CIBER - SEGURIDAD

EN LA ERA DE LA MOVILIDAD DIGITAL

CCIT tictac SAFE

Equipo TicTac

Dirección de desarrollo de programas:
Ana Milena Bula Páez

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

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

Diseño y diagramación:
Paula Cruz Giraldo

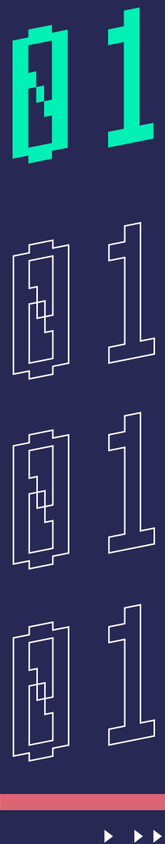
Sobre el TicTac
El TicTac es el primer tanque de análisis y creatividad del sector TIC en Colombia, establecido por la CCIT con el fin de proponer iniciativas de política pública orientadas a la transformación digital del país, con base en la sostenibilidad y competitividad económica, la inclusión social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

CIBER - SEGURIDAD

EN LA ERA DE LA MOVILIDAD DIGITAL

CROWDSTRIKE FORTINET

Contenido



PRÓLOGO

Alberto Samuel Yohai
Presidente Ejecutivo CCIT

La movilidad ha traspasado las fronteras del mundo físico para convertirse en un concepto de gran relevancia en los escenarios digitales. Por ejemplo, hoy en día no solo se habla del tráfico vehicular sino del tráfico de datos, que se ha vuelto uno de los activos más importantes en el mundo para empresas de todos los sectores de la economía y de todos los tamaños.

Hace dos años este concepto cobró gran relevancia por el gran volumen de datos que se mueven por las diferentes redes. Por ello se ha convertido en uno de los más importantes desafíos de las empresas alrededor del mundo poder proteger sus propios datos, así como los de sus clientes, proveedores y demás miembros de su cadena de valor.

El intercambio constante de información y su capacidad de transportar archivos infectados ha convertido a todo tipo de dispositivos en blancos para los ciberdelincuentes. Si bien la tecnología ha facilitado y mejorado muchos procesos, los dispositivos móviles modernos resultan atractivos para la sustracción o robo, debido tanto a su valor económico (del propio hardware), como al valor asociado a la información sensible y personal que almacenan.

Este estudio tiene como objetivo evidenciar el panorama actual referente a ciberseguridad y la importancia de protegernos para salvaguardar la integridad de la información. Los invitamos a conocer de primera mano las herramientas y buenas prácticas como resultado de la investigación realizada con nuestros aliados, que con seguridad les proporcionará interesantes alternativas para poner en práctica.

02

02

02

02

INTRODUCCIÓN

En los últimos años se ha demostrado que la tecnología es el mejor aliado de las compañías y en general, de todas las personas; un ejemplo claro de ello es la forma en la que actualmente funciona el modelo de trabajo en el que se evidencia la migración de lo presencial a lo virtual. Si bien este cambio de modelo laboral surgió en gran parte a raíz de la pandemia, el mismo le ha exigido a todas las compañías el reto de abrir su información y darle un manejo diferente, así como permitir que sus colaboradores puedan trabajar desde cualquier punto y desde cualquier aparato tecnológico que cuente con conexión a internet y permita acceder a la información corporativa.

De igual manera esta implementación de nuevas formas para salvaguardar la información, surge como respuesta a las necesidades de la era de la movilidad digital, en la cual los ciudadanos en su día a día deben desplazarse de un lugar a otro junto con la información para desempeñar sus labores; de allí la importancia de destacar la relevancia del rol que desempeña el Chief Information Security Officer (CISO) en las compañías ya que en cabeza de él se encuentra la obligación de implementar todos los mecanismos necesarios que aseguren las mejores prácticas de ciberseguridad empresarial y todos los retos que esto conlleva.

De acuerdo con lo anterior se puede evidenciar de manera clara la importancia de la implementación de la ciberseguridad en los diferentes ámbitos, teniendo en cuenta ese gran reto que han tenido que afrontar no solo las empresas sino en general los particulares para proteger la información contra los crímenes cibernéticos.

Actualmente las cifras que se reportan en materia de ciberseguridad al cierre del primer semestre de 2022, aseguran que algunas tipologías del cibercrimen han demostrado una reducción significativa como la Violación de Datos Personales, la Suplantación de Sitios Web para Capturar Datos Personales y el Uso de Software Malicioso que presentaron variaciones del **-11%**, **-13%** y **-27%** respectivamente.

Hay otro tipo de vectores que siguen creciendo, como el acceso abusivo a sistema informático que presentó 6.407 casos, es decir 46% más que en el mismo periodo del año anterior, ubicándolo como el delito con mayor crecimiento, y el hurto por medios informáticos que presentó un incremento del 15% con 11.078 casos denunciados.

Por medio de este estudio, se dará a conocer las últimas tendencias del cibercrimen, la forma de proteger la data que se encuentra en la nube y por supuesto algunas recomendaciones clave para la protección de la identidad; recordemos que no basta con implementar algunas herramientas, ya que también resulta importante hacer un debido seguimiento al buen uso de los accesos empresariales y de los equipos que han sido asignados a los colaboradores así como el desarrollo de capacitaciones constantes en materia de vulnerabilidades y nuevas técnicas de robo ya que estas últimas resultan ser indispensables para alertar, detectar y manejar un posible caso de ciberataque.

03

03

03

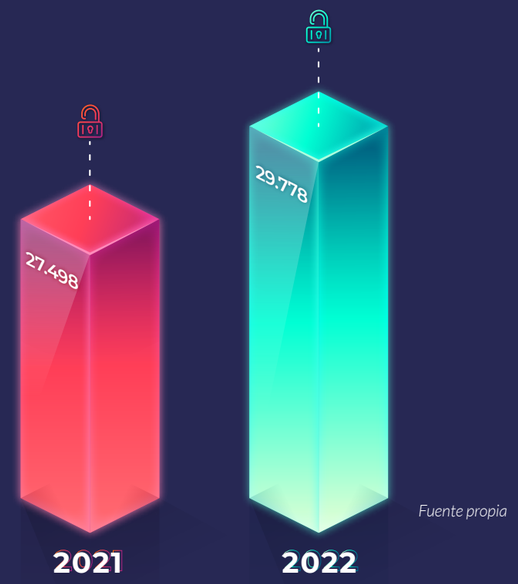
03

COMPORTAMIENTO DE
LAS CIFRAS DEL CIBERCRIMEN
2022

Escrito por: CR (RA) Fredy Bautista García

Sigue creciendo el Hurto por Medios Informáticos y el Acceso Abusivo a Sistema informático

Durante el primer semestre del 2022, las cifras de ciberdelitos denunciados ante el SPOA Sistema Penal Oral Acusatorio de la Fiscalía General de La Nación[1] se han incrementado en un **8%** respecto a los registros del año inmediatamente anterior; este incremento corresponde a la variación de **2.280** casos más en la presente anualidad.



29.778 DENUNCIAS
01 enero 2022 - 30 junio 2022

27.498 DENUNCIAS
2021

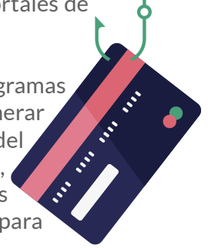
Fuente propia

Pese a lo anterior, algunos delitos de tipo penal como la Violación de Datos Personales, la Suplantación de Sitios Web para Capturar Datos Personales y el Uso de Software Malicioso presentan una **reducción significativa** que fluctúa entre **-11%**, **-13%** y **-27%** respectivamente.

[1] https://adenunciar.policia.gov.co/Adenunciar/Login.aspx?ReturnUrl=%2fadenunciar%2f

Este hallazgo no resulta menor, teniendo en cuenta que los principales vectores de ataques utilizados para materializar las afectaciones a la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos en Colombia, históricamente se han basado en ataques de phishing mediante la suplantación justamente de sitios web con la finalidad de apoderarse de las credenciales bancarias o información relevante como datos personales de usuarios desprevenidos que luego son utilizados para la suplantación de identidad y la configuración de otros tipos penales asociados al cibercrimen como la estafa y la extorsión.

Sin embargo, no todas son buenas noticias, pues al contrario, el número de denuncias de hurto por medios informáticos presentan un incremento del 15%, siendo que durante el 2021 se registraron **9.593** casos en comparación a **11.078** denuncias instauradas durante el 2022, es decir una variación de **1.485** casos más. Lo que permite confirmar que la motivación de los ciberatacantes sigue basándose en el interés económico y la facilidad de poder obtener rentas monetarias de una manera rápida mediante el compromiso de las cuentas bancarias de las víctimas a través del apoderamiento de sus credenciales para el acceso a los portales de interacción con las entidades.



Si bien es cierto, otros tipos de ataques como la infección de los sistemas informáticos con programas maliciosos para cifrar la información conocidos genéricamente como ransomware, pueden generar una grave afectación en las operaciones de las empresas e incluso comprometer la continuidad del negocio ante la interrupción del acceso controlado a los sistemas informáticos de las compañías, resultando claramente con que el **mayor impacto económico** lo siguen generando las defraudaciones a los activos financieros mediante la manipulación de los sistemas informáticos para apoderarse de los activos en las cuentas bancarias de las empresas.

Al verificar las posibles causas generadoras del incremento en el número de casos denunciados por hurto por medios informáticos, deben considerarse las numerosas campañas de malware asociadas a la suplantación de entidades gubernamentales aprovechando los contextos de la política y realidad nacional, pues se incrementaron los casos de infecciones vinculadas a enlaces maliciosos en correos electrónicos que suplantaron a la registraduría nacional del estado civil como lo es el caso del reciente correo **“Reactivar mi Cédula”** en el que se utilizó la cuenta reportesc@registraduria.gov.co de apariencia legítima pero que suplanta al dominio de la entidad mediante técnicas de Spoofing mail[2], veamos:

[2] Email Spoofing es una técnica que utilizan los atacantes para ocultar la verdadera dirección del remitente en un correo malicioso y sustituirla por una legítima suplantando la identidad de una empresa o un usuario al utilizar un dominio auténtico.

Fuente propia

Casos similares han sido detectados por el COLCERT (Equipo de Emergencia Cibernética de Colombia), en los cuales se ha suplantado a la Dirección de Impuestos y Aduanas Nacionales, o incluso a la Fiscalía General de la Nación.

Otra causa para analizar respecto al incremento del hurto por medios informáticos en Colombia se encuentra relacionada con el incipiente modelo de implementación de modelos MFA o múltiples factores de autenticación de usuarios al interior de las compañías. Los cuales suelen adicionar una capa a las ya poco seguras "contraseñas", tales como la implementación de controles biométricos vinculados a los dispositivos o la generación de **OTP** por sus siglas en inglés (One Time Password), y que mediante estos se generan códigos de un solo uso que han resultado ser muy eficientes a la hora de prevenir la suplantación de sesiones y de accesos no autorizados por parte de los cibercriminales.

Fuente propia

Es importante igualmente considerar la implementación de controles duales para la autorización y aprobación de la dispersión de pagos de nóminas o pagos de facturas a proveedores, pues esta última situación es aprovechada por las redes del cibercrimen para la materialización del denominado fraude del gerente o fraude de CEO o fraude BEC (Business Email Compromise) por sus siglas en inglés. Recordemos que en el último informe del FBI[3] las cifras de fraudes BEC a nivel global durante el 2021 superaron los 2.4 billones de dólares siendo por ende la modalidad delictiva que mayor afectación económica le infringe a las empresas y personas a nivel mundial.

El fraude BEC es posible bajo la materialización de modelos de ingeniería social implementados por los cibercriminales a través de los cuales mediante técnicas de robo de información basadas en el envío de enlaces con formularios fraudulentos para obtener datos sensibles o incluso mediante la utilización de llamadas telefónicas para "sonsacar" información crítica de los procesos comerciales y de producción en las compañías.

Finalmente es importante considerar el comportamiento del acceso abusivo a sistema informático, delito que registró durante el 2021; un total de **4.390** casos en comparación a 6.407 denuncias registradas durante la presente anualidad; lo anterior equivale a una variación de 2.017 casos más denunciados en 2022, esto es un 46% de incremento porcentual que claramente lo ubica como el delito de mayor crecimiento durante el presente año.

Esta cifra refleja el volumen de interacciones que los cibercriminales tienen con los sistemas que van a comprometer pues recordemos que los accesos abusivos se dan en las fases iniciales de los ciberataques bien porque se realiza por agentes externos que han conseguido desarrollar el método efectivo de acceso a un sistema vulnerado o por la acción irresponsable de *insiders* como en el caso de los empleados deshonestos que por fuera de lo acordado con sus empleadores acceden a activos informáticos con el fin de modificarlos, alterarlos o sustraer información que luego entregan a las organizaciones del cibercrimen con fines de monetización o utilización en escenarios posteriores de ciber fraude.

Las principales ciudades del país; siguen siendo las de mayor incidencia del fenómeno del cibercrimen pues en su orden Bogotá, Medellín, Barranquilla, Cali y Bucaramanga concentran más del 70% de las denuncias instauradas durante el primer semestre del 2022, aspecto asociado a la penetración de internet, número de usuarios en plataformas de e-commerce y banca virtual.

Lo anterior claramente denota la necesidad de seguir adoptando mecanismos que faciliten la sensibilización de los usuarios a través de ciber academia, socialización de los riesgos y la participación de todos los roles de las organizaciones en los procesos de formación y capacitación en materia de ciberseguridad empresarial.

[3] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

04

04

04

04

CIBERAMENAZAS A DISPOSITIVOS MÓVILES 2022

Escrito por: CR (RA) Fredy Bautista García

El uso permanente de las tecnologías móviles ha concentrado la atención de los ciberdelincuentes y las ha convertido en objetivos principales de las ciber amenazas en el presente año, destacándose primordialmente el impacto del código dañino para plataformas móviles como un riesgo y una amenaza real de impacto a usuarios personales y empresas en Colombia.

Entre las principales tendencias detectadas por SAFE (C2USER)[1] para 2022 se destacan las siguientes:

El malware para móvil continúa evolucionando y añadiendo técnicas que le permiten evadir los antivirus siendo el principal método de infección las descargas de apps en tiendas y mercados no autorizados.

El Smishing como vector de ataque seguirá creciendo, se han identificado víctimas que reciben un SMS con un enlace a la aplicación. Este enlace luego es utilizado para descargar un troyano. Otro método de distribución son las falsas ventanas emergentes a través de las cuales se descarga e instala por ejemplo el malware TeaBot[2].

Las características principales de los programas maliciosos detectados establecen que los mismos disponen de capacidades para obtener permisos de “root” y así obtener funcionalidades de keylogger mediante la instalación de otras apps.

Se ha evidenciado igualmente el uso de herramientas de acceso remoto (RAT, por sus siglas en inglés – Remote Access Trojan) que permiten al delincuente tomar el control administrativo del dispositivo e interceptar las credenciales de las aplicaciones bancarias o incluso las contraseñas de un solo uso (OTP, por sus siglas en inglés – One Time Password).

Nuevas variantes de malware utilizan aplicaciones de mensajería para su distribución teniendo inclusive la capacidad de acceder a los dispositivos y obtener información personal de los usuarios incluyendo sus credenciales.

Existen otros vectores de dispersión de infección que han sido identificados a través de documentos de Word, Excel y PDF mediante mensajes que parecen provenir aparentemente de fuentes legítimas.

[1] https://c2usercisoslab.com/quienes-somos/

[2] TeaBot es un malware dirigido principalmente a aplicaciones bancarias y de criptomonedas, aunque también recopila información de otras aplicaciones instaladas.

Recomendaciones

La pantalla de bloqueo es el principal mecanismo de defensa frente al acceso físico no autorizado al dispositivo móvil por parte de un potencial atacante.

Los dispositivos móviles modernos resultan muy atractivos para su sustracción o robo debido tanto a su valor económico (del propio hardware), como al valor asociado a la información sensible y personal que almacenan. Se recomienda limitar la funcionalidad disponible en la pantalla de bloqueo para un tercero que no conoce el código de acceso.

Código de acceso o huella dactilar digital

Se recomienda proteger el dispositivo móvil mediante un código de acceso asociado a la pantalla de bloqueo. Aunque este código será solicitado al usuario en múltiples ocasiones a lo largo del día, es necesario seleccionar un código de acceso robusto, de al menos seis (6) u ocho (8) dígitos, y preferiblemente combinando letras y números.

Comunicaciones a través de USB

Se recomienda no conectar el dispositivo móvil a puertos USB desconocidos y no aceptar ninguna relación de confianza a través de USB si no se tiene constancia de estar conectando el dispositivo móvil a un ordenador de confianza.

Para evitar la instalación de apps a través de USB, se recomienda (en función de la plataforma móvil) no habilitar las capacidades de depuración mediante USB del dispositivo móvil, disponibles específicamente para los desarrolladores de apps, y no dejar el dispositivo móvil desatendido sin bloquear.

Actualización del sistema operativo y de las aplicaciones

Se recomienda disponer de un sistema operativo siempre actualizado en el dispositivo móvil. Asimismo, se recomienda disponer siempre de la última actualización de todas las apps instaladas en el dispositivo móvil.

Cifrado del dispositivo móvil

Se recomienda hacer uso de las capacidades nativas de cifrado del dispositivo móvil, con el objetivo de proteger todos los datos e información asociadas al usuario u organización almacenados en el mismo.

Recuerde Siempre:

Utilice contraseñas seguras

Mantenga su software actualizado

Deshabilite la conectividad remota

Proteja su dispositivo móvil

Conozca sus aplicaciones

1

Utilice contraseñas seguras: use diferentes contraseñas para diferentes programas y dispositivos No elija opciones que permitan que su dispositivo recuerde sus contraseñas.

2

Mantenga el software actualizado. Instale actualizaciones para aplicaciones y el sistema operativo de su dispositivo tan pronto como estén disponibles.

3

Deshabilite la conectividad remota. Algunos dispositivos móviles están equipados con conexión inalámbrica y tecnologías como Bluetooth, que pueden conectarse a otros dispositivos. Deshabilite estas características cuando no están en uso.

4

Proteja su dispositivo móvil. Para evitar robos y accesos no autorizados, nunca deje su dispositivo móvil desatendido en un lugar público y bloquee su dispositivo cuando no esté en uso.

5

Conozca sus aplicaciones. Asegúrese de revisar y comprender los detalles de una aplicación antes descargarlo e instalarlo. Tenga en cuenta que las aplicaciones pueden solicitar acceso a su ubicación e información personal. Elimine cualquier aplicación que no use regularmente para aumentar su seguridad.

05
05
05
05

ASEGURANDO LAS NUBES PÚBLICAS

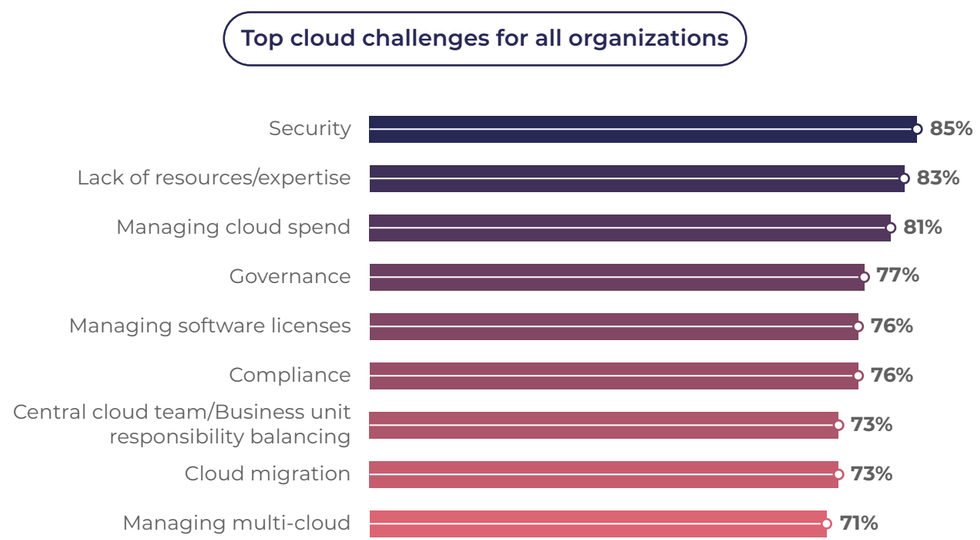
Escrito por: Carlos Robledo - BDM seguridad en la nube
de Fortinet Colombia y Ecuador

FORTINET

Actualmente para todos los participantes de la industria de tecnología, no es ningún secreto los grandes beneficios que las nubes públicas entregan a las organizaciones, sin importar la industria. Disponibilidad, Flexibilidad y Escalabilidad han probado ser los componentes de esa navaja suiza, que sirven para transformar prácticamente cada rincón de las empresas.

No obstante, cada organización tiene una jornada distinta y es importante reconocer, con absoluta claridad, los retos que debemos sortear en el corto y mediano plazo, cuando nos comprometemos con ese caso de negocio que reposa tras bambalinas de una jornada de **nube pública. Años atrás, cuando aún no había muchos casos de éxito (o fracaso) a la hora de adoptar la nube pública**, solían existir esos acalorados debates sobre qué es más importante, si construir un nuevo plan de gobierno, garantizar cumplimiento, seguridad o gestionar los gastos. Por fortuna, a hoy ya existen reportes, como el de nube pública de Flexera, donde se documenta claramente la priorización que las organizaciones vienen definiendo a la hora de adoptar la nube.

Y es por eso que se ha convertido en una estrategia prioritaria en las organizaciones, como lo demuestra la gráfica inferior.



Gráfica 1: *Reporte Flexera 2022 – Pareto de retos para la adopción de nube pública.*

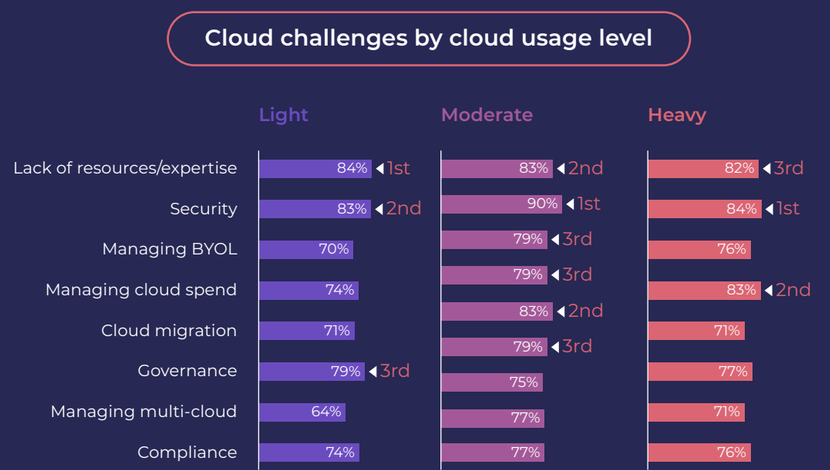
¿Interesante?

La gran mayoría de nosotros teníamos razón; todos los elementos son extremadamente importantes, no obstante, nos pusimos de acuerdo con que la seguridad va primero.

Va primero porque es ese elemento transversal a una jornada de adopción que realmente abona madurez al resto de los retos. Si definimos claramente una estrategia de ciberseguridad estaremos minimizando los problemas de cumplimiento, facilitando el entendimiento del nuevo gobierno, minimizando riesgos de consumos excesivos por brechas de seguridad y por supuesto, agregando conocimiento que nos permita aumentar nuestra experticia en nube pública.

Lo curioso de esta priorización por la seguridad es que, para el caso de Colombia, no es tanto por un acuerdo sino porque en muchos casos las empresas han sido víctimas de ciber-atacantes que encuentran a las organizaciones en la mitad de una jornada de adopción de nube como un momento ideal para hacer de las suyas.

No obstante, no deja de ser una gran victoria en contra de los ciber-criminales, la priorización de los retos en torno a la madurez en el uso de las nubes públicas, como se puede detallar en el reporte de Flexera.



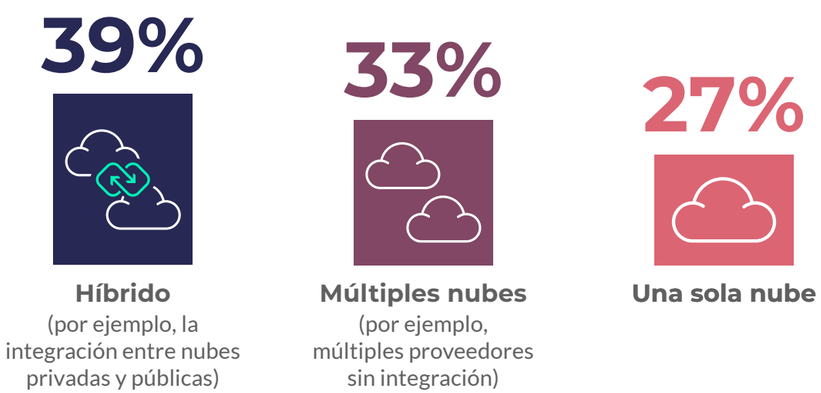
Gráfica 2: *Reporte Flexera 2022 – Priorización de retos versus madurez de adopción de nube pública*

Muchas veces se considera el total de los centros de datos para realizar el caso de negocio para adoptar una nube pública; lo cual no es sorpresa, porque no aprovecharíamos todo lo que estos nos ofrecen.

El problema detrás es que en muchas ocasiones es imposible migrar todo nuestro inventario de tecnología (especialmente en empresas de tamaño medio y grande) pues tenemos aplicaciones críticas que se caracterizan por ser antiguas (legacy) e incompatible con las nubes.

Algunas de estas se pueden migrar, pero otras que se crearon hace varios años son parte del común ejemplo de "si funciona no se deben tocar", y por más caso de negocio que exista, terminan quedando por fuera, con los riesgos que generan.

Por esta razón, la mayoría de las organizaciones terminan configurando en su organización la famosa arquitectura híbrida, que más que una decisión es realmente su única opción. Abajo una gráfica que nos indica la distribución de las arquitecturas.



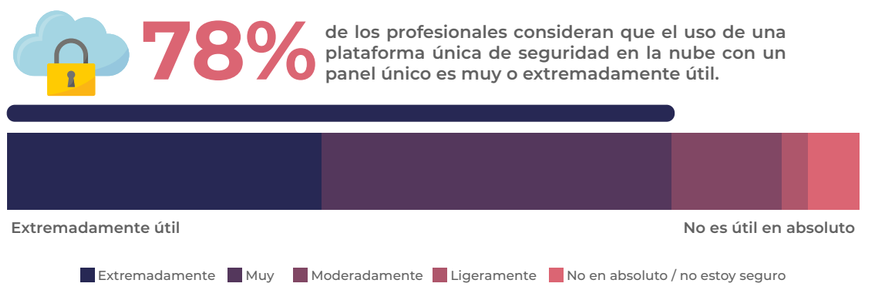
Gráfica 3: *Reporte de Ciberseguridad Fortinet 2022 – Arquitecturas organizacionales*

Este gráfico nos indica algo adicional, y es que como si no fuera suficiente reto adoptar una nube pública, increíblemente las organizaciones se han esforzado (por increíble que parezca) en mantener la política de "los huevos en distintas canastas" y comenzamos a construir no solo arquitecturas híbridas, sino también con el apellido de híbridas multi-nube.

Lo anterior tiene varios argumentos, algunos válidos, otros del siglo pasado, sin embargo, exacerba un elemento en específico y llama la atención del enemigo número 1 de la ciberseguridad: la complejidad.

Lo veíamos atrás, el segundo gran reto de las empresas es adoptar una nube sin tener el suficiente conocimiento y con recursos sin experiencia real; es decir, no olvidemos que incluso crear una máquina virtual es distinto en cada nube pública y diferente entre ellas; nuestro perímetro está tremendamente difuminado y cada paso en la adopción es una posible brecha de ciberseguridad.

¿Cómo hacemos para lidiar con esto? Pues la respuesta hoy la dan las mismas empresas, y es justamente adoptando la mayor cantidad de elementos multi-nube posibles, para devolver la uniformidad de distintos elementos, sin importar cuántas nubes queramos adoptar. Abajo una gráfica del reporte de ciberseguridad de Fortinet 2022 que nos permite evidenciar sobre esta tendencia.



Gráfica 4: *Reporte de Ciberseguridad Fortinet 2022 – Solución de seguridad multi-nube*

Así las cosas, es claro que adoptar una estrategia de seguridad multi-nube es hoy tendencia para la mayoría de las empresas, y es esta precisamente, la propuesta que Fortinet pone sobre la mesa para sus clientes minimizando la curva de aprendizaje en su dimensión de ciberseguridad.

El tiempo de nuestras organizaciones de tecnología deben ser realmente invertidos en lograr esa disponibilidad, flexibilidad y escalabilidad teniendo presente que con Fortinet agregamos ese gran elemento de tranquilidad.

Su nube no se cuida sola, necesita de tecnologías de vanguardia que le permitan no solamente disfrutar del rendimiento y ahorro que la nube le entrega, sino también de las ventajas que le genera enfocarse en el negocio, mientras nosotros en Fortinet protegemos su nube.

En conclusión, ¡A la nube, por supuesto que sí; y si es cibersegura, mucho mejor!

PROTECCIÓN DEL ACTIVE DIRECTORY

FRENTE A ATAQUES ACTUALES: REDUCIR RIESGOS PARA LA SEGURIDAD AD

CROWDSTRIKE

Uno de los principales objetivos de ciberseguridad en las organizaciones es reducir la superficie de ataque y los costes de seguridad.

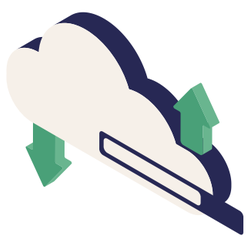
En todas las organizaciones se presentan retos en la seguridad de la red que hacen más difícil cada día encontrar una protección efectiva, factores como el incremento de tráfico de internet, la proliferación de dispositivos conectados, el aumento de usuarios con modelos de teletrabajo y una mayor sofisticación de los ciberdelincuentes dificulta la seguridad de la red.

Esto genera problemas como la sofisticación de ataques cibernéticos, amenazas contra la cadena de suministro, usurpación de las cuentas, compromiso de las credenciales cuya autentificación depende de AD, ataques de ransomware que actualmente esta es la táctica de ataque más lucrativa, vulneración de credenciales; así como el aumento de las primas de ciberseguros que van del **10%** al **30%** durante la segunda mitad del 2020 y la reducción de límites de cobertura más concretamente en sectores de alto riesgo como la sanidad. La seguridad tradicional del AD es incapaz de frenar los ataques actuales.

Las organizaciones requieren controles que puedan reducir rápidamente la superficie de ataque y mejorar la probabilidad de seguir funcionando durante y después de los ataques.

El objetivo de las validaciones técnicas de Enterprise Strategy Group (ESG) es informar a los profesionales de TI sobre las soluciones de tecnología de la información para empresas de cualquier tipo y tamaño.

Según las investigaciones de ESG, un **85%** de las empresas reconoce que la seguridad de la red ahora es más difícil que hace dos años.



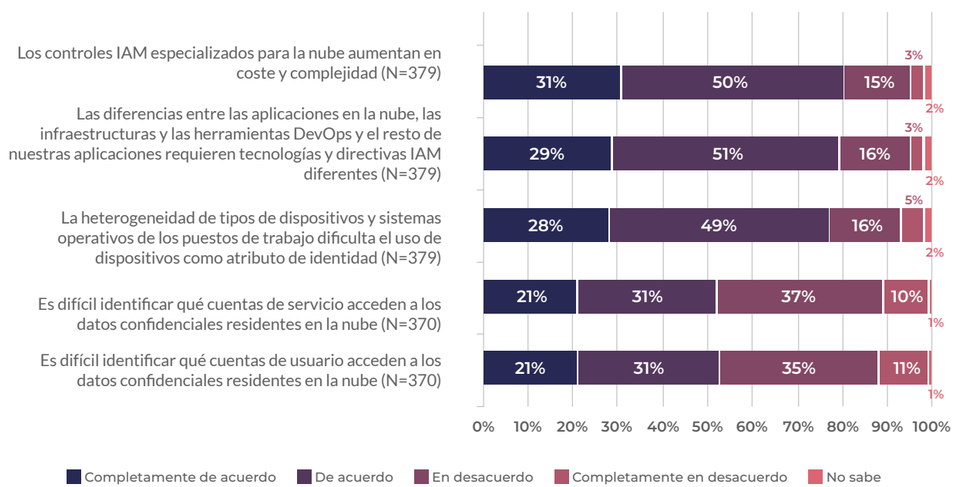
Detección y prevención de amenazas

Los controles especializados de administración de identidades y accesos (IAM) en la nube aumentan el coste y la complejidad, mientras que las aplicaciones en la nube, las infraestructuras locales modernas y las herramientas DevOps requieren diferentes tecnologías y directivas del IAM.

Sin embargo, en Active Directory los privilegios están ocultos detrás de grupos anidados, privilegios personalizados para cada usuario o entidad y otras técnicas, por lo que se hace extremadamente difícil identificar a los usuarios con privilegios excesivos o insuficientes.

La heterogeneidad de los dispositivos y la nube complica la administración de identidades

Responda a cada una de estas afirmaciones generales sobre IAM, según el uso que hace su organización de los servicios en la nube (porcentaje de encuestados).



Esto quiere decir que cada vez es más difícil detectar un robo de identidad

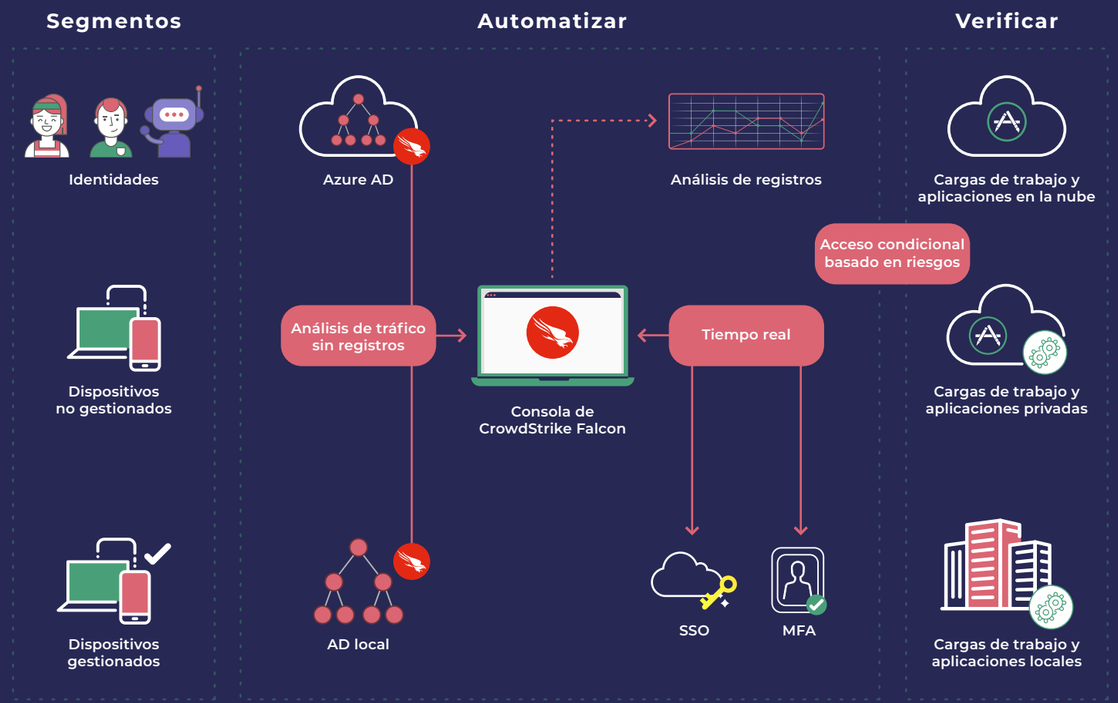
De acuerdo con investigación publicada por Forrester Research el año pasado el **80%** de los incidentes sobre datos tiene una conexión con credenciales privilegiadas comprometidas.

Es esencial que proteja su AD lo antes posible.

Una solución de protección de identidad efectiva debe permitir a la organización:

- Mejorar la higiene de AD con visibilidad continua y unificada, con controles de seguridad de las identidades en AD/Azure AD, SSO y los servicios de federación en configuraciones híbridas.
- Detectar y responder automáticamente a los ataques contra AD en directo.
- Acelerar la detección de incidentes con segmentación basada en la identidad: clasificación automática de todas las cuentas -humanas, de servicios y con privilegios- para responder a preguntas sobre quién, dónde, cuándo y por qué.
- Determinar y corregir las lagunas de seguridad en cuentas con privilegios y patrones de autenticación mediante la evaluación continua de los riesgos asociados a usuarios y dispositivos.
- Implementar acceso condicional fluido y autenticación multifactor basada en el riesgo (MFA) incluso en herramientas y aplicaciones antiguas.
- Conseguir visibilidad detallada y control de la seguridad sobre protocolos cifrados, como NTLM y LDAP/S.
- Reducir el ruido mediante la correlación de ataques más fiable del sector y mejorar el tiempo medio de detección y neutralización de las amenazas como el ransomware y los ataques contra la cadena de suministro.

CrowdStrike Falcon Identity Protection



Fuente: *Enterprise Strategy Group*

CrowdStrike Falcon Identity Protection permite un despliegue fácil y una rentabilización más rápida

ESG (Enterprise Strategy Group) validó funciones de CrowdStrike Falcon Identity Protection con una serie de sesiones de demostración, su objetivo era revelar el valor inmediato que obtienen los clientes a las pocas horas de instalar Falcon Identity Protection. **(ver reporte completo ESG).**

Algunas recomendaciones para una protección de identidad efectiva son:

- Analice en tiempo real el tráfico de autenticación en los sistemas para detectar comportamientos anómalos, esto puede ser la clave de la identificación a ataques de ransomware por medio de rutas anormales de acceso a través del uso de credenciales válidas.
- Identifique en tiempo real los accesos válidos que un usuario hace desde dispositivos que nunca se han realizado previamente, esto puede mostrar situaciones de movimientos laterales maliciosos.
- Analice los accesos remotos como RDP hacia sistemas críticos como el directorio activo e identificar si es por medio de una cuenta de servicio o un usuario “humano”, y así detener accesos maliciosos sistematizados.
- Realice el análisis y clasificación de las cuentas de servicio y cuentas de usuarios para poder detectar un mal uso o exceso de privilegios para las actividades que no lo requieran.
- Realice el análisis en tiempo real del tráfico de autenticación para identificar y prevenir ataques como: “Pass the hash “, Golden Ticket, exfiltración de credenciales de directorio, entre otros.

Referencias

1. https://adenunciar.policia.gov.co/Adenunciar/Login.aspx?ReturnUrl=%2fadenunciar%2f

2. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

3. https://c2usercisoslab.com/quienes-somos/

4. CrowdStrike. 2021. Reducción de Riesgos con CrowdStrike Falcon Identity Protection. https://www.crowdstrike.com/resources/white-papers/falcon-identity-protection-esg-technical-validation/


CCIT
tictac
SAFE
SEGURIDAD APLICADA AL FORTALECIMIENTO EMPRESARIAL