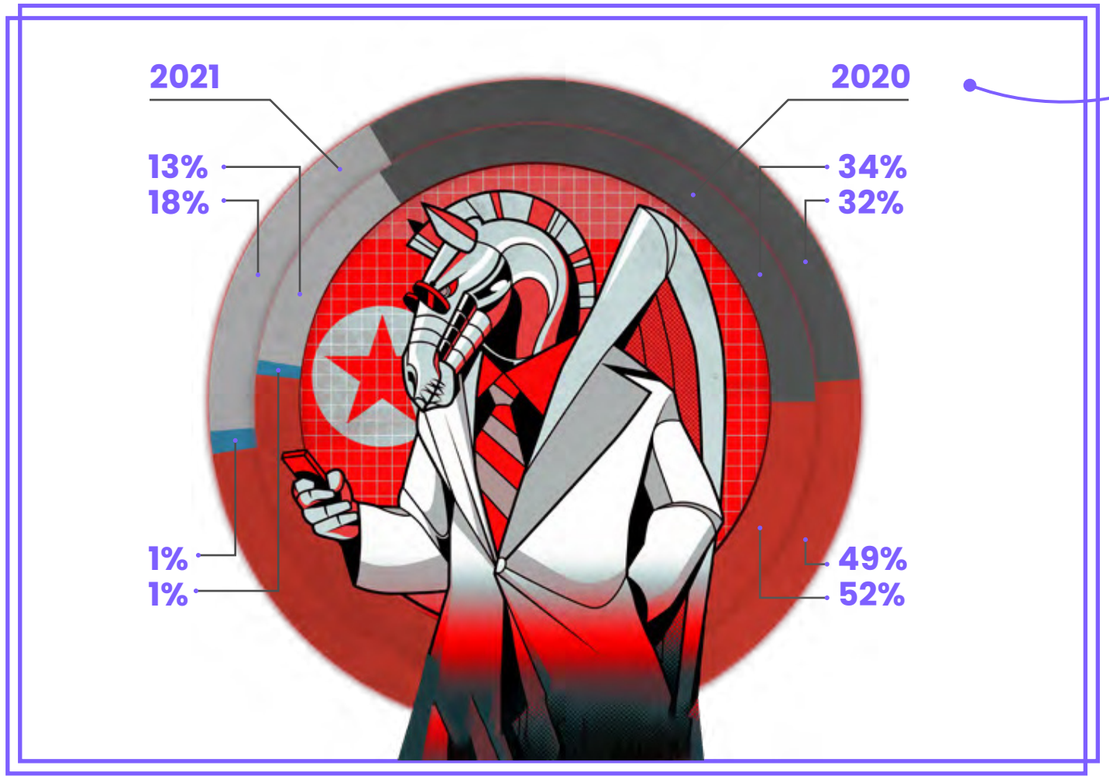
Los ataques de estilo "Lock-and-Leak", como el uso de ransomware para encriptar datos críticos —interrumpiendo las actividades de una organización— y luego filtrarlos, han ganado relevancia entre los grupos que se denominan hacktivistas y grupos criminales de alto perfil. Toda la información filtrada es amplificada a través de páginas y foros dedicados a compartir los datos con otros adversarios, para atraer la atención hacia el ataque.

Sin embargo, estas operaciones de alto perfil no son el único problema. Últimamente, los adversarios aprovechan el caos inicial para realizar ataques simultáneos, más sutiles, cuyo objetivo es explorar las defensas de las agencias gubernamentales en búsqueda de vulnerabilidades que sirvan como nuevo punto de entrada. Estos "ataques sombra" usualmente derivan en futuras disrupciones con ransomware o eliminación de datos, mucho más complejas.

CrowdStrike Intelligence

sigue de cerca a diferentes grupos que se especializan en ataques de tipo "Lock-and-Leak".

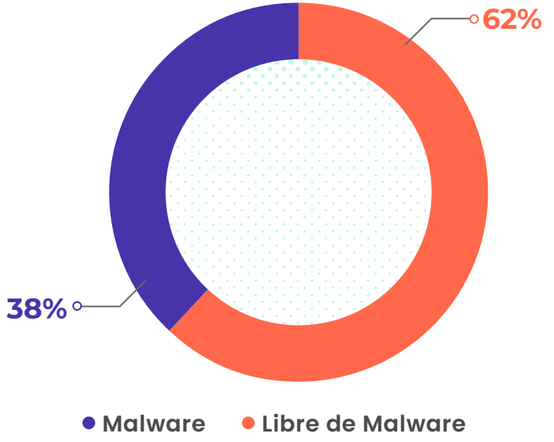
El éxito de estas operaciones simultáneas ha permitido que los adversarios interrumpan las actividades de numerosos objetivos clave en sus respectivas regiones y el mundo con una eficiencia mayor que otros modelos de ataque. Es muy probable que la tendencia se mantenga en aumento a lo largo de todo el año.



- **CiberCrimen:** La principal motivación de estos ataques es financiera.
- **Hacktivismo:** Actividades pensadas para ganar visibilidad y transmitir un mensaje político.
- **Ataque dirigido:** Patrocinados por estados rivales. Incluye ciberespionaje y operaciones disruptivas.
- **Sin atribuir:** Data insuficiente para determinar la motivación del ataque.

2 Los adversarios se apartan del uso de malwares

Durante el 2021, los ataques sin malware casi duplicaron a los ataques con malware. Los adversarios que se especializan en este tipo de ataque usan un enfoque conocido como "vivir del campo", es decir, utilizan vulnerabilidades intrínsecas de las plataformas que atacan o roban credenciales legítimas del personal encargado de la seguridad para para infiltrarse, en lugar de escribir malware al endpoint.



El 62% de los ataques que analizó CrowdStrike Intelligence durante el último trimestre del 2021 fueron libres de malware. Este tipo de ataques está diseñado para saltarse las defensas tradicionales y dificultar su detección.

Los tres puntos críticos para el 2022 son:

- Identidad
- Datos
- Nube

El aumento en el robo de credenciales y extorsiones a personal crítico han contribuido a la creación de nuevos mercados donde adversarios especializados comercian credenciales y contraseñas, que luego son utilizados en los mencionados ataques "Lock-and-Leak".

3 Explotación de Log4Shell y vulnerabilidades derivadas

En noviembre del año pasado, se descubrió una importante vulnerabilidad en las librerías de registro Apache Log4j2. Esta vulnerabilidad, bautizada como Log4Shell, permite que los atacantes tengan acceso remoto a los sistemas, que pueden aprovechar para entregar paquetes maliciosos o adquirir datos sensibles.

Varios adversarios han incorporado este exploit a su arsenal y los ataques han aumentado en complejidad desde entonces. El principal riesgo de Log4Shell es su carácter general dentro de los sistemas, lo que dificulta medir el impacto de la vulnerabilidad y permite que los adversarios tengan acceso a una amplia variedad de entornos para atacar.

Sin embargo, no todos los productos comprometidos con esta vulnerabilidad pueden explotarse de la misma manera: los adversarios necesitan ajustarse a cada caso particular, lo que ha impedido, hasta ahora, que este vector se popularice.

CrowdStrike Intelligence cree que, a medida que los adversarios ganen experiencia en la explotación de Log4Shell, veremos un aumento en la integración de la vulnerabilidad entre sus vectores de ataque.

Conclusiones

Los ataques siguen aumentando en precisión y complejidad. Estos son algunos insights que le ayudarán a adaptarse y optimizar la seguridad de su organización.

1. Construya una cultura de ciberseguridad

Una higiene IT robusta a lo largo de toda la organización es la mejor forma de prepararse. Las áreas críticas, como endpoints y trabajos en la nube, deben ser una prioridad.

2. Conozca a su adversario

Detrás de cada ataque, hay una persona con sus propias motivaciones e intereses. Infórmese sobre los grupos que operan contra su sector y sus principales vectores de ataque. La inteligencia de CrowdStrike Falcon X puede ayudarle a mantenerse al día.

3. Invierta en agilidad

Durante una infiltración, cada segundo hace la diferencia. Invierta en soluciones que aporten visibilidad y agilidad a sus equipos de seguridad, para que puedan responder a los ataques con las tácticas adecuadas.

4. Adelántese a las tendencias

El 80% de los ataques actuales se producen por robo de credenciales legítimas. Utilice soluciones de analítica conductual, como CrowdStrike Falcon Identity Threat Protection, para identificar en tiempo real accesos sospechosos y actuar antes de que sea tarde.

5. Implemente el modelo Zero Trust

El auge del robo de identidad y el amplio mercado para los datos secuestrados significan que las amenazas pueden estar dentro de su propia organización. Adoptar un modelo Zero Trust es más importante que nunca.

6. Invierta en detección de amenazas

62% de los ataques son libres de malware, por lo que la tecnología sola no puede prevenirlos. Contar con el apoyo de expertos que cierren las brechas tecnológicas, como Falcon Complete y Falcon OverWatch, es una excelente forma de apoyar a su equipo.

7. Establezca una estructura a prueba de errores

Los errores humanos siguen siendo un factor decisivo en las incursiones a datos en la nube. Es importante establecer una estructura con roles y patrones definidos, que ayuden a reducir los errores en las operaciones.

05

Predicciones 2022

¿Cómo responder a un Incidente Informático?

Escrito por: César Romero Architect Systems Engineer

FORTINET

Si fuera posible escoger una palabra para describir los eventos de ciberseguridad de finales de 2021 y principios de 2022, sería definitivamente “velocidad”, ya que los cibercriminales hoy operan a gran velocidad y se resalta detalladamente en el reporte semestral “Global Threat Landscape”[3] de los laboratorios de FortiGuard para H2 de 2021.

Los hallazgos muestran que los ciber criminales están desarrollando ataques más rápido que nunca. Se continúa explotando la creciente superficie de ataque de los entornos híbridos recientemente creados por la pandemia, usando estrategias de cibercrimen persistentes que son más destructivas y menos predecibles que las que hemos visto en el pasado.

Como si el Covid-19 no nos hubiese traído suficientes emociones, el 2021 nos trajo nuevos retos para las áreas de tecnología y sus equipos de seguridad e infraestructura. Si bien algunas amenazas las vimos aparecer por primera vez, muchas otras probaron que siguen siendo omnipresentes, y que se mantienen vigentes causando tanto daño como lo han hecho en los años anteriores.

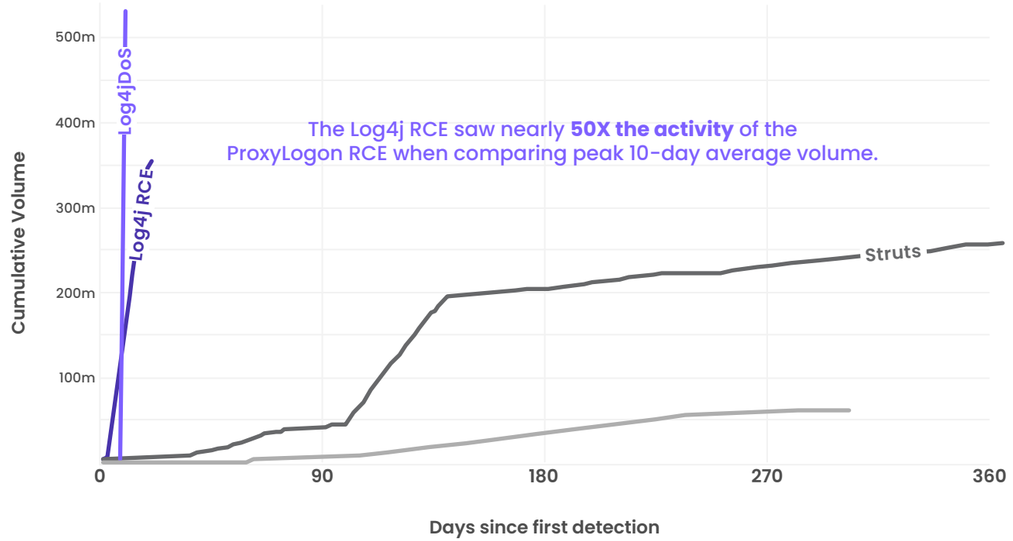
A continuación, algunas de las enseñanzas que nos deja el 2021 y nos recuerdan cómo estas amenazas - tanto nuevas como viejas – trabajan en tándem para poner a prueba nuestras medidas de seguridad.

[3] report-q1-2022-threat landscape.pdf (fortinet.com)

1

Log4j nos demostró la velocidad de los exploits

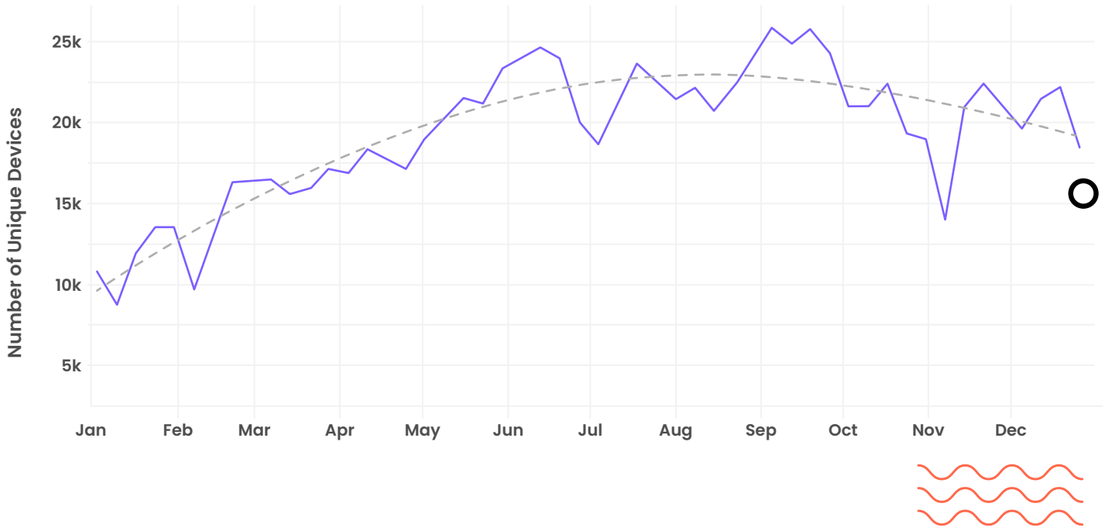
En solo 21 días, Log4j alcanzó 1,4 veces el volumen acumulado que logró la infame falla de Struts (CVE-2017-5638) en un año.



2

Adversarios apuntando rápidamente a nuevos vectores – Linux

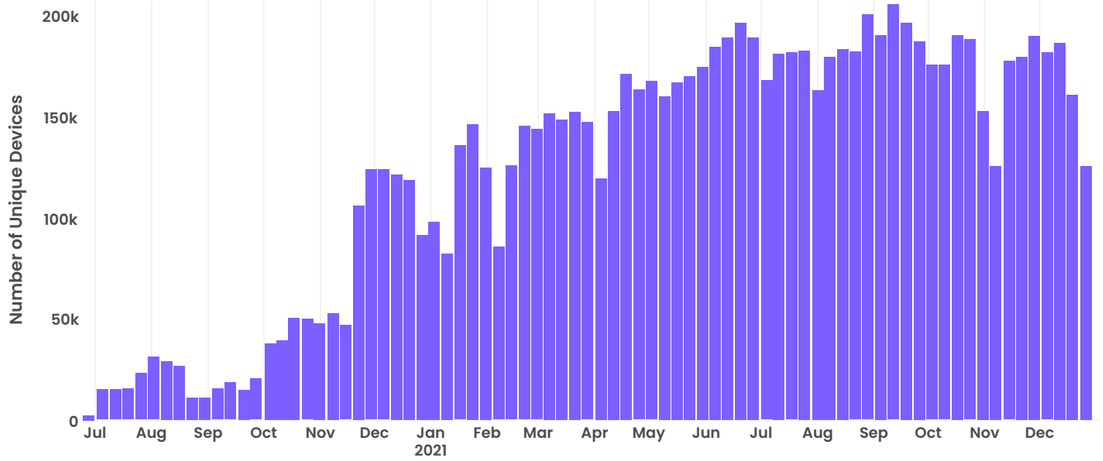
No hace mucho, Linux era una de las plataformas menos atacadas, pero esas épocas quedaron atrás y en 2021 se doblaron las detecciones de malware en archivos ELF (formato binario para Linux).



3

Los ataques de Ransomware siguen siendo implacables

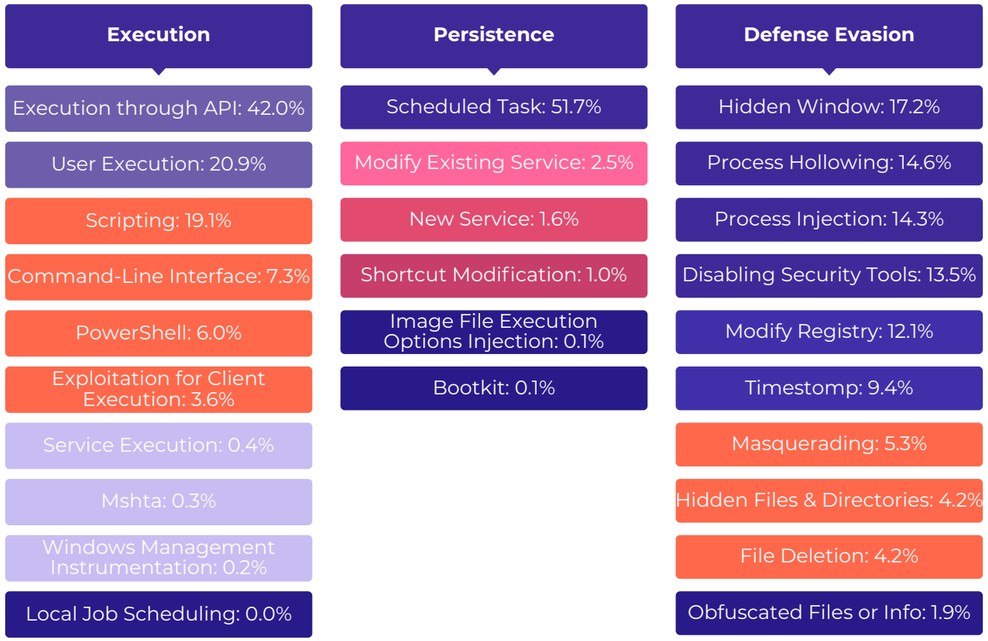
Si bien los ataques muestran una variedad de nuevas cepas de ransomware, otra tendencia problemática es el uso de ransomware viejo que se está actualizando, mejorando, y reusando.



4

Una comprensión más profunda de las técnicas de ataque detiene a los criminales más rápido

Detener a los adversarios en una etapa temprana es más crítico que nunca, si se logran identificar estas técnicas, en algunas ocasiones una entidad podría cerrar efectivamente los métodos de ataque de un malware.



Technique prevalence for select tactics during H2 2021

Los incidentes son inevitables y la respuesta inmediata es fundamental

Estamos siendo testigos de un periodo trascendental en la evolución de la arquitectura empresarial de las entidades. Si asemejamos el roadmap tecnológico de las empresas con el curso de un rio, sucesos históricos como la pandemia y la creciente adopción de la transformación digital representarían las cascadas que hacen que el rio cambie su nivel, composición y velocidad. Son estos grandes eventos los que terminan definiendo la historia de quienes estarán listos para responder eficientemente contra los incidentes, y quienes se les inundará el patio trasero ante un eventual desborde.

Adicionalmente, los ataques continúan acelerando en sofisticación y (como lo mencionamos previamente) velocidad. Ejemplos como la automatización del malware y las técnicas de evasión, hacen difícil no solo detenerlos, sino que ayudan a una propagación más veloz. Los adversarios ahora ocupan más tiempo haciendo reconocimiento ('stalkean' nuestra red) para identificar víctimas específicas. Pasan semanas mapeando y eludiendo nuestros controles de seguridad. Cuanto más acechan, más daño pueden legar a infringir. Esto les da la oportunidad no solo de plantar el malware que mejor se acomode, sino de encontrar las formas más eficientes para exfiltrar nuestra información o tomarla como rehén.

Las organizaciones se han venido dando cuenta que no pueden escapar de los incidentes, pero claro que es posible mitigarlos. Definir un plan de respuesta ante incidentes (IR) **antes** de que se presente alguno es clave dentro de cualquier estrategia de ciberseguridad.

¿Qué es Respuesta a Incidentes?

IR es el proceso de detectar, investigar, y gestionar las consecuencias de un incidente o violación de seguridad. El objetivo es limitar la cantidad de daño (costo y reputación) causado por el ataque y reducir el tiempo de recuperación.

Típicamente este proceso requiere equipos especializados, las herramientas correctas, y procesos bien documentados.

Habilidades necesarias para responder eficientemente ante un incidente

Típicamente los equipos de TI están enfocados en la operación diaria de las herramientas de seguridad. La mayoría enfocados en prevención de amenazas, y equipos dedicados a la implementación, configuración, y gestión de las herramientas.

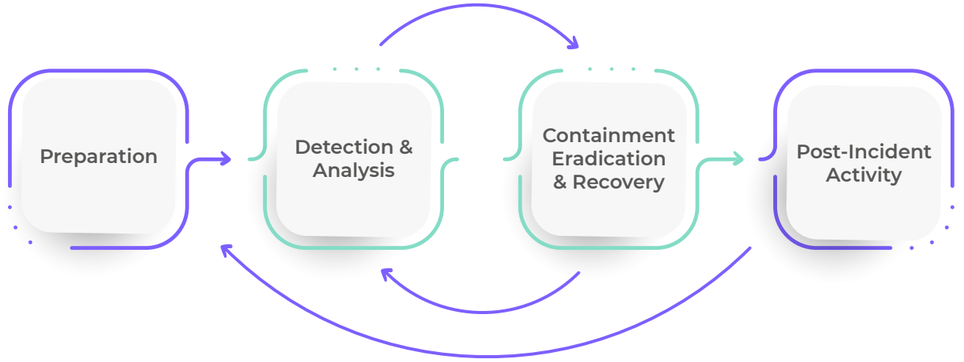
En contraste, cuando una entidad se encuentra en el medio de un incidente, se requiere un set de habilidades ante emergencias y conocimiento especializado en ciberseguridad. Estos incluyen habilidad en:

- Autenticación y control de accesos
- Análisis de código malicioso.
- TTP (tácticas, técnicas y procedimientos por sus siglas en inglés) de los adversarios.
- Diseño de los protocolos.
- Vulnerabilidades de seguridad.
- Fallas en implementación.
- Análisis forense digital.

En conclusión, necesitan conocer las herramientas y el actuar de los ciber atacantes, más que las tecnologías y operación de la ciber defensa.

Proceso de Respuesta a Incidentes

Todas las acciones de respuesta tienen que ocurrir mucho más rápido (y con mayor precisión) que las operaciones estándar. La lista de procesos operacionales y los tiempos varían según la entidad, pero podemos encontrar una buena guía en la publicación de NIST "Computer Security Incident Handling Guide"[4], si bien es del 2012, no mucho ha cambiado desde entonces. En el siguiente gráfico se puede observar el ciclo de vida definido por la NIST para la respuesta a incidentes:



Preparación

Las metodologías de IR suelen hacer mucho énfasis en esta fase, donde se definan las capacidades requeridas para responder, y la máxima prevención posible a través del fortalecimiento de los controles en las redes, aplicaciones e infraestructura. Si bien el equipo de IR no hace parte de esta fase, es fundamental para el éxito del programa.

Mantener la cantidad de incidentes relativamente bajo es clave para la protección de los procesos de negocio de las entidades. Si los controles de seguridad son mínimos o muy antiguos, el gran volumen de incidentes puede sobrepasar la capacidad del equipo de IR. Algunas de las prácticas recomendadas para asegurar los sistemas, redes, y aplicaciones:

[4] SP 800-61 Rev. 2, Computer Security Incident Handling Guide | CSRC (nist.gov)

Evaluaciones de riesgo periódicas sobre los sistemas y aplicaciones misionales.

Seguridad de las estaciones con soluciones de nueva generación.

Seguridad de red a través de un 'Mesh' de Ciberseguridad.

Entrenamiento y concientización a los usuarios finales.

Detección y Análisis

Debido a la gran cantidad de formas en que puede ocurrir un incidente, no es viable tener un paso a paso de como manejar cada incidente. Las entidades deben estar preparadas para identificar los posibles vectores de ataque, los cuales pueden estar dados por distintos signos del incidente (precursores e indicadores). Algunas de las herramientas para identificar estos signos incluyen:

- SIEM
- EDR
- Sandbox
- Deception
- Indicadores de CSIRTs
- SOAR

Se debe realizar un análisis exhaustivo de los registros y eventos relevantes, así como los mecanismos forenses de los archivos y memoria en búsqueda de cargas útiles (*payloads*) maliciosas.

Todos estos entregables dependerán de la preparación, madurez y herramientas internas que se tengan desplegadas en la entidad. Es de vital importancia iniciar en esta fase la documentación de todos los hechos relacionados con el incidente. Parte de la información que se debería tener dentro del seguimiento es la siguiente:

- Estado actual del incidente
- Resumen del incidente
- Estaciones comprometidas identificadas
- Cuentas comprometidas identificadas
- Línea de tiempo documentada de eventos relevantes
- Análisis del malware a profundidad
- Artefactos forenses e IoCs identificados
- Identificación de datos exfiltrados y métodos usados
- Acceso inicial a la entidad y paciente cero
- Siguientes pasos (ej. Restaurar backups, actualizar, etc.)
- Información de contacto de los involucrados

Así mismo es importante realizar la priorización de los incidentes con base en el impacto a la organización, y la debida notificación a las distintas partes (CIO, CISO, CSIRT gobierno, RRHH, COLCERT, etc.)

Contención, Erradicación y Recuperación

Esta fase o puede ocurrir secuencialmente y seguir un patrón iterativo. La contención brinda tiempo para definir una estrategia de remediación a la medida, por lo que es esencial definir qué se va a realizar (ej. Apagar los sistemas, desconectarlos de la red, deshabilitar ciertas funciones). Estas estrategias varían dependiendo del tipo de incidente (ataque de DDoS, ransomware, etc.), por lo que se podría definir la adecuada con base en algunos de los siguientes criterios:

- Potencial daño y robo de recursos
- Necesidad de preservación de evidencia
- Disponibilidad del servicio
- Tiempo y recursos para implementar la estrategia
- Efectividad de la estrategia
- Duración de la solución

Si bien la razón principal para recolectar evidencia es resolver el incidente, esta se puede necesitar para asuntos legales. Dado esto es importante mantener documentada y protegida la cadena de custodia.

Identificar al atacante puede ser un proceso lento y poco apreciado, pero puede llegar a minimizar en gran medida el impacto al negocio. Algunas de las actividades más comunes para identificar al atacante incluyen:

- Validación de IoCs relevantes
- Búsqueda del host en motores de búsqueda
- Uso de bases de datos de incidentes
- Monitoreo de canales de comunicación

Luego de se ha logrado contener, es necesario erradicar componentes del incidente, eliminando cuentas de usuario comprometidas e identificando las vulnerabilidades que fueron explotadas. Es importante identificar todas las estaciones comprometidas de tal forma que se puedan remediar.

En la recuperación se restauran los sistemas a la operación normal, y se confirma que están funcionales. Algunas de las actividades que se incluyen acá son restaurar backups confiables, reconstruir sistemas de cero, reemplazar archivos comprometidos, instalación de parches, cambio de contraseñas, y fortalecimiento de los controles de seguridad.

Actividades Post-Incidente

Una de las partes más importantes de la IR y la más comúnmente omitida: lecciones aprendidas. Realizar una reunión luego de un incidente mayor puede ser increíblemente útil para mejorar las medidas de seguridad y el proceso de IR en sí. Algunas de las preguntas a responder en la reunión incluyen:

¿Qué pasó exactamente?

¿Qué tan bien se siguió el proceso de IR? ¿Se siguieron los procesos documentados? ¿Fueron adecuados?

¿Qué información se hubiera necesitado más pronto?

¿Qué se haría diferente la próxima vez?

¿Qué acciones correctivas podrían prevenir incidentes similares en el futuro?

¿Qué herramientas adicionales se necesitan para detectar, analizar, y mitigar futuros incidentes?

Con toda esta información se puede estudiar las debilidades de seguridad de la entidad, así como en los procesos de IR, la cual se puede utilizar para definir procesos de evaluaciones de riesgo, que llevaran a la selección e implementación de controles adicionales.

Recomendaciones finales

Las recomendaciones principales expuestas para el manejo de incidentes se resumen a continuación:

- Adquirir herramientas y recursos que aporten valor durante el manejo de incidentes.
- Prevenir incidentes al asegurar redes, sistemas, y aplicaciones.
- Identificar precursores e indicadores a través de alertas generadas por las soluciones de seguridad.
- Establecer mecanismos de colaboración con equipos externos (CSIRTs, COLCERT, etc.)
- Perfilar redes e infraestructura.
- Entender comportamientos normales de la red, sistemas y aplicaciones.
- Tener una política de retención de registros.
- Realizar correlación de eventos.
- Mantener y usar una base de conocimiento de la información.
- Registrar toda la información una vez se sospecha que ha ocurrido un incidente.
- Proteger la información de los incidentes.
- Priorizar el manejo de los incidentes con base en factores relevantes.
- Establecer estrategias y procedimientos para contener los incidentes.
- Seguir los procedimientos establecidos para el manejo y recolección de evidencia.
- Realizar reuniones de lecciones aprendidas después de incidentes importantes.

06

Aproximación a un marco de ciberseguridad:

Breve análisis

Escrito por: CR (RA) Fredy Bautista García

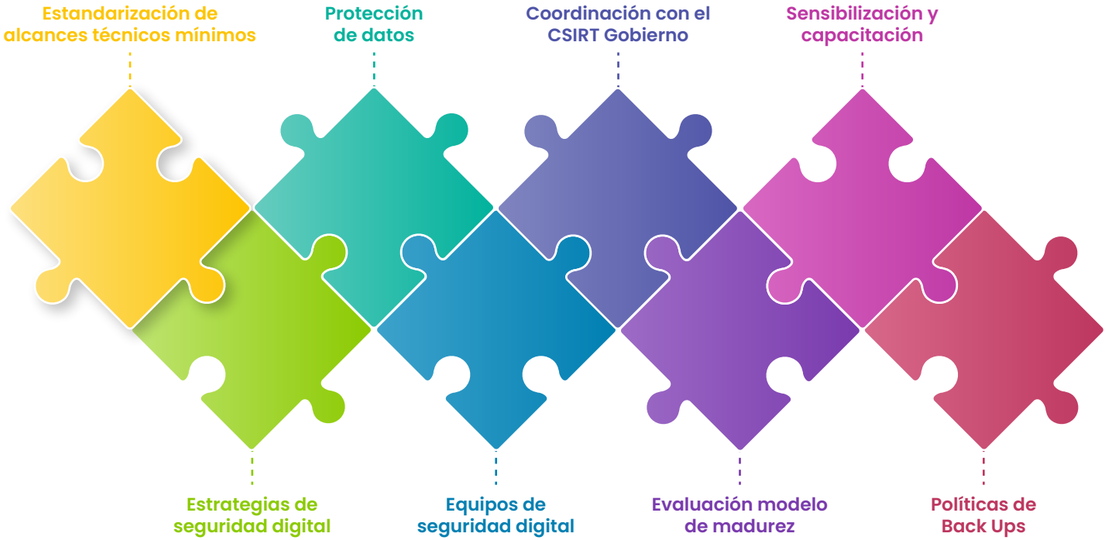
Durante el 2022, el sector público ha venido implementando diferentes normativas enfocadas a reiterar el cumplimiento de buenas prácticas para el aseguramiento de la información, la protección de los datos y la gestión de riesgos en el entorno digital. La reciente expedición de la circular 001 y la Directiva presidencial 02 de febrero de 2022, reafirmaron los lineamientos y directrices de la política de seguridad y confianza digital en el País.

Estos documentos fueron base para la promulgación del decreto No. 338 del 08 de marzo del 2022, enfocado al fortalecimiento del modelo de gobernanza digital en el país. Desde el programa SAFE de la CCIT, reconocemos la importancia en el avance de las capacidades gubernamentales para garantizar el fortalecimiento de la seguridad digital.

La Circular 01 del 17/02/2022 del Departamento Administrativo de la Presidencia de la República y consejería presidencial para la transformación digital estableció algunos deberes de los Proveedores de servicios en la nube (CSP), al recomendar a las entidades del estado contar con elementos de seguridad nativos ante ataques de denegación de servicio (DoS) y ataques de denegación de servicio distribuido (DDoS), así como garantizar la seguridad de los datos en reposo y tránsito.

En el mismo sentido la circular estableció que las entidades deben requerir a los proveedores la garantía de disponer de herramientas especializadas, las cuales pueden ser adquiridas por las entidades para reforzar sus esquemas y garantizar la seguridad ante vulnerabilidades al hardware sobre su infraestructura, la segmentación de clientes y la instalación de parches de seguridad, aspectos de suma importancia para reducir riesgos para los servicios informáticos prestados por las entidades.

En la misma línea fue publicada la directiva presidencial 02 del 24/02/2022 mediante la cual se reiteró la política pública en materia de seguridad digital dirigida a todas las entidades públicas de la rama ejecutiva del orden nacional; y estableció algunas directrices para garantizar una implementación segura de la política de Gobierno liderada por el MINTIC.



Se destacan entre otros aspectos los siguientes:

1. **Estandarización de alcances técnicos** mínimos exigibles respecto a la seguridad de la infraestructura, la protección de los datos y la garantía de resiliencia corporativa oportuna ante cualquier incidencia que comprometa la oportunidad y disponibilidad de la información. (Respecto a la contratación de servicios en la nube).

2. **Implementación de una estrategia de seguridad digital** en la que se integran los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital en concordancia con el modelo de seguridad y privacidad de la información MSPI

3 **Priorización de la protección de datos personales** e información sensible de las entidades mediante la gestión efectiva de riesgo en el entorno digital con un enfoque preventivo y proactivo.

4 **Conformación de equipos o grupos de seguridad digital**, encargados de verificar la aplicación de políticas y estrategias al interior de la entidad.

5 **Coordinación con el CSIRT Gobierno,** para la gestión de incidentes de seguridad digital mediante el diseño de un procedimiento que permita su tratamiento, investigación y gestión.

6 **Realización de una evaluación del modelo de madurez** en seguridad de la información mediante el instrumento de autodiagnóstico del MSPI de Mintic.

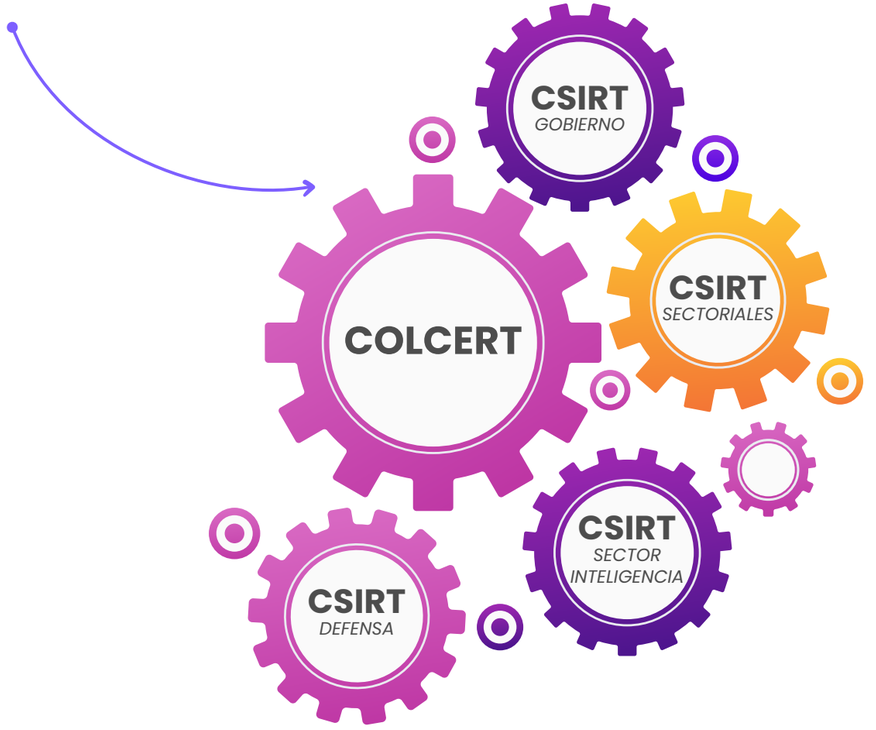
7 **Sensibilización y capacitación a todos los funcionarios** de las entidades en materia de seguridad digital y sus implicaciones, así como formación especializada para las áreas a cargo de la seguridad digital.

8 **Generación de políticas de Back Ups** y respaldos de la información y procedimientos de copias de seguridad, así como la disposición de planes de continuidad de negocio, orientados a contener, responder, recuperar y reanudar la operación ante la materialización de un ciberataque.

Todas las anteriores recomendaciones, contribuyen de manera significativa al aseguramiento de la información y a la robustez de las plataformas de las entidades como de los proveedores tecnológicos.

Con el fin de dar alcance al Decreto único reglamentario del sector de las tecnologías de la información y las comunicaciones (Decreto 1078 del 2015), el pasado mes de marzo del 2022 fue expedido el Decreto 338 del 08/03/2022 que incorporó un nuevo título al marco regulatorio de las TICs denominado los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructura críticas cibernéticas, la gestión de riesgos y la respuesta a incidentes de seguridad digital.

Inicialmente estableció los sujetos obligados refiriéndose a las entidades de la administración pública y los particulares que cumplen funciones públicas denominándolos como autoridades para efectos del cumplimiento del decreto con alcance a las personas jurídicas de derecho privado que tengan a cargo la prestación de servicios y que administren y gestionen **infraestructuras críticas cibernéticas** o de servicios esenciales. Posteriormente definió conceptualmente los Equipos de Respuesta, Equipos Sectoriales de Incidentes de Seguridad Digital, Infraestructuras Críticas Cibernéticas, riesgos de seguridad digital, servicios esenciales, vulnerabilidad de seguridad digital entre otros.



En el mismo sentido estableció el modelo de gobernanza de seguridad digital como un sistema de trabajo compuesto por un conjunto de políticas de operación, principios, normas, reglas, procedimientos de toma de decisiones y programas compartidos por las múltiples partes interesadas de la seguridad digital del país, con el fin de fortalecer las capacidades para la gestión de riesgos e incidentes de seguridad digital y la respuesta proactiva y reactiva a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes de información que en conjunto constituyen el entorno digital en el país.

Respecto a los niveles de las acciones en el marco del modelo de gobernanza de seguridad digital del país, el decreto en análisis estableció los niveles estratégico, táctico y operacional.

El nivel estratégico será el responsable de definir la política y la prioridad estratégica dentro de la estrategia nacional, así como los objetivos a largo plazo y el modo en el que las múltiples partes interesadas deben interactuar entre sí. Por su parte el nivel táctico elabora los planes procesos y procedimientos para coordinar las actividades de seguridad digital y finalmente el nivel operacional establece el status en el que se implementan y llevan a cabo actividades tareas y rutinas definidas por el nivel. Otro aspecto importante dentro del modelo de gobernanza son las instancias de decisión y para ello se establecen en su orden de jerarquía las siguientes:

La coordinación Nacional de Seguridad digital.

El comité Nacional de Seguridad digital.

Los grupos de trabajo de seguridad digital.

Las mesas de trabajo de seguridad digital.

Los puestos de mando unificado de seguridad digital.

Y es que precisamente de manera reciente ha venido cobrando mucha importancia la implementación de los puestos de mando unificado de seguridad digital como una instancia de colaboración y coordinación interinstitucional cuyo objetivo es el de articular y facilitar la toma de decisiones estratégicas y operacionales necesarias para la prevención y gestión de un incidente cibernético que ocurra sobre una infraestructura crítica o servicio esencial. **En el marco de estos puestos de mando unificado se han gestionado por ejemplo los PMU CIBERNÉTICOS durante el proceso electoral del 2022.**

Otro segundo elemento de importancia es la **identificación de infraestructuras críticas cibernéticas y servicios esenciales,** aquí vale la pena destacar que durante los últimos años en el marco de la política trazada desde el CONPES 3701 de 2011 lineamientos de la Política en ciberseguridad y ciberdefensa, el CONPES 3854 del 2016 Política de seguridad digital y el CONPES 3995 del 2020 Política de seguridad y confianza digital, el Comando Conjunto de Ciberdefensa de las FFMM CCOCI por sus siglas; en coordinación con el Equipo de Respuesta Nacional a Emergencias Cibernéticas COLCERT, han venido liderando las denominadas **mesas de infraestructura crítica** nacional mediante las cuales se han establecido los catálogos e inventarios de infraestructuras críticas cibernéticas qué servirán como fuente de información para dar cumplimiento a lo establecido en la sección cuatro del decreto en análisis, que dispone de la realización de un inventario de las infraestructuras críticas públicas cibernéticas nacionales.

Los criterios establecidos para la elaboración de este catálogo, establece de manera inicial el desarrollo o actividad o servicio fundamental que permite el mantenimiento de actividades sociales o económicas nacionales o que cuenten con información privilegiada del nivel estratégico o de seguridad del Estado.

Por supuesto que la prestación de dicha actividad o servicio depende de una red o sistema de información o la utilización de las TIC y finalmente considera que un ataque o un incidente sobre estas redes traería un efecto significativo en la prestación de dicho servicio.

Como ya lo mencionamos el decreto establece doce (12) meses para la realización del inventario de infraestructuras críticas cibernéticas y de servicios esenciales mediante una metodología que incorporará la identificación de un representante ante el Comité Nacional de Seguridad Digital de cada una de estas infraestructuras dentro de los sectores catalogados. Es importante igualmente conocer que la normativa establece igualmente el deber de vinculación de las infraestructuras críticas ante el MINTIC específicamente al Grupo de Respuesta a Emergencias Cibernéticas de Colombia COLCERT; **aspecto que implícitamente conlleva a traslado del equipo de coordinación de emergencias cibernéticas del Ministerio de Defensa hacia el Ministerio de las Tecnologías de la Información** y las que le comunicaciones, situación NO por cuanto debe garantizarse que el nivel de coordinación y respuesta permita la vinculación de las Fuerzas Militares y la Policía Nacional; instituciones que desde hace más de 12 años han venido desarrollando un proceso de madurez en sus capacidades para la respuesta ante ciberincidentes y la investigación judicial de los ciberdelitos.

El decreto 338 del 2022 establece igualmente unas obligaciones respecto a la **implementación de un plan de seguridad digital,** la protección de las redes tanto en de las infraestructuras críticas cibernéticas como los servicios esenciales y los sistemas de información en el ciberespacio debiendo realizar evaluaciones del riesgo de seguridad digital de manera periódica. No obstante, lo anterior, no se define la periodicidad ni frecuencia de estas evaluaciones sin embargo sí exige que las autoridades cuenten con normas, políticas, procedimientos, así como recursos técnicos, administrativos y humanos necesarios para la gestión efectiva del riesgo.

Finalmente se destaca es la definición del **modelo nacional de atención y gestión de incidentes**; instrumento que permitirá articular los equipos de respuesta a incidentes de seguridad digital en sus diferentes niveles con el COLCERT, CSIRT Gobierno, CSIRT Defensa, CSIRT del sector de inteligencia y los CSIRT sectoriales, así como los equipos de respuesta a incidentes de seguridad digital de los diferentes sectores definidos como críticos o prestadores de servicios esenciales.

Al respecto, deberá trabajarse en un protocolo para incorporar los estándares a la gestión de incidentes de seguridad digital nacional estableciendo los roles, responsabilidades, mecanismos de comunicación y tiempos de respuesta que debe cumplir cada equipo, así como la responsabilidad sobre el procesamiento o tratamiento de los datos personales, la adopción de medidas de responsabilidad demostradas para el debido tratamiento de la información y la protección de la información referente a incidentes de seguridad digital.

Aunque no se detalla de manera tácita el mecanismo de intercambio de información o seguimiento a los incidentes sí se establece que se utilizará una plataforma nacional de notificación y seguimiento de incidentes de seguridad digital que permitirá el intercambio de información útil entre los equipos sectoriales mediante mecanismos de comunicación segura y confiable garantizando la Protección de Datos de carácter personal.

La plataforma de intercambio deberá garantizar la disponibilidad, la autenticidad, la integridad y la confidencialidad de la información además de facilitar el acceso a las autoridades competentes para poder efectuar el seguimiento y el estado de situación de los incidentes en el ámbito de las competencias.

El reto es significativo pues las autoridades deben contar con una taxonomía, criterios para establecer la criticidad de los incidentes, los mecanismos de intercambio de información sobre ciber amenazas, las capacidades disponibles para el análisis de muestras de artefactos maliciosos(malware), el registro y notificación de vulnerabilidades de las entidades que compartan información en esta plataforma, así como la generación de estadísticas e informes agregados.

Respecto al deber de denuncia, señala que ante la materialización de una conducta punible deberá instaurarse la respectiva denuncia ante las autoridades competentes para que se adelanten las investigaciones por parte de los organismos de investigación judicial.

Reflexiones finales

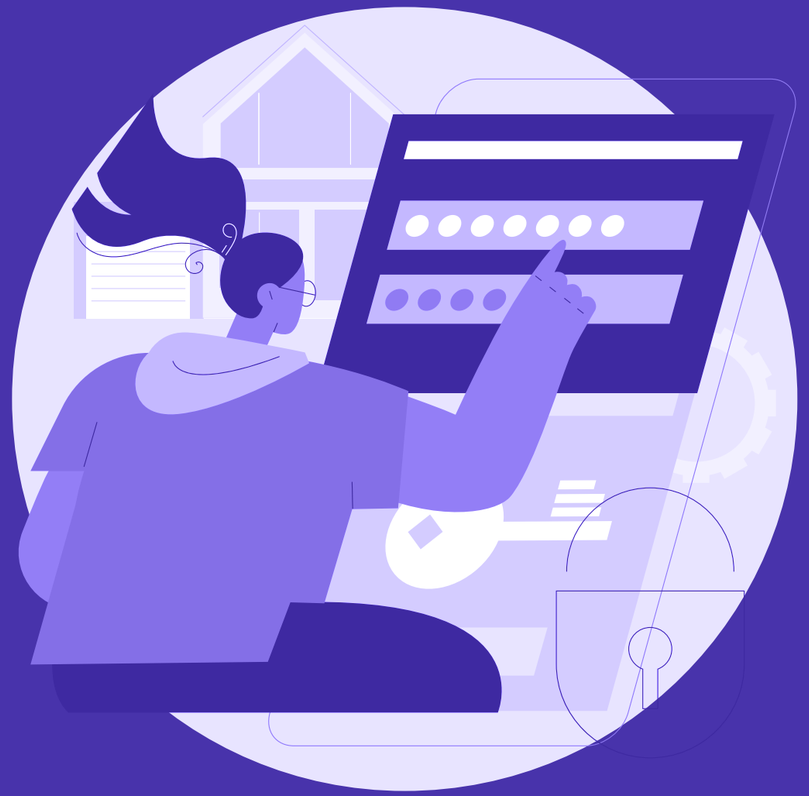
Cómo queda claro este Decreto consigue articular muchas de las necesidades previamente identificadas dentro de la comunidad responsable de la gestión de los incidentes en el país, puesto que establece además de un marco de definiciones conceptuales sobre las cuales se deben entender y comunicar las entidades, el establecimiento de las instancias decisorias, la designación oficial de los puestos de mando unificado de seguridad cibernética como órgano táctico y operativo para la gestión de incidentes de ciberseguridad en situaciones de crisis o coyunturas y el modelo relacional entre los equipos de respuesta en las diferentes instancias o niveles de responsabilidad dentro del ecosistema de seguridad digital.

El reto es hacer un seguimiento a las medidas establecidas de cara a su cumplimiento y que además se garanticen los principios de seguridad jurídica a los operadores de tecnología con responsabilidad en la norma ante las tareas a implementar que seguramente ya tendrán fijadas y situadas por los niveles de madurez de seguridad y experiencia de los últimos años.

Creemos en todo caso que esta normativa se constituye en un hito importante para el País, casi en el mismo nivel de Ley 1928 del 24/07/2018 por medio de la cual Colombia aprobó el convenio sobre la ciberdelincuencia o la misma expedición de la ley 1273 de 2009, que configuro nuevos tipos penales en nuestro ordenamiento jurídico y que permite hoy en día asegurar la persecución de los Ciberdelitos en Colombia.

Referencias

1. CrowdStrike. 2022 Global Threat Report. Consultado en marzo del 2022. Disponible en: https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2022GTR.pdf



CCIT
tictac
SAFE
SEGURIDAD APLICADA AL FORTALECIMIENTO EMPRESARIAL