IA PARA LA PROTECCIÓN Y PREVENCIÓN DE AMENAZAS

INFORME ANUAL DE CIBERSEGURIDAD

CCIT tictac SAFE
SEGURIDAD APLICADA AL FORTALECIMIENTO EMPRESARIAL

Equipo TicTac

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

Colaboradores:
CrowdStrike
Fortinet
Huawei
Centro Cibernetico de la policia

Diseño y diagramación:
Luisa Fernanda Blanco

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.

IA PARA LA PROTECCIÓN Y PREVENCIÓN DE AMENAZAS

INFORME ANUAL DE CIBERSEGURIDAD

CROWDSTRIKE FORTINET HUAWEI

Contenido

01

PRÓLOGO

Alberto Samuel Yohai
Presidente Ejecutivo CCIT

Abordar la ciberseguridad en búsqueda de proteger la información de una compañía es una tarea que requiere no solo de un equipo humano y especializado en la materia, sino también de la tecnología, la cual ha ofrecido un abanico de posibilidades que se convirtieron en el apoyo ideal para adelantarse y atender las posibles brechas de seguridad.

Según un estudio realizado por MinTIC, cerca del 28% de las empresas en el país han adoptado sistemas de ciberseguridad basados en tecnologías maduras, en este caso el 1.8% ha aprovechado la inteligencia artificial.

Otros estudios han demostrado que en la región profesionales de TI han podido desplegar la Inteligencia Artificial en un 44% para la detección de seguridad y amenazas, lo que demuestra que la tecnología seguirá siendo un aliado ideal para estar un paso delante de los ciberatacantes.

En esta oportunidad, el programa SAFE, del Tanque de Análisis y Creatividad de las TIC (TicTac) y sus aliados, han enfocado este estudio en la Inteligencia Artificial, una tecnología que está siendo usada para detectar con antelación posibles intrusiones y así mismo permitiendo que los ingenieros de TI tomen decisiones con mayor precisión.

Los invitamos a que conozcan las diferentes posibilidades que nos brinda esta tecnología y que hoy día es la mano derecha de los equipos de seguridad de la información de un gran número de compañías en el país.

02

INTRODUCCIÓN

Tres años después del inicio de la pandemia por Covid-19 empezamos a dar prioridad a la ciberseguridad. Ahora, este tema cobra mayor relevancia en las empresas, ya que deben adecuar, actualizar e implementar herramientas tecnológicas que permitan mantener las operaciones activas de manera más responsable, pensando no solo en la operatividad y continuidad del negocio, sino también en los riesgos que la digitalización trae consigo.

Los ciberdelincuentes son cada vez más sofisticados y estratégicos y las empresas deben ir un paso delante de ellos; el uso de analítica de datos y ahora de la Inteligencia artificial (IA) han sido fundamentales para hacer frente a los posibles ataques cibernéticos.

La IA, al ser una tecnología que aprende constantemente y se adapta fácil a los patrones que va adoptando, ha logrado impactar de forma positiva las áreas de la ciberseguridad, ya que se ha demostrado que detecta con precisión las amenazas, y puede ir un paso adelante a través del análisis e investigación de ataques comunes, convirtiéndose así en una ventaja, ya que si bien los equipos de seguridad o TI trabajan continuamente por proteger la información esta herramienta ayuda a optimizar las tareas realizadas por el equipo humano.

Actualmente, los sistemas de Inteligencia Artificial se han encargado de categorizar con exactitud los ataques tipo malware, además, detectan con antelación otras posibles amenazas. Esto, con el propósito de proporcionar la estrategia adecuada para evitar pérdidas de información.

En este estudio, abordaremos la Inteligencia Artificial y sus diferentes maneras de aplicarla al uso adecuado de la ciberseguridad. A través de nuestros aliados enfocaremos nuestros esfuerzos en mostrar las posibilidades que la tecnología nos entrega y la forma adecuada de ponerla al servicio de las compañías y sus colaboradores.

03

COMPORTAMIENTO DE LAS CIFRAS DEL CIBERDELITO

2021 - 2023

Escrito por:
CR (RA) Fredy Bautista García
AB. Experto cibercrimen Daniel Aguilar

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

En los últimos 10 años, el número de casos registrados anualmente en el sistema de denuncias de la Fiscalía General de la Nación creció más de 60.000 casos. En 2013, cuando se empezaron a conocer los primeros casos de Ransomware[1] en Colombia y se adelantaban las campañas de sensibilización para enfrentar el creciente problema de SpearPhishing[2], se conocieron 3.380 registros, una década después los registros señalan un consolidado de 65.794.

El 2022 se convirtió en el segundo año con mayor incremento en las cifras del Ciberdelito con una diferencia de 14.000 casos respecto a 2021, únicamente superado por el 2020, año de la pandemia del COVID19, cuando el incremento anual registró más de 22.000 casos en comparación con el 2019 que equivalen a cerca del 109% de variación porcentual.

Gráfica No.1 Evolución 2009-2022 Denuncias Ciberdelitos

[1] Ransomware genéricamente se refiere a cualquier tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.

[1] SpearPhishing refiere a la evolución del engaño clásico del correo electrónico que incorpora procesos de ingeniería social e información personalizada de la víctima, aspecto que incrementa la ventana de éxito del atacante.

Este análisis permite señalar que, efectivamente el porcentaje de incremento de los ciberdelitos viene creciendo de manera significativa, cada año, y que el comportamiento de estabilidad al alza tuvo un punto de inflexión en 2019, particularmente atribuible a un escenario en el que confluyen múltiples factores; entre los que destacamos los siguientes:

1. Incidencia del factor geopolítico en el contexto global. Los grupos de amenazas como los el APT C36[3] han sido más activos en los últimos años en Colombia.

2. Incremento en el número de servicios de comercio electrónico y servicios de banca digital. El sector Fintech en Latinoamérica indica que las Billeteras virtuales vienen creciendo un 27% cada año, tendencia que será duplicada para el 2025; todo lo anterior aumenta el nivel de exposición y apetito de los ciber atacantes.

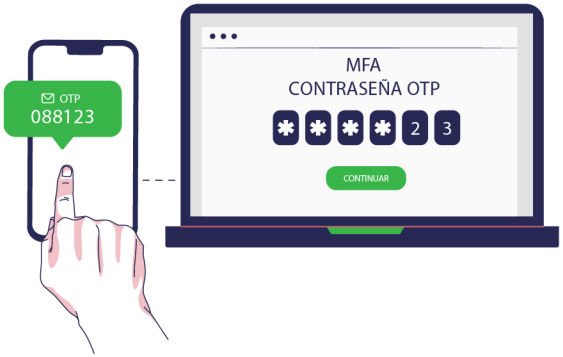
3. Concienciación y sensibilización insuficientes como herramienta de detección temprana y prevención de ataques en fases iniciales.

4. Percepción de la ciberseguridad como un gasto elevado en la operación de las Empresas en Colombia.

5. Desactualización de los sistemas y del recurso humano por fuga de talentos de Ciberseguridad. Alta rotación y poca claridad en la designación de los responsables en la estructura organizacional.

[3] APT-C-36 es un presunto grupo de espionaje de América del Sur que ha estado activo desde al menos 2018. El grupo se dirige principalmente a instituciones gubernamentales colombianas, así como a importantes corporaciones en el sector financiero, la industria petrolera y la fabricación profesional. Fuente : https://attack.mitre.org/groups/G0099/

Cifras del Ciberdelito en 2022



Durante el **2022**, las denuncias en Colombia por Ciberdelitos crecieron un 26%, cada 8 minutos se registró una nueva denuncia en nuestro País, por infracciones a la ley 1273/2009, siendo el hurto por medios informáticos el delito con mayor número de registros: un total de 25.413 equivalente a un 34% más que en el 2021.

El hurto por medios informáticos incluye diversas modalidades que tienen como finalidad el apoderamiento de un activo, a través de una manipulación informática o comprometiendo generalmente credenciales de acceso a sistemas informáticos que la experiencia señala vinculadas a sistemas bancarios.

El segundo tipo penal más denunciado es el acceso abusivo a sistema informático (13.318 casos), que sanciona todas las conductas asociadas a la intrusión informática; el registro en cifras de la Fiscalía General de la Nación obedece en gran parte a la cualificación del tipo que hacen los analistas que identifican en el ingreso abusivo a un sistema la fase inicial de un ciberataque.

Comparativamente con el 2021 (8.208 casos) **el delito aumentó un 62%.**

El tercer delito más denunciado sigue siendo la Violación de datos personales con un total de **12.775** hechos registrados, un 3% más respecto al 2021, cuando fueron informados los 12.419; las modalidades asociadas corresponden generalmente a **suplantaciones de identidad, robos de identidad y fuga de datos**, incluida la venta de datos en los mercados de la internet profunda.

El cuarto delito con mayor número de noticias criminales en Colombia sanciona la suplantación de sitios Web, tipo penal asociado a modalidades como SpearPhishing, Phishing y Pharming. Las cifras indican un incremento 4% al revisar comparativamente los registros del 2021 (12.419) frente al 2022 (12.775).

Los datos analizados indican igualmente que el delito que porcentualmente más creció en Colombia es la interceptación de datos informáticos; las cifras del 2021 (1.331) frente al 2022 (1.927) indican un **aumento del 45%**. Estos registros pueden estar relacionados con los casos de ciber espionaje empresarial y otras afectaciones a la información confidencial.

En su orden, las ciudades con mayor afectación son:

Estas ciudades representan un 65% del total de casos presentados. Los casos se presentan particularmente en las principales ciudades con relación a la densidad poblacional e índice de uso de tecnologías y penetración de Internet.

Sectores más afectados

Los sectores **industriales, gobierno, educación y salud,** fueron los más comprometidos en ataques durante el 2022, un 67% del total de denuncias se registran por parte de empresas y entidades del sector público y privado. La anterior cifra señala un proceso de madurez en las organizaciones respecto al deber de denuncia.

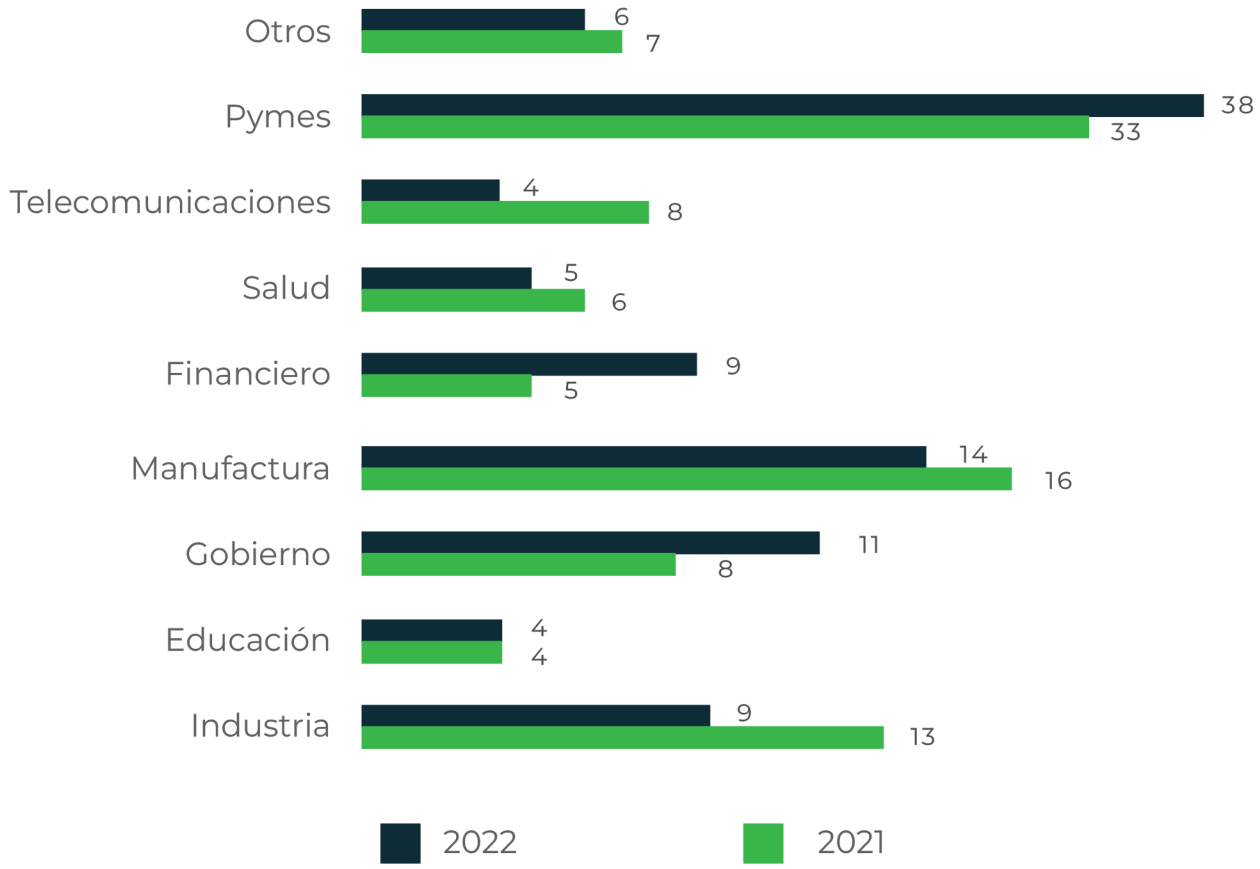
Las pequeñas y medianas industrias (Sector PYME) siguen siendo el sector más afectado por los ciberataques en Colombia. Esto, obedece principalmente a las débiles estrategias de ciberseguridad implantadas por los responsables de estas organizaciones, bien sea, porque no se identifica dentro de la cadena productiva la necesidad de incorporar a los costos de la operación de los negocios la ciberseguridad como un factor estratégico, o por desconocimiento de las amenazas por parte de quienes realizan la gestión operativa de los negocios.

Las estadísticas más optimistas señalan que solo el 7% de las pymes que sufren un ciberataque en el primer año de trabajo subsisten y pueden continuar; en la mayoría de los casos deben cerrar, pues las pérdidas ocasionadas por los atacantes superan ampliamente el capital de inversión inicial hoy considerado para el funcionamiento de estas organizaciones.

En 2022 fue llamativo el incremento del número de casos de fuga de datos en entidades del Gobierno, es muy importante que se sigan fortaleciendo las capacidades de detección temprana y procesos post incidente que permitan detectar y reaccionar oportunamente a las fugas de información para disminuir la ventana de tiempo de exposición de los datos comprometidos.

La creación de una agencia nacional de ciberseguridad podría ser la solución para unificar y fortalecer las capacidades técnicas y humanas para enfrentar la problemática del ciberdelito pero también para poder propiciar la generación de políticas aplicables que involucren a la Academia y al clúster de empresas de ciberseguridad y expertos, así como a la sociedad civil como partes activas en una estrategia nacional de ciberseguridad.

Sectores más afectados 2021-2022



El balance del Cibercrimen 2021-2022 refleja la gravedad del problema del ciberdelito en Colombia y la necesidad de fortalecer la ciberseguridad en todos los sectores. Es importante que las empresas, gobiernos y ciudadanos tomen medidas para protegerse de estos delitos, como la implementación de medidas de seguridad informática, la educación sobre los riesgos y amenazas del ciberespacio, y la cooperación con las autoridades para denunciar y perseguir a los delincuentes.

ANÁLISIS PROSPECTIVO DE LAS AMENAZAS A LA CIBERSEGURIDAD EN 2023

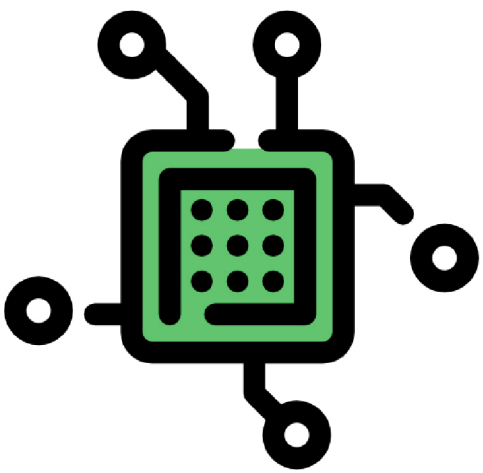
Redactado por:
CR. Fredy Bautista y Daniel Aguilar

En la actualidad, la ciberseguridad es uno de los temas más importantes en el mundo digital, y se ha convertido en una prioridad para las empresas y organizaciones de todos los tamaños. Cada año, surgen nuevas amenazas y desafíos en este ámbito, y es vital estar al tanto de las tendencias y los riesgos potenciales para proteger adecuadamente nuestros sistemas y datos.

En este sentido, es necesario analizar de forma prospectiva las amenazas de ciberseguridad que se esperan para el año 2023 en Colombia y en el mundo, con base en información estadística de las principales agencias de ciberseguridad.

1. Inteligencia Artificial y Ciberseguridad

La inteligencia artificial (IA) es una tecnología que está transformando el mundo de la ciberseguridad. Esta disciplina se está adaptando a las nuevas amenazas de seguridad y al aumento constante de los ataques cibernéticos. La IA se ha convertido en un pilar fundamental en la defensa contra el cibercrimen, permitiendo la protección y prevención de amenazas a través de la identificación temprana de actividades sospechosas.



Según un informe del Banco Interamericano de Desarrollo (BID), el costo anual de los ciberataques en Latinoamérica y el Caribe podría superar los US$ 90 mil millones en 2025, con un promedio de más de 18.5 millones de ataques cada año. Estos datos reflejan la importancia de contar con tecnologías como la IA para proteger y prevenir el cibercrimen en la región y en todo el mundo.

En este sentido, la IA tiene el potencial de detectar amenazas de seguridad antes de que causen daño, al tiempo que reduce el tiempo de respuesta y los costos asociados a los incidentes de ciberseguridad. La IA también puede proporcionar una visión holística del estado de la seguridad de una organización, identificando vulnerabilidades en su infraestructura y desarrollando estrategias de prevención.

No obstante, la implementación de la IA para la ciberseguridad plantea desafíos importantes. Uno de los principales desafíos es el aumento del volumen de datos que se deben analizar, lo que puede generar falsos positivos y dificultar la identificación de amenazas reales. Además, la falta de talento especializado en IA puede retrasar su adopción, especialmente en países como Colombia en los cuales la brecha digital sigue vigente.

A pesar de estos desafíos, la IA está transformando la forma en que se aborda la ciberseguridad en todo el mundo. Según un estudio de Gartner, para el año 2025, el 50% de las organizaciones de todo el mundo utilizarán la IA para la prevención de amenazas y la respuesta a incidentes. Además, el informe destaca que la IA se está utilizando cada vez más para identificar patrones de comportamiento y amenazas emergentes, lo que permitirá a las organizaciones anticiparse a futuros ataques.

Es necesario destacar que la IA no es una solución mágica para la ciberseguridad. Su adopción debe ser complementaria a otras tecnologías y prácticas de seguridad, y debe ser implementada de manera responsable y ética. Además, es fundamental que los gobiernos y las organizaciones trabajen juntos para fomentar la investigación y el desarrollo de la IA en ciberseguridad y garantizar que se utilice para proteger a la sociedad en lugar de perjudicarla.

A medida que aumenta la frecuencia y la sofisticación de los ataques cibernéticos, la IA puede proporcionar una ventaja crítica al identificar amenazas de seguridad en tiempo real. Aunque todavía existen desafíos importantes en su implementación, la adopción responsable de la IA puede ser una estrategia valiosa para mejorar la ciberseguridad y proteger a la sociedad.

La IA es capaz de procesar grandes cantidades de datos y de detectar patrones en tiempo real, lo que permite a las empresas identificar y prevenir amenazas de forma más rápida y eficiente. La IA también puede detectar patrones de comportamiento sospechosos en los usuarios, lo que permite a las empresas identificar y prevenir amenazas internas antes de que se conviertan en problemas.

La IA también puede ser utilizada para detectar y prevenir el phishing y otros tipos de ataques de ingeniería social. Los sistemas de IA pueden analizar correos electrónicos y otros mensajes para detectar posibles amenazas, como enlaces maliciosos o archivos adjuntos sospechosos.

Además, la IA también puede ser utilizada para proteger los sistemas de Internet de las cosas (IoT). Los dispositivos IoT pueden ser vulnerables a los ataques cibernéticos, pero la IA puede detectar y prevenir estos ataques mediante la identificación de patrones de comportamiento sospechosos en los dispositivos.

Aunque la IA tiene una gran cantidad de beneficios para la protección y prevención de amenazas cibernéticas, también hay algunos desafíos. Uno de los mayores desafíos es la falta de datos de entrenamiento de alta calidad. La IA necesita grandes cantidades de datos para funcionar de forma efectiva, y si los datos no son de alta calidad, la IA puede generar falsos positivos y falsos negativos.

Otro desafío es la complejidad de los sistemas de IA. La IA es un sistema complejo que requiere un alto nivel de especialización para su desarrollo y mantenimiento. Esto puede resultar costoso para muchas empresas, especialmente para las pequeñas y medianas empresas.

La IA es una herramienta valiosa para la protección y prevención de amenazas del cibercrimen y ciberseguridad. La IA puede detectar y prevenir amenazas de forma más rápida y eficiente que los sistemas tradicionales de seguridad, y puede identificar patrones de comportamiento sospechosos en los usuarios y en los dispositivos IoT.

Aunque existen algunos desafíos, como la falta de datos de entrenamiento de alta calidad y la complejidad de los sistemas de IA, la IA sigue siendo una tecnología prometedora en la lucha contra los ciberataques.

2. LEAK WARE : Ransomware y fuga de datos

En 2022, la cantidad de ataques de Ransomware en Colombia aumentó en un 122% en comparación con el año anterior, sin embargo los cibercriminales vienen utilizando técnicas complementarias que hacen trascender el escenario hacia uno de mayor complejidad.

Existe consenso por parte de la Comunidad de expertos en ciberseguridad frente a las fases de un ciberataque específicamente en la etapa de reconocimiento y es que las organizaciones del cibercrimen primero están identificando los activos de información que pueden extraer o ex filtrar de una organización con fines extorsivos para luego realizar la identificación de las herramientas que utilizan para facilitar este ataque tanto en él escaneo de vulnerabilidades como la identificación del mejor mecanismo de intrusión o de acceso y sostenimiento dentro de una red o un sistema.

Una vez ha sido sembrada la cepa del Malware que se encarga del cifrado de la información, de forma simultánea el centro de comando y control de la red de ciber atacantes; está recibiendo la notificación del volumen de datos ex filtrados de una organización, particularmente megas o gigas de información que quedan en poder de las estructuras del cibercrimen.

Durante el año 2022 Colombia fue testigo de múltiples ataques en los cuales compañías del sector de salud o instituciones del Estado vieron comprometidas públicamente su información y expuestos los datos, en algunos casos sensibles, de clientes y proveedores. Para 2023 se espera que la consolidación de esta técnica conocida como LeakWare, que no es más que la combinación de los ataques de Ransomware y la fuga de datos (Data Leaks) .

Para enfrentar este desafío la organización debe consolidar procesos internos que involucren a las áreas legales y de cumplimiento para que cuente con la capacidad de realizar la gestión para el tratamiento de los datos personales post incidente.

A pesar de los esfuerzos de la Superintendencia de Industria y Comercio de establecer un Marco de buenas prácticas[4] para el tratamiento adecuado de los datos personales que incluyen la publicación de una guía para el tratamiento de datos y la implementación de controles para prevenir la ocurrencia de incidentes de seguridad, los esfuerzos durante el 2022 fueron insuficientes puesto que crecieron los casos conocidos de publicación de datos personales en mercados ilegales, aspecto relacionado con el incremento en el número de noticias criminales conocidas por apertura de procesos penales derivados por incidentes de suplantación de identidad, robo de identidad y otras modalidades asociadas a este fenómeno.

Para minimizar el impacto en la afectación de la información comprometida de tal manera que se garanticen los derechos fundamentales y constitucionales respecto al habeas data de los usuarios; las organizaciones deben mejorar el nivel de conciencia y disponer de un oficial de Protección de Datos que hoy más o menos node vincular los conocimientos legales con la evidencia digital derivada del Ciberataque, es decir que le permita a la organización combinar las dos técnicas y garantizar a los usuarios titulares de los datos un adecuado tratamiento conforme a la legislación aplicable[5] y una mejor gestión del riesgo legal y de cumplimiento a la empresa afectada.

[4] https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf
[5] https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

3. PHISHING y DEEPFAKE: ATAQUES MÁS SOFISTICADOS

Durante el 2023 el Phishing continuará evolucionando gracias a la utilización de técnicas de inteligencia artificial que le permitirán a los atacantes trabajar particularmente sobre plantillas predispuestas de mensajes convincentes para engañar a los usuarios. Los típicos errores de ortografía tan frecuentes en los cuerpos de texto de los mensajes de engaño que envían los cibercriminales cada vez serán menos notorios y las técnicas para el ocultamiento del origen del mensaje les permitirá utilizar dominios creíbles o suplantados mediante técnicas de spoofing y de ocultamiento tanto en los enlaces hacia donde se redirecciona la navegación de los usuarios como en las cuentas de origen utilizadas para la maniobra de engaño.

Estos mensajes podrían estar acompañados de información preparada manera de deepfake es decir hoy la recopilación de imágenes de video que involucran audio con el cual hoy los cibercriminales suplantarán a los ejecutivos de una compañía para conseguir particularmente el desvío de grandes capitales de dinero mediante transacciones fraudulentas o el despacho de mercancías valiosas suplantando a clientes y proveedores en la cadena logística de las organizaciones.

En 2023 los ataques cibernéticos basados en Phishing y DeepFake podrían estar vinculados también al escenario del contexto geopolítico de la región; otro factor de interés podría ser el proceso electoral en el mes de octubre del 2023 que facilitaría la participación de actores de amenaza como lo ha sido el APTc 36 que se ha especializado en suplantar entidades como la Registraduría Nacional del Estado civil, la Fiscalía General de la Nación, la Policía Nacional y DIAN para engañar a los usuarios en Colombia y dispersar malware que compromete la información de los sistemas pero particularmente dirigido hacia entidades del Estado.

Es importante entonces que dentro del mapa de gestión de riesgos de una organización y de la caracterización de los riesgos informáticos; los fraudes de suplantación de clientes y proveedores basados en DeepFake se actualicen de tal manera que los controles duales y la implementación de reglas con clientes y proveedores sean suficientes ante este nuevo escenario de ciber estafas y ataques[6].

[6] https://www.incibe.es/protege-tu-empresa/blog/historias-reales-deepfake-mi-jefe-circulando-red

A pesar del anterior panorama el INCIBE publicó recientemente algunas medidas proactivas para mitigar los daños que podría los DeepFake pueden ocasionar a una organización, estos son:

Monitorizar las redes sociales: es muy importante llevar un control, ya no solo de las menciones a la cuenta de la empresa, sino de los hashtags o localizaciones de la empresa.

Establecer un plan de crisis: en caso de que esto suceda, es aconsejable tener preparado un plan para hacerle frente, frenarlo y reaccionar a tiempo y con contundencia.

Formar y concienciar al personal para detectar suplantaciones: sobre todo a aquellas personas que trabajan en puestos relacionados con pagos o que gestionan servicios clave para la empresa.

Tomar precauciones cuando se usen videoconferencias.

Actualizar los procedimientos de pago: de forma que todos los pagos tengan que ser autorizados por correo electrónico o de forma presencial y nunca por teléfono. Además, en caso de ser pagos mayores, que sean autorizados por más de una persona en la empresa.

Contratar un seguro: verificando que tenga cobertura ante fraudes basados en DeepFake.

PRIORIZAR LOS RIESGOS DE LA SUPERFICIE DE ATAQUE CON INTELIGENCIA DE ADVERSARIOS Y CONOCIMIENTOS IMPULSADOS POR IA

Redactado por:

CROWDSTRIKE

Los ataques cibernéticos van en aumento, especialmente entre las pequeñas y medianas empresas: un informe encontró que el 70 % de las empresas más pequeñas han sufrido un ataque. Muchas pequeñas y medianas empresas no están preparadas para el aumento de las amenazas a la seguridad. De hecho, el 45% de estos negocios reportan tener medidas de seguridad insuficientes para prevenir ataques cibernéticos. Este artículo analiza un posible punto débil: las superficies de ataque en las aplicaciones de software.

¿Cuáles son los riesgos asociados con la visibilidad limitada de la superficie de ataque?

El último informe de violación de datos de Verizon indica que el 70% de los ataques son perpetrados por actores de amenazas externos. Estos atacantes ven claramente y explotan puntos débiles en el perímetro de la red que las empresas dejan desprotegidos. Esto no es sorprendente, ya que los datos de CrowdStrike Falcon Surface (antes Reposify) muestran que, en promedio, las organizaciones desconocen el 64 % de sus activos conectados a Internet.

En 2016, Gartner predijo que para 2020, el 30 % de los ataques exitosos experimentados por las empresas se producirán en sus recursos de TI en la sombra. Nuestro análisis reciente indica que alrededor del 38 % de los ataques exitosos en 2019 fueron el resultado de TI en la sombra, configuraciones incorrectas y exposiciones desconocidas a Internet que podrían haberse evitado si las organizaciones tuvieran una mejor visibilidad de su superficie de ataque.

Superficie de ataque de una aplicación de software

Una superficie de ataque es la suma de todas las posibles exposiciones a riesgos de seguridad en el entorno de software de una organización. Dicho de otra manera, es el conjunto de todas las vulnerabilidades potenciales (conocidas y desconocidas) y controles en todos los componentes de hardware, software y red.

Las superficies de ataque se pueden clasificar en tres tipos básicos:

Superficie de ataque digital.

La superficie de ataque digital abarca todo el entorno de red y software de una organización. Puede incluir aplicaciones, código, puertos y otros puntos de entrada y salida.

Superficie de ataque físico.

Las superficies físicas de ataque incluyen todos los dispositivos de punto final de una organización: sistemas de escritorio, portátiles, dispositivos móviles y puertos USB.

Superficie de ataque de ingeniería social.

Los ataques de ingeniería social se aprovechan de las vulnerabilidades de los usuarios humanos. Los tipos más comunes de ataques contra las organizaciones incluyen el phishing selectivo, el uso de pretextos y otras técnicas de manipulación utilizadas para engañar a las personas para que proporcionen acceso a información confidencial.

Identificar la superficie de ataque de una aplicación de software requiere mapear todas las funciones que deben revisarse y probarse en busca de vulnerabilidades. Esto significa atender todos los puntos de entrada o salida en el código fuente de la aplicación.

Cuanto mayor sea la superficie de ataque de una aplicación de software, más fácil será para un atacante o pieza de malware acceder y ejecutar código en una máquina objetivo.

¿Qué es la gestión de superficie de ataque externa (EASM)?

La gestión de superficie de ataque externa (EASM) se refiere al descubrimiento, monitoreo, evaluación, priorización y reparación continuos de los vectores de ataque de la superficie de ataque externa de una organización. Una superficie de ataque externa, también conocida como superficie de ataque digital, es la suma de los activos de Internet de una organización y los vectores de ataque asociados que pueden explotarse durante un ataque.

Los activos orientados a Internet incluyen cualquier cosa, desde nombres de dominio, certificados SSL y protocolos hasta sistemas operativos, servidores, dispositivos IOT y servicios de red. Estos activos están dispersos en entornos locales, en la nube y proveedores externos y representan la forma más fácil de acceder a redes internas y datos confidenciales.

Implementación de la gestión de la superficie de ataque

La gestión de la superficie de ataque en aplicaciones de software tiene como objetivo detectar debilidades en un sistema y reducir la cantidad de vulnerabilidades explotables. El objetivo de analizar la superficie de ataque es hacer que los desarrolladores y especialistas en seguridad sean conscientes de todas las áreas de riesgo de una aplicación. La conciencia es el primer paso para encontrar formas de minimizar el riesgo.

En última instancia, las empresas pueden utilizar el análisis de la superficie de ataque para implementar lo que se conoce como seguridad Zero Trust a través de conceptos básicos como la segmentación de la red y estrategias similares.

Tenga cuidado con estas vulnerabilidades de software comunes:

Problemas de control de acceso.

A menudo, los desarrolladores de software terminan insertando reglas en múltiples ubicaciones en el código, fallas que pueden exponerse y explotarse fácilmente.

Defectos de inyección.

Las fallas de inyección incluyen llamadas al sistema operativo y llamadas a bases de datos "back-end" a través de SQL. A menudo, estos campos carecen de un filtro de entrada, lo que los hace vulnerables a los ataques.

Problemas de autenticación.

Cuando las funciones de la aplicación relacionadas con la administración de sesiones y la autenticación se implementan de manera incorrecta, los atacantes pueden obtener acceso a un sistema con los mismos permisos que los usuarios objetivo.

Problemas de entidad externa XML.

La configuración débil de los analizadores XML que procesan la entrada XML que contiene referencias a entidades externas puede generar problemas como la exposición de información confidencial y la denegación de servicio (DoS).

API personalizadas.

Las API agregan vulnerabilidad a través de autenticación de usuario rota, autorización de nivel de objeto rota, exposición excesiva de datos y otros problemas.

Formularios web.

Agregar formularios web proporciona más formas de enviar datos directamente a su servidor. Una amenaza de formulario web común son los ataques de secuencias de comandos en sitios cruzados (XSS), en los que un atacante obtiene una secuencia de comandos maliciosa para ejecutar en el navegador de un usuario.

¿Cómo ayuda una solución de gestión de superficie de ataque externo?

La gestión de la superficie de ataque externa es simplemente la única forma de descubrir, gestionar y monitorear su red sin perímetro a escala. Dado que Shadow IT es tan frecuente y los errores humanos son inevitables, la gestión de la superficie de ataque externa está ocupando un lugar central con cada vez más empresas que establecen equipos dedicados para la gestión y reducción de la superficie de ataque.

CrowdStrike Falcon® Surface identifica activos desconocidos y expuestos a Internet para que los equipos de seguridad puedan proteger mejor su perímetro digital en constante evolución. Falcon Surface les permite detectar, priorizar y administrar todos los activos expuestos a Internet que están centralizados o remotos en entornos locales y proveedores subsidiarios, en la nube y de terceros con un enfoque de cero intervención.

La tecnología inteligente de mapeo y asociación de Internet de Falcon Surface indexa continuamente todo Internet y mapea automáticamente los activos conocidos y desconocidos de las empresas, descubriendo exposiciones, riesgos y configuraciones incorrectas dentro y más allá de sus rangos de red oficiales.

Todos los activos expuestos, conocidos y desconocidos, se clasifican, analizan y priorizan automáticamente de acuerdo con la puntuación de riesgo contextualizada. Las alertas personalizables activan notificaciones para problemas que requieren atención inmediata. Falcon Surface también genera pasos de remediación accionables y de implementación rápida.

Los motores de asociación habilitados para inteligencia artificial (IA) correlacionan un activo con su fuente independientemente de la propiedad "oficial" o no, a través de múltiples identificadores como certificados, subdominios u otros medios. Además, la plataforma puede hacer coincidir una organización con su industria, un componente clave para contextualizar los riesgos de mayor prioridad para la seguridad de la red.

Para cada riesgo identificado, como las versiones de final de vida (EOL) de la aplicación, Falcon Surface genera automáticamente pasos de remediación accionables y de implementación rápida para TI y seguridad equipos para solicitar la mitigación de vulnerabilidades en tiempo real. Con su remediación quirúrgica pero clara pasos, optimiza la productividad de los equipos, aumenta la eficiencia y reduce el tiempo de exposición.

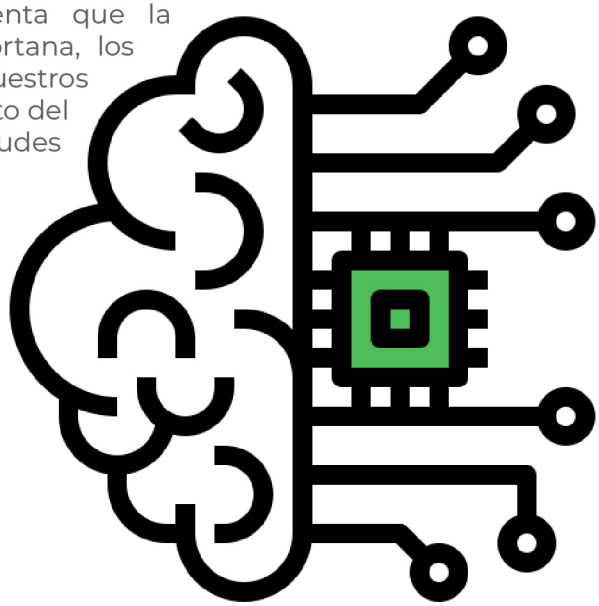
Inteligencia Artificial; que la tecnología trabaje en pro de su ciberseguridad

Redactado por:

FORTINET®

¿Cómo saber si este documento que va a leer está o no creado con ChatGPT?, aunque ya existen herramientas que permiten detectar la generación de textos con una IA (es irónico que una IA se use para detectar otra IA) será una pregunta que todos nos deberemos hacer de aquí en adelante, las herramientas de IA han llegado y puede ser un cliché pero lo hacen para quedarse, el trabajo de todos es usarlas para nuestro favor pero también considerar que se usaran para afectarnos, es una realidad a la que hay que acomodarse.

Las herramientas de inteligencia artificial ya existen hace algunos años, solo que no eran usadas por todos en todos los ámbito. Anteriormente era usadas por expertos que tenían la forma de entrenarlas y poder generar la información que requerían de acuerdo con sus necesidades, ejemplo en Fortinet nuestros laboratorios de investigación FortiGuard usan IA para el reconocimiento de malware de forma dinámica y en tiempo real. Aunque también las usábamos y probablemente algunos no habíamos caído en cuenta que la Inteligencia Artificial esta por detrás de Siri, Alexa, Cortana, los asistentes personales que todos tenemos en nuestros dispositivos y que por medio de técnicas de procesamiento del lenguaje natural pueden entender las preguntas y solicitudes de los usuarios.



Sin embargo, gracias a ChatGPT hoy ya hablamos del acceso y uso de la IA en cualquier campo o tarea y además por cualquier persona con acceso a Internet y un browser web. Esta herramienta usada de la forma adecuada permitirá mejorar la productividad de muchas de nuestras tareas del día a día, tanto laboral como personal, por ejemplo, podríamos preguntarles a los estrategas de marketing digital que usan para crear sus contenidos. La generación de texto con lenguaje natural como ChatGPT no es lo único que tenemos hoy, existen más tecnologías:

Generación de Imágenes y Vídeos
Son modelos de IA que pueden generar imágenes y videos a partir de descripciones de texto o voz. Estos sistemas utilizan técnicas de generación de adversarios y redes neuronales para crear imágenes y videos realistas. Ejemplos de generación de imágenes y videos AI son DALL-E de OpenAI y Deep Dream Generator.

Análisis de Sentimientos y Emociones
Son modelos de IA que pueden detectar emociones y sentimientos en el lenguaje humano. Estos sistemas utilizan técnicas de análisis de texto y aprendizaje automático para identificar las emociones y sentimientos expresados en un texto. Ejemplos de análisis de sentimientos y emociones AI son IBM Watson Tone Analyzer, Google Cloud Natural Language y Microsoft Azure Text Analytics.

Text-to-Speech (TTS) AI:
Son modelos de IA que pueden generar voces humanas realistas a partir de texto escrito. Estos sistemas utilizan técnicas de síntesis de voz para transformar el texto en voz hablada. Ejemplos de TTS AI son Google Cloud Text-to-Speech, Amazon Polly y Microsoft Azure Text-to-Speech.

La inteligencia artificial (IA) ha demostrado ser una herramienta valiosa en muchos campos, incluyendo la medicina, la manufactura, la educación y muchos otros. Entre las ventajas de la IA se incluyen la capacidad de automatizar tareas repetitivas, analizar grandes cantidades de datos en poco tiempo y mejorar la precisión y la eficiencia en la toma de decisiones.

Sin embargo, también hay desventajas potenciales en el uso de la IA, especialmente cuando se trata de aplicaciones malintencionadas. Por ejemplo, algunas personas pueden utilizar herramientas de IA para llevar a cabo ciberataques, lo que podría causar daños significativos a individuos y organizaciones. Además, la IA también puede ser utilizada para crear contenido falso o engañoso, como noticias falsas o imágenes manipuladas.

Herramientas de generación y análisis de texto están facilitando la vida de desarrolladores de malware, atacantes sin importar si son experimentados o nuevos y otros ciber actores, veamos un poco de esta facilidad a la cual cualquier persona tiene acceso.

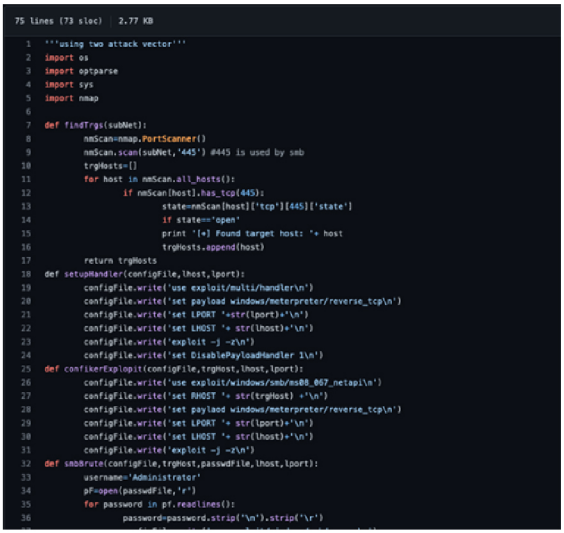


Imagen 1. Fuente: https://github.com/royari/smb-exploit/blob/master/smb-exploit.py

En la anterior imagen (imagen 1) podrán encontrar código hecho en un lenguaje de programación llamado Python, el código es utilizado para explotar vulnerabilidades en un protocolo llamado SMB, para un atacante avanzado que no sea el autor de este tomará trabajo analizarlo y probarlo, para un atacante nuevo será mucho más difícil pero no imposible usarlo, pero con mayor tiempo de análisis y pruebas que el atacante experimentado. Hoy, con tecnologías de IA como ChatGPT esto se hace más sencillo, veamos que nos puede decir ChatGPT cuando le pedimos una explicación del código como lo vemos.

Con solo pedir en lenguaje natural a ChatGPT que nos explique el código (Imagen 2), obtendremos resultados en pocos segundos (Imagen 3). Si quisiéramos seguir indagando por cómo usarlo y con que herramientas al final tendremos un ciber arsenal listo para usar, probablemente con ejemplos. ChatGPT está tratando de controlar esto, y cuando se pregunta directamente por ataques evita dar respuestas, pero aún no es tan inteligente si mi pregunta tiene un contexto por ejemplo académico.

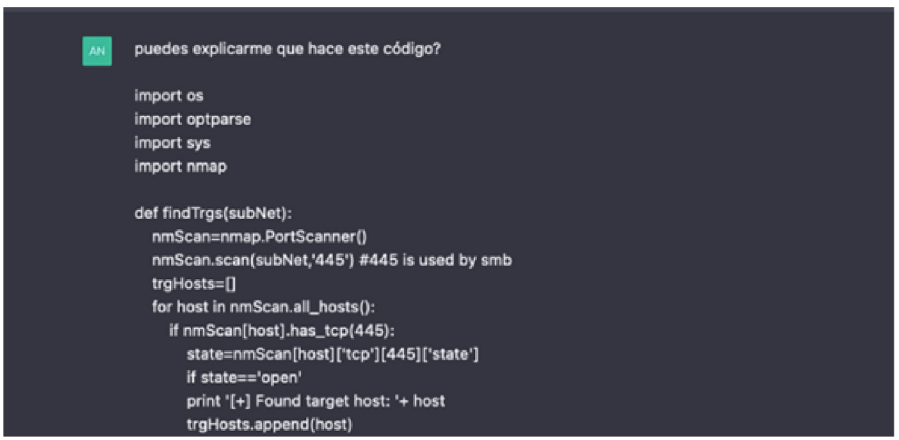


Imagen 2. Fuente: ChatGPT

Si pensamos en otras herramientas, tendremos distintos escenarios de ataques usando por ejemplo creación de voz que simula las de otras personas, comportamientos similares a las herramientas que hoy usan entidades financieras como Bots de atención al cliente, entre otras.

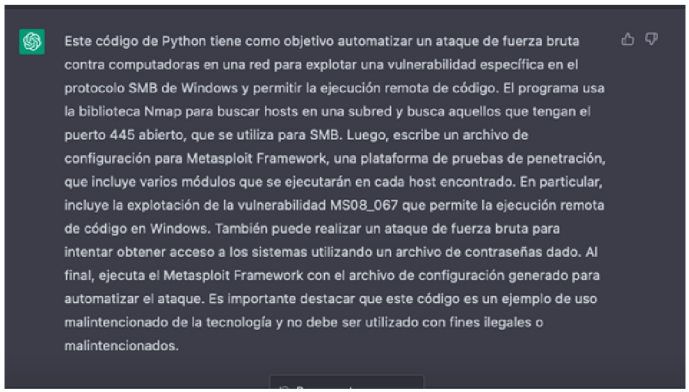


Imagen 3. Fuente: ChatGPT

Cada vez se tiene un escenario más desafiante cuando hablamos de proteger información, infraestructura tecnológica, infraestructura crítica, personas y otras. Estos ejemplos son solo una parte de lo que se puede lograr, lo bueno es que también podemos considerar el uso de estas tecnologías para protegernos y es algo que empresas y fabricantes estamos haciendo.

Las tecnologías de Inteligencia Artificial pueden ayudar en la protección contra ciberataques de varias maneras, algunas de ellas son:

Detección de anomalías

Los sistemas de detección de intrusos basados en IA pueden monitorear el tráfico de red y el comportamiento de los usuarios para detectar patrones anómalos que puedan indicar un ataque en curso.

Análisis de malware

Los sistemas de análisis de malware basados en IA pueden identificar comportamientos maliciosos en el código de software y en los archivos adjuntos de correo electrónico, lo que puede ayudar a bloquear ataques antes de que causen daño.

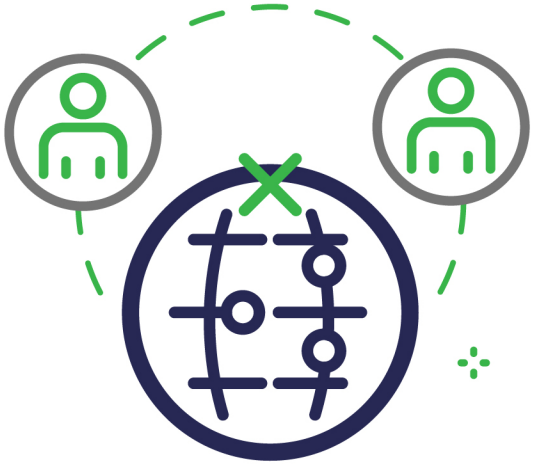
Respuesta automática a incidentes

Los sistemas de respuesta a incidentes basados en IA pueden actuar rápidamente para aislar sistemas comprometidos, detener la propagación de malware y minimizar el tiempo de inactividad en caso de un ataque.

Automatización de tareas de seguridad:

La IA puede ser utilizada para automatizar tareas de seguridad tediosas y repetitivas, como el análisis de registros de eventos y la aplicación de parches de seguridad, lo que libera a los analistas de seguridad para centrarse en tareas más importantes.

En general, la IA puede mejorar significativamente la eficacia de los sistemas de seguridad y ayudar a las organizaciones a protegerse contra una amplia variedad de amenazas en línea. Las herramientas actuales ya lo incluyen, debemos estar seguros de que lo usamos y que están correctamente entrenados para nuestras necesidades.



LA IMPORTANCIA DE UN MODELO DE GOBERNANZA EN CIBERSEGURIDAD

Redactado por:

HUAWEI

Un modelo de gobernanza de la seguridad cibernética es un marco que establece las políticas, los procedimientos, los controles y las responsabilidades necesarias para administrar de manera efectiva la seguridad de la información y los sistemas cibernéticos de una organización o nación.

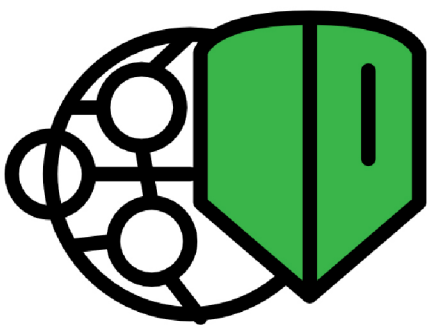
El modelo está diseñado para proteger los activos de información críticos, prevenir ataques cibernéticos y garantizar la continuidad del negocio; así como también busca crear una cultura de ciberseguridad en una organización o país que promueva la concientización y educación sobre los riesgos y amenazas cibernéticas para garantizar el desarrollo de la transformación y economía digital.

El modelo de gobernanza de la ciberseguridad consta de varios elementos como:

- **La identificación y evaluación de riesgos**
- **La implementación de medidas de seguridad**
- **La gestión de incidentes**
- **La auditoría y el seguimiento continuo de la ciberseguridad**

Este modelo puede ser aplicado tanto a nivel de organizaciones privadas como a nivel de países, y puede incluir la adopción de normas y estándares internacionales de ciberseguridad, como la norma ISO 27001:2022.

La gobernanza de Internet es un tema clave en la actualidad. Con una dependencia creciente de la tecnología y la conectividad, la ciberseguridad se ha convertido en una preocupación cada vez mayor para los gobiernos, las empresas y los ciudadanos de todo el mundo. Este artículo explorará tres áreas clave de la gobernanza de Internet: I). Cómo los modelos de gobernanza pueden fomentar un enfoque proactivo de la ciberseguridad, II). La importancia de la privacidad y la protección de la información y III). Los modelos de gobernanza estatal y del sector privado para la ciberseguridad.



Cómo un modelo de gobernanza fomenta un enfoque proactivo de la ciberseguridad

En un mundo cada vez más conectado, la ciberseguridad proactiva es fundamental para garantizar la protección en línea. Las defensas cibernéticas ya no son suficientes para proteger a las organizaciones e individuos de los riesgos del ciberespacio. Se necesitan soluciones proactivas para prevenir ataques y garantizar la seguridad en línea. Para fomentar un enfoque proactivo de la ciberseguridad, se necesita un modelo de gobernanza sólido que fomente la colaboración y la responsabilidad compartida. Debido que este es un reto común de la sociedad, la responsabilidad debe ser compartida por todos los actores, incluyendo gobiernos, empresas, industria, fabricantes de tecnología, gremios, entre otros.

El modelo adoptado por Brasil es un ejemplo de un enfoque proactivo de la ciberseguridad. En lugar de centrarse en la defensa cibernética y la criminalización del delito cibernético, Brasil ha adoptado un enfoque más amplio que incluye la concientización del usuario final y la responsabilidad comprobada.

El SIAT (Sistema de Investigação e Análise de Tráfego) es el sistema brasileño de monitoreo de tráfico de internet que permite la detección temprana de amenazas de seguridad y ciberataques, creado por el Centro de Defesa Cibernética (CDCiber), entidad perteneciente al Ministerio de Defensa de Brasil encargada de coordinar la defensa cibernética del país, y el Departamento de Seguridad de Información y Comunicación (DSIC-GSI), órgano que compone el gabinete, es directamente responsable por la coordinación de acciones de seguridad cibernética, lo que incluye la operación y manutención de un centro de tratamiento de incidentes en las redes de la Administración Pública Federal (APF) han sido responsables de implementar este enfoque en el sector empresarial y ha tenido mucho éxito en la promoción de una cultura de ciberseguridad proactiva, tal como se muestra en el artículo publicado en la revista latinoamericana de estudios de seguridad (junio-noviembre) 2017 “The brazilian cybersecurity policy as a strategy of regional leadership”.

La importancia de la privacidad y protección de la información

La privacidad y la protección de la información son fundamentales para la seguridad en línea. Los datos personales son valiosos y deben tratarse con cuidado. Las empresas y los gobiernos deben proteger los datos personales de los ciudadanos y garantizar la privacidad de la información. La privacidad es un derecho humano fundamental que debe protegerse tanto en línea como fuera de línea.

La protección de la información es especialmente importante en sectores críticos como la salud y el gobierno. Los datos personales en estos sectores pueden ser utilizados para cometer fraude o para dañar la reputación de un individuo. Además, los gobiernos deben garantizar que la información confidencial sea tratada con el mayor cuidado para proteger la seguridad nacional.

La concientización de las personas en los riesgos digitales

La concientización de las personas sobre los riesgos digitales es esencial para prevenir ataques en línea. Las personas deben entender los riesgos y saber cómo protegerse. Los gobiernos, las empresas y las organizaciones no gubernamentales pueden ayudar a promover la conciencia a través de campañas de concienciación y capacitación.

La educación sobre seguridad en línea es especialmente importante para los niños y jóvenes. Muchos niños tienen acceso a Internet sin supervisión y pueden ser víctimas de ciberacoso o explotación en línea. Es importante que los padres, tutores y educadores enseñen a los niños a proteger su información personal y a reconocer los riesgos y peligros que existen en la red.

En cuanto a la concientización de las personas en los riesgos digitales, es importante destacar que la educación es un elemento clave en la lucha contra el cibercrimen.

Según un informe de la Organización de Estados Americanos (OEA), en el año 2020, sólo el 32% de los países de la región contaban con programas educativos sobre ciberseguridad en las escuelas. Esta cifra refleja la necesidad de fortalecer los esfuerzos de educación y concientización en la materia.

Además, es importante mencionar que la gobernanza de la ciberseguridad no solo debe limitarse a los sectores públicos, sino que también es necesario un enfoque de colaboración con el sector privado. Los ataques cibernéticos pueden tener graves consecuencias para las empresas, tanto económicas como reputacionales, por lo que es fundamental que existan medidas de seguridad efectivas en el sector privado.

En este sentido, la norma ISO 27032, proporciona un marco de trabajo para la gestión de la seguridad cibernética en las organizaciones privadas. Este estándar establece una serie de directrices para la identificación, evaluación y tratamiento de riesgos relacionados con la seguridad de la información en el ámbito cibernético, En particular, ofrece unas líneas generales de orientación para fortalecer el estado de la ciberseguridad en una empresa, centrándose en diferentes aspectos técnicos y otros relacionados[7]:

Seguridad en las redes

Seguridad en Internet

Seguridad de la Información

Protección de las Infraestructuras Críticas para la Información

La gobernanza de la ciberseguridad es un tema crucial en la lucha contra el cibercrimen. Es necesario adoptar un enfoque proactivo que involucre a todos los actores relevantes, tanto del sector público como del sector privado. La educación y la concientización son elementos clave para prevenir los ataques cibernéticos, y la adopción de modelos de gobernanza efectivos puede contribuir significativamente a la protección de la información y la seguridad de las redes y sistemas de información.

[7] ISO/IEC 27032:2012 "Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad"

En Colombia, el modelo de gobernanza en ciberseguridad se aplica a través de la Estrategia Nacional de Ciberseguridad (ENC), que es liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). La ENC tiene como objetivo proteger los activos de información críticos del país, prevenir los ciberataques y garantizar la continuidad del negocio.

Los principales componentes del modelo de gobernanza en ciberseguridad en Colombia incluyen:

Política Nacional de Ciberseguridad

Define las directrices y principios para la gestión de la ciberseguridad en el país.

Plan Nacional de Ciberseguridad

Es un plan estratégico que establece las líneas de acción y objetivos a corto, mediano y largo plazo para mejorar la ciberseguridad en Colombia.

Marco Legal

Establece las normas y regulaciones necesarias para proteger la información y garantizar la seguridad cibernética.

Capacitación y Concientización

Es fundamental contar con programas de capacitación y concientización para que las personas estén conscientes de los riesgos cibernéticos y adopten comportamientos seguros.

Gestión de Incidentes

Es importante contar con planes y procedimientos para gestionar y responder de manera efectiva a incidentes de seguridad cibernética.

Cooperación Internacional

La cooperación con otros países y organismos internacionales es esencial para compartir información y buenas prácticas, y para mejorar la capacidad de respuesta ante amenazas cibernéticas globales.

La aplicación de un modelo de gobernanza en ciberseguridad tiene varios beneficios, tanto para las organizaciones como para los países en general.

Algunos de los principales beneficios son los siguientes:

Mejora la protección de los datos y la privacidad de los usuarios	El modelo de gobernanza en ciberseguridad ayuda a proteger los datos y la privacidad de los usuarios mediante la implementación de medidas técnicas y organizativas adecuadas
Reduce el riesgo de ciberataques	La aplicación de medidas de seguridad proactivas y la concientización de los usuarios sobre los riesgos digitales puede reducir significativamente el riesgo de ciberataques.
Incrementa la confianza de los usuarios	Al aplicar un modelo de gobernanza en ciberseguridad, las organizaciones y los países pueden demostrar su compromiso con la protección de los datos y la privacidad de los usuarios, lo que puede incrementar la confianza de los usuarios en ellos.
Cumplimiento normativo	La implementación de un modelo de gobernanza en ciberseguridad ayuda a las organizaciones y los países a cumplir con las leyes y normativas de seguridad de la información.
Ahorro de costos	La prevención de ciberataques puede evitar costos significativos asociados a la recuperación de los sistemas afectados, la investigación de los incidentes, la notificación a los usuarios afectados, entre otros.

La aplicación de un modelo de gobernanza en ciberseguridad puede ayudar a garantizar la protección de los datos y la privacidad de los usuarios, reducir el riesgo de ciberataques, incrementar la confianza de los usuarios, cumplir con las leyes y normativas de seguridad de la información y ahorrar costos asociados a incidentes de seguridad.

Referencias

Referencias
Referencias

1. https://www.crowdstrike.com/cybersecurity-101/attack-surface/
2. https://www.crowdstrike.com/cybersecurity-101/external-attack-surface-management/
3. https://www.crowdstrike.com/blog/why-easm-is-the-foundation-of-zero-trust-architecture/
4. https://www.crowdstrike.com/blog/crowdstrike-falcon-surface-adversary-driven-external-attack-surface-management-technology/
5. https://www.crowdstrike.com/blog/


CCIT
tictac
SAFE
SEGURIDAD APLICADA AL FORTALECIMIENTO EMPRESARIAL