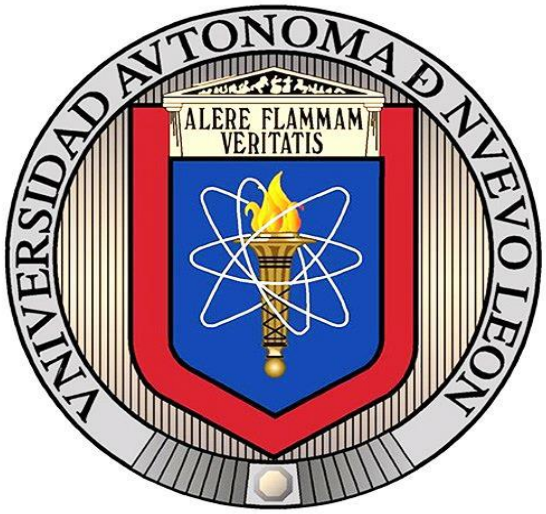
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS



TESIS

EL RANSOMWARE Y LA CULTURA DE SEGURIDAD

POR
LIC. ALEXIS VIELMA MONTAÑEZ

EN OPCIÓN AL GRADO DE
MAESTRÍA EN INGENIERÍA EN SEGURIDAD DE LA INFORMACIÓN

JUNIO, 2022

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

SUBDIRECCIÓN DE POSGRADO

EL RANSOMWARE Y LA CULTURA DE SEGURIDAD

POR
LIC. ALEXIS VIELMA MONTAÑEZ

EN OPCIÓN AL GRADO DE
MAESTRÍA EN INGENIERÍA EN SEGURIDAD DE LA INFORMACIÓN

SAN NICOLÁS DE LOS GARZA, NUEVO LEÓN, MÉXICO **JUNIO 2022**

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

SUBDIRECCIÓN DE POSGRADOS

Los miembros del comité certifican que han leído la disertación que presenta **Alexis Vielma Montañez** como requisito parcial para obtener el grado de:

MAESTRÍA EN INGENIERÍA EN SEGURIDAD DE LA INFORMACIÓN

_____
Dr. Miguel Ángel Valdés Alvarado
Sinodal

_____
Mtro. Alfredo Juan Halun Tafich
Sinodal

_____
Mtro. José Carlos Rodríguez Reyna
Asesor

_____
Mtro. José Alberto Cárdenas Jaimes
Coordinador de la Maestría en Ingeniería en Seguridad de la Información

Junio, 2022

Declaración de Derechos de Autor

Declaro por este medio haber escrito yo mismo esta disertación y que presento exclusivamente mis investigaciones.

Lic. Alexis Vielma Montañez

San Nicolás de los Garza, Nuevo León, México **Junio, 2022**

I. INTRODUCCIÓN

1.Tema de Investigación

En los últimos años, ha habido un aumento en el uso y la popularidad de los programas maliciosos por el creciente uso de los dispositivos inteligentes, ambientes computacionales automatizados y la implementación del uso de sistemas digitales personales para la comunicación empresarial ya sean móviles o portátiles. Y entre los programas maliciosos que tuvieron un aumento de uso significativo, resalta una variante que secuestra computadores y encripta sus datos para pedir un rescate.

Esta variante es conocida como "*ransomware*", que ha probado ser un programa altamente efectivo por sus tácticas de miedo además de la gran capacidad de impacto y destrucción que puede tener para cualquier negocio y usuario afectado. Con la entrada de la pandemia del COVID-19 en el 2019 se comenzaron a utilizar con mayor medida las tácticas de ataque que usan la ingeniería social para afectar a los empleados y usuarios dentro de las compañías, así como dentro de sus hogares, aprovechando la falta de conocimiento y cultura de la seguridad de los mismos.

La falta de cultura y conciencia de la seguridad es un problema grave que puede llegar a ser muy costoso en cómo afecta las probabilidades de un ataque exitoso y el impacto a las operaciones de una organización, así como por la pérdida de datos que ocasionan. El problema de la desinformación y desinterés puede yacer en todos los niveles de una empresa, haciendo que los hábitos que se generan dentro de ella, así como su cultura de seguridad sean pobres, abriendo un amplio espectro de probabilidades para ataques futuros y quitando eficiencia en las actividades del negocio

Para afrontar este tipo de carencias y amenazas cibernéticas se puede construir una cultura solida de seguridad, basada en la conciencia sobre las amenazas y la importancia de la prevención. Usando tácticas defensivas, con el apoyo de la administración de la empresa, los departamentos dentro de ella y de autoridades internacionales se puede mitigar y resolver los ataques crecientes de ransomware al mismo tiempo que se disminuye el riesgo de otro tipo de incidentes y *malware*,

incluyendo los ataques más difíciles de detectar como los son los que se realizan dentro de la red loca o personal de un usuario lejos del ecosistema de red de la empresa.

2. Antecedentes de Estudio

El "*ransomware*", nombre que se le asignó a este tipo de programa malicioso, está compuesto por dos palabras en inglés: "*Ransom*" que se refiere a un secuestro que exige rescate y "*Malware*", cuyo nombre se les da a los programas maliciosos en este idioma. El Ransomware es un programa virulento que inhabilita la maquina donde se ejecuta y bloquea el acceso a la información dentro de ella usando como herramienta principal la manipulación de credenciales y la encriptación de archivos. Posteriormente un rescate monetario es exigido a cambio de la liberación de la información secuestrada.

Figura 1: Pantalla de infección de *Ransomware*.

Fuente: Aisvector (2018).

Aunque el uso de programas maliciosos sea un concepto que se percibe como muy contemporáneo y apegado al auge de la internet, las menciones de *ransomware* datan de 1989. Fue en este año, cuando un biólogo llamado Joseph

L. Popp repartió disquetes a diferentes individuos conteniendo un *malware* al que llamó "AIDS". Este *malware*, encriptaba las computadoras después del encendido número noventa del sistema infectado, exigiendo un rescate de ciento ochenta y nueve dólares que se enviaba a una dirección postal en Panamá. (Savage, Coogan, & Lau, 2015).

El primer *ransomware* moderno vino desde las regiones interiores de Rusia, con la campaña de ataque en el 2005 de "GPCode" un virus troyano que usaba el método de encriptación simétrica para tomar posesión de los archivos de las víctimas. Esta primera variante moderna era débil contra los programas de análisis y desencriptación lo cual, obligó a los creadores a refinar sus algoritmos de ataque.

Un año más tarde en el 2006 el método de ataque del *ransomware* comenzó a incrementar su popularidad por la efectividad que tenía contra usuarios individuales. Además del factor "miedo" que se le inculcaba al individuo afectado. "Crysip" apareció en marzo del mismo año, usando un método de copia de archivos con contraseñas. Se aseguraba de borrar todos los documentos originales, y dejaba las carpetas con contraseña a la vista de la víctima, asegurándole a la misma que se le daría acceso una vez pagado el rescate. (Richardson, R., & North, M. M. ,2017).

Meses después se inició también la campaña de ataque de "Archiveus" que operaba de forma similar a Crysip, pero en lugar de pedir un rescate monetario pedía la compra de medicamentos de farmacias específicas y exigía el número de identificación del pedido para dar acceso al sistema (Richardson, R., & North, M. M. ,2017).

En el 2007 la variante "Locker" comenzó a desarrollarse, siendo este el método que, a diferencia de sus antecesores, no usaba algoritmos para encriptar la información, en cambio este inhibe la computadora y sus sistemas evitando su uso completamente. En ese mismo año, dentro de las mismas regiones rusas, "Locker" usaba este nuevo método para programar un bloqueo que proyectaba una imagen pornográfica en la pantalla de la computadora, evitando cualquier otra acción más que la exposición de la imagen. El pago acordado se organizaba para ser enviado vía SMS o llamando a un numero de paga premium. Estos ataques fueron extendiéndose por toda Europa y EE. UU (Savage, Coogan, & Lau, 2015).

Los métodos de encriptación usados en estos *malware* evolucionaron rápidamente al año siguiente con el uso de un algoritmo de llave RSA de 1024 bits, siendo este el

algoritmo de criptografía más ampliamente usado por su factorización de números enteros. Este algoritmo basaba el resultado en el producto de estos cálculos para la protección de la información.

La variante del toryano “Gpcoder”, de nombre: “GPcode.Ak” usaba esta llave para secuestrar los datos de la computadora y dejar en una nota de texto las demandas de los atacantes, pidiendo dinero en inversiones de oro o en la reserva “*Liberty*”. (Nadir, I., & Bakhshi, T. ,2018).

Dando un salto de tiempo al año 2011 a mitad del año, el *ransomware* tuvo una explosión en incremento de popularidad y uso, ya que en ese año estaban surgiendo los métodos de pagos anónimos y digitales como paypal o transferencias por medios web. Se detectaron hasta ciento veinte mil casos nuevos de ataques alrededor del año y entrando el 2012, un kit de herramientas para sistemas operativos llamado “Citadel” fue liberado. El contenido que tenía Citadel podía facilitar la programación y distribución de nuevos *ransomware*. Esta herramienta costaba tres mil dólares el adquirirla, promocionando que con el programa malicioso se podían obtener ingresos mucho mayores.

Como competencia en el mercado también fue liberado “Lyposit”, el cual estaba diseñado para programar *ransomware* que pareciera que provenía de oficinas gubernamentales. “Lyposit” adaptaba la procedencia de estas oficinas según la región en la que era ejecutado. (Richardson, R., & North, M. M. ,2017).

Durante este periodo, el uso de encriptación en vez de las variaciones “locker” fue más prominente ya que los “locker” eran fácilmente derrotados a pesar de las mejoras que implementaban sus programadores y surgieron métodos de encriptación más convincentes. Usando ingeniería social y tácticas de miedo, el engaño consistía en disfrazar el *malware* para hacer pasar los mensajes maliciosos y descargas varias de los programas como mensajes legítimos. Un ejemplo siendo notificaciones del FBI, argumentando que se había roto una ley federal, esta táctica fue implementada por el *malware* llamado “Reventon”. Otra notificación venia en mensajes del sistema de Windows, usado por la variante de troyano “Randsom.C”. (Richardson, R., & North, M. M. ,2017).

En el año del 2013, uno de los *ransomware* más famosos fue lanzado en agosto, distribuido a las víctimas por otro programa llamado "Gameover ZeuS banking". Después evolucionó a ser enviado masivamente por cuentas de correo que parecían ser de UPS o FedEx. Este programa llamado "CryptoLocker" fue desarrollado por Slavik, un hacker que implementó el concepto de llaves privadas y públicas en su algoritmo de encriptación y liberación de la información, afectando principalmente a las carpetas principales del sistema de Office. Se le daba un día a la víctima para pagar el valor de dos bitcoins (cien dólares en ese año) por medio de varias transferencias bancarias internacionales como CashU o MoneyPak y si el tiempo se agotaba sin que el rescate fuera pagado, la cantidad podía aumentar hasta diez bitcoins (Richardson, R., & North, M. M. ,2017).

Varias versiones del *malware* salieron meses después como CryptoLocker 2.0 y una imitación con el nombre de "LockerEmerged". Se estima que se pagaron alrededor de cuarenta y un mil novecientos veintiocho bitcoins, solo con el 3% de las victimas que accedió al pago (Nadir, I., & Bakhshi, T. ,2018).

Yahoo en este año fue víctima de un gran ataque informático que afectó a más de mil datos personales y sensibles de sus usuarios. Uno de sus grandes errores fue haber callado durante años el incidente, algo que provocó que su CEO fuera cesado de sus funciones. La brecha de seguridad le costó a la compañía unos tres mil millones de dólares ya que se expusieron datos sensibles como direcciones de email, claves, cumpleaños, números de teléfonos, así como nombres y apellidos de las personas registradas en la plataforma. (APD, 2018).

A mediados del 2014 una coalición de agencias del gobierno, empresas de seguridad y universidades tumbaron los servidores de distribución Cryptolocker. Dos empresas encontraron la base de datos de llaves de encriptación y liberaron un servicio gratuito al público donde las victimas podían obtener su llave y desencriptar sus máquinas. Desafortunadamente en poco tiempo se desarrolló otro programa de *ransomware* llamado "CryptoDefense" que, aunque empezó como un programa fácil de eliminar mejoró su versión a "CryptoWall", explotando una vulnerabilidad de java permitiéndole inyectar publicidad engañosa para infectar al sistema. Se estima que estas dos campañas de ataque recaudaron un millón treinta cuatro mil dólares.

La compañía Sony tuvo una serie de ciberataques a varias de sus divisiones que provocaron unas pérdidas millonarias a la organización. Uno de los ataques mencionados, fue llamado por el propio Barack Obama como “intento de extorsión”. Este ataque fue el que afectó principalmente al departamento audiovisual.

Los atacantes se dedicaron a robar correos y películas de la compañía, provocando la cancelación de rodajes cinematográficos que se estuvieran filmando en el momento y haciendo lo mismo con los estrenos cinematográficos programados. Además de los ataques, se produjeron amenazas personales y tras una larga investigación, el FBI responsabilizó de todos los incidentes a Corea del Norte. (APD, 2018).

A fines de 2015 el FBI estimó que las víctimas habían pagado veintisiete millones de dólares en rescates a los atacantes detrás de CryptoLocker. Pero se vio un incremento en CryptoWall superando a Cryptolocker como la versión líder de *ransomware* en poco tiempo, siendo más usada en crimenes que su contraparte. Además, se realizó un estudio de Kaspersky que encontró que para 2014-2015, los ataques de *ransomware* aumentaron en un diecisiete por ciento, pero los ataques de cripto *ransomware* aumentaron en un impresionante cuatrocientos cuarenta y ocho por ciento. (Richardson, R., & North, M. M. ,2017).

En febrero del 2016, se descubrió que el programa malicioso llamado “Xbot” apuntaba a dispositivos Android en Australia y Rusia. No solo encripta archivos, sino que también intentaba robar datos bancarios en línea. En julio, el *ransomware* “Locky” mejoró el sistema agregando un mecanismo a prueba de fallos que comienza a cifrar archivos incluso si el *ransomware* no puede solicitar una clave de cifrado única, esto dependiendo de los servidores de los delincuentes, que se podía deber a que la computadora objetivo estaba fuera de línea, en modo suspensión o bloqueando las comunicaciones. Se calculó que el *ransomware* generó doscientos nueve mil millones de dólares en los primeros tres meses de 2016. (Richardson, R., & North, M. M. ,2017).

Durante el primer trimestre, “McAfee Labs” midió un millón doscientos mil ataques de *ransomware*. Este fue un aumento del veinticuatro por ciento con respecto al cuarto trimestre de 2016, con una versión mejorada de “CryptoWall” que tomó como base e implemento sus mejoras a partir de CryptoDefense (Nadir, I., & Bakhshi, T. ,2018). Esta nueva versión no solo cifra los archivos en la computadora infectada, sino que también

apunta a cualquier almacenamiento externo o unidades compartidas conectadas al objetivo, infectando objetivos tales como memorias USB, discos duros externos y secundarios en la maquina o Incluso CDs.

De los *ransomware* más usados en el 2016 destacaron “CTB-Locker” que es la abreviatura de “Curve-Tor-Bitcoin”, Cryptowall y TorrentLocker. Tanto CryptoWall como CTB-Locker tienen programas de ventas afiliados. TorrentLocker recolecta direcciones de correo electrónico cuando infecta una computadora para enviar spam a otros usuarios y expandir la lista de infectados usándola exponencialmente. (Richardson, R., & North, M. M. ,2017).

En mayo del 2016 llegó el *ransomware* como servicio de paga. Al utilizar el sitio web TOR, los atacantes podrían crear *ransomware* de forma gratuita y distribuirlo a sus víctimas. El sitio maneja el pago del rescate y se lleva un 20 por ciento de comisión total, convirtiéndolo en un negocio extremadamente popular entre la comunidad hacker.

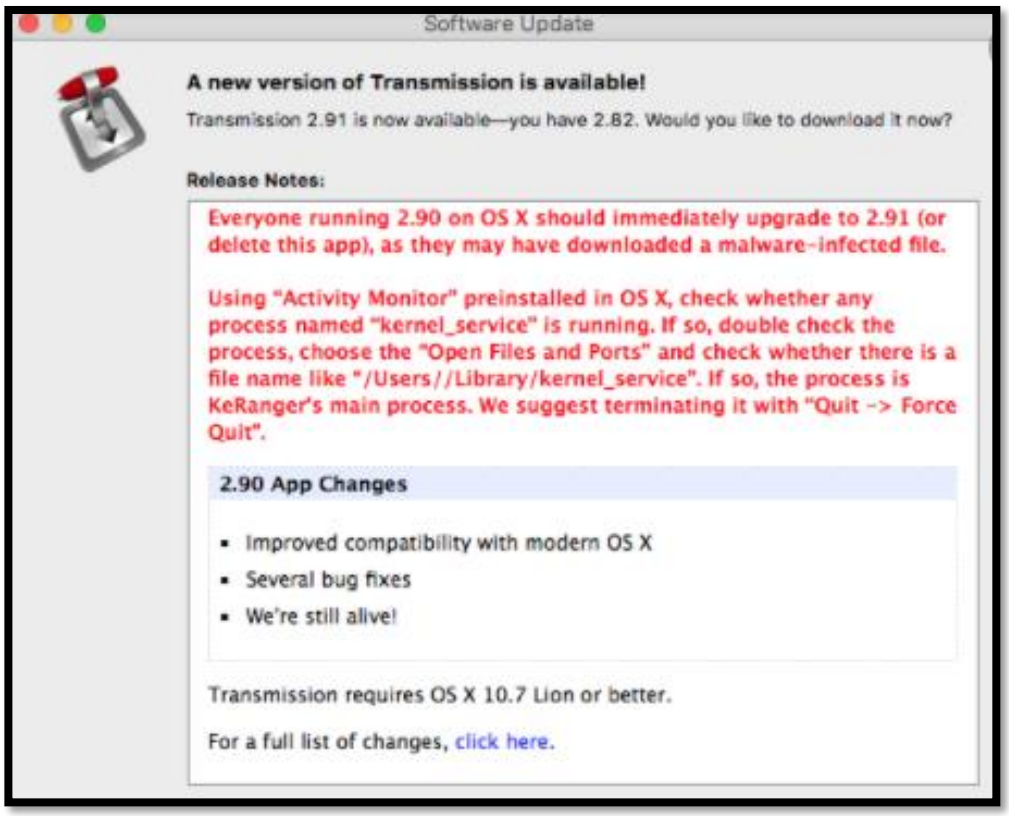
Seis meses después, LockerPin fue lanzado Infectando ahora los sistemas Android, expandiendo el rango de víctimas ahora a servicios y aparatos móviles. Dentro del sistema del celular, cambiaba el PIN de desbloqueo cobrando un rescate de quinientos dólares. (Richardson, R., & North, M. M. ,2017).

En octubre, un nuevo informe de “Cyber Threat Alliance” informó que el daño total del *ransomware* ascendía a trecientos veinticinco millones de dólares. En noviembre, “Linux.Encoder.1.0” fue descubierto por Dr. Web, una empresa rusa de seguridad informática. Este nuevo software malicioso se enfocaba en los sistemas Linux, que, hasta el momento de su creación, no eran objetivos muy populares por su escaso mercado global. El programa ataca tanto archivos de datos como archivos asociados con aplicaciones web como el navegador. (Richardson, R., & North, M. M. ,2017).

En noviembre, surgió la cuarta iteración de “Cryptowall” incluyendo un protocolo modificado para ayudar a evitar la detección, además de alterar los nombres de los archivos cuando los cifra, lo que dificulta determinar qué archivos estaban afectados y confundiendo a la víctima como a quien quisiera intervenir y recuperarlos. Se descubrió un *ransomware* como serviciode paga solo del lenguaje JavaScript (Nadir, I., & Bakhshi, T. ,2018). El uso de JavaScript permite un ataque multiplataforma, incluidos Linus y MacOS X. Esto le permitió a ese servicio de *ransomware* infectar a miles de sitios web

de WordPress. (Richardson, R., & North, M. M. ,2017). WordPress es una plataforma de blogs popular que se convirtió en una página de servicio de hosting para páginas web haciéndolo el objetivo ideal.

Figura 2: Ejemplo de mensaje infectado con ingeniería social.



Fuente: Kim, A. , (2016).

En abril del siguiente año, salió un *ransomware* llamado “Petya”, el comportamiento de este hace que todo el disco duro sea inaccesible hasta que se pague el rescate y para ello, sobrescribe el registro de arranque maestro de la computadora infectada. Sin el arranque maestro, el sistema operativo no puede reconstruir los archivos no cifrados, dejando inútil cualquier intento de ingreso al disco duro por otro medio. (Richardson, R., & North, M. M. ,2017).

Después de estos incidentes, meses después se crea “KeRanger”. Se estima que KeRanger es el primer ataque de *ransomware* dirigido a computadoras Apple. Una vez instalado, tarda tres días en activarse y está diseñado para cifrar más de 300 tipos de

archivos. La compañía tuvo que lanzar una actualización para bloquear este *ransomware* dirigido. (Richardson, R., & North, M. M. ,2017).

En el año 2017 se crearon “Philadelphia”, “Kirk”, “Doxware” y uno de los ransomaware más infames de los últimos años, llamado “Wanna Cry”, lanzado en mayo. Para este incidente fue señalado como responsable al norcoreano “Park Jin hyok” como autor del *malware*. Este programa fue responsable de un ataque a escala mundial que afectó compañías grandes y agencias, cubriendo un estimado de ciento cuarenta y un mil computadoras. (APD, 2018).

Después de un año en el 2018 se creó uno de los *ransomware* que todavía es relevante en el año actual (2021): “RobinHood”, un programa que se distingue por ser distribuido no por métodos de spam ni mensajería o email. El método por el que este *malware* es propagado es por servicios de acceso remoto al escritorio, donde el atacante podía copiar el virus dentro de la máquina. Otro método era por virus troyanos que viajaban en archivos o anuncios infectados de publicidad. Una vez que RobinHood infecta la máquina, detiene los 181 servicios asociados al antivirus; bases de datos; servidores de correo electrónico y otros servicios que pudieran evitar la encriptación. (Krauss, 2021).

Fue dentro del 2019 que se creó otro tipo del *malware* llamado “Sodinokibi” que se especializa en sistemas Windows, cuya propagación sigue el modelo RaaS (*Ramsonware as a Service*), que como se comenzó a ver anteriormente, adapta su funcionalidad de acuerdo al usuario que renta el servicio o compra este programa malicioso. Para infectar los sistemas recurre a diferentes técnicas para dificultar su análisis e identificación de sus firmas por parte de otros programas de seguridad, por ejemplo, la detección de antivirus o sistemas de detección de intrusión (IDS). Esta característica lo hace extremadamente peligroso ya que pasa desapercibido ante controles de este tipo, entrando en la nueva categoría de “*malware* adaptivo”, *Malware* que puede modificar su propio código para no ser identificado. (Lovelace, R., 2021).

Siguiendo la evolución de *malware* adaptivo fue creado el ransomaware “DarkSide” en el verano del 2020, también creado como un servicio contratable y personalizado con cobro de comisión. Este programa puede cobrar desde doscientos mil dólares hasta dos millones. El grupo de hackers detrás de la programación de Darkside,

comparte el mismo nombre del *malware* y comenzó con tácticas de ataque masivo a empresas y organizaciones grandes, además de usar su infiltración para robo de otro tipo de datos sensibles. (Lovelace, R., 2021).

Únicamente en América Latina, entre enero y septiembre de 2020, se detectaron y bloquearon alrededor de un millón trecientos mil de intentos de ataque de *ransomware*, lo que se traduce en cinco mil ataques por día. En septiembre de este año, un ataque a un hospital importante en Dusseldorf resultó en la primera muerte relacionada con *ransomware* en la historia. En el mismo mes, UHS, una de las cadenas de proveedores de atención médica más grandes de los Estados Unidos, fue golpeada por un ataque de *ransomware* que provocó el bloqueo de computadoras y sistemas telefónicos. (APD, 2018).

En el año actual de 2021, un ataque a un oleoducto se reportó cuando la empresa de colonial Pipelines fue infectada por el *malware DarkSide*, que tomo control de los sistemas y los bloqueo dejando los servicios y administración inservibles, además de parar la producción. (Krauss, 2021).

El costo real de un ataque de *ransomware* envuelve las pérdidas de ingresos durante el tiempo de inactividad; Las tarifas pagadas a expertos en ciberseguridad; Varias multas que se ponen por autoridad federal e internacional; Y daños a la reputación; Siguiendo incluso la pérdida de negocios físicos o capitalización.

3. Antecdentes y Planteamiento del Problema

El *ransomware* tiene métodos diferentes de propagación, diferenciando sus formas de ataque entre ellos dependiendo de la víctima a la que se tiene como objetivo. Hay métodos que son más efectivos para un negocio u organización, o para un individuo en sistema independiente y personal. Los métodos más comunes de infección son los *kits* de explotación de vulnerabilidad; Los archivos maliciosos adjuntados en correos electrónicos y los enlaces de URL también enviados por medio de correo engañoso. Siguiendo el modo de operar de estos métodos por correo electrónico, las victimas reciben un correo que implementa varias tácticas de ingeniería social y engaño, incitando la interacción con su contenido. (Surati&Prajapati, 2017).

Las estrategias de la creación de estos correos maliciosos rondan desde la falsificación de identidades de compañías que suelen usar las víctimas, o el robo de identidad de algún contacto de confianza. Es una estrategia común que se aliente a la víctima a interactuar de forma activa con el contenido del correo, ya sea descargando un archivo que está infectado con el programa malicioso; Abriendo algún documento que contiene una rutina maliciosa en él; Entrando a una página web fraudulenta que contenga una descarga automática del archivo infectado, o un formulario engañoso para obtener información. (Surati&Prajapati, 2017).

Los métodos alternativos a la ingeniería social son la explotación de vulnerabilidades y los kits de herramientas de explotación se pueden incluso conseguir como servicios contratables. Estos kits tienen información y código especializado en una debilidad ya documentada del sistema computacional de la víctima, usándolo como entrada y forma inicial de infección. Esto puede ser visto en versiones desactualizadas de los sistemas operativos, así como de programas o servicios usados dentro del sistema o la red. Los parches de seguridad son necesarios en ambos ámbitos de trabajo, el digital y el físico, incluyendo los equipos que conviven en el ecosistema alrededor de los computadores, servidores y demás herramientas usadas para las operaciones del día al día. (Martins, A., & Elofe, J.,2002)

Todo lo anterior tiene como elemento común el factor humano, siendo los empleados la primera y última línea de defensa. Los empleados son los encargados de la administración, mantenimiento, supervisión y manejo de estos equipos, así como las herramientas que se usan en ellos.

> *"Implementar soluciones técnicas de seguridad de la información no es suficiente. La efectividad de los controles de seguridad de la información depende de la competencia y confiabilidad de las personas que lo implementan y usan. Podría haber controles de seguridad adecuados como firewalls, pero si la administración no los maneja de manera efectiva o si los usuarios no saben cómo operar correctamente un firewall, el elemento humano se convierte en el factor dependiente y no la tecnología. En cualquier momento, los usuarios interactúan con los activos informáticos de alguna manera y por alguna razón. Esta interacción*

representa el eslabón más débil de la seguridad de la información." (Martins, A., & Elofe, J.,2002).

Esto arroja nueva luz sobre los problemas dentro de la cultura que se ejerce en las organizaciones. Dando paso a que los ataques de Ransomware sean exitosos y convertirse en el modelo de negocio que se tiene en la actualidad. La manera en que las personas interactúan con el medio ambiente de trabajo y sus activos en el día a día, se convierte con el tiempo en habito y parte de la cultura laborar que si tiene dentro de la organización. Es importante que esta cultura se desarrolle y crezca de una base enfocada en la seguridad. Un ejemplo de tal comportamiento podría ser que la información del cliente deba manejarse con confidencialidad o que solo el personal de mantenimiento autorizado pueda realizar reparaciones y dar servicio al equipo informático. (Martins, A., & Elofe, J.,2002).

El problema con la cultura de la seguridad de la información que se tiene a nivel nacional es bajo, como se puede observar en el caso del ataque a las instalaciones de Pemex en el 2019. El Ransomware "WannaCry", responsable de este ataque y del paro masivo de operaciones, atacaba específicamente vulnerabilidades del sistema operativo de Windows XP, sistema que los encargados de seguridad de la empresa no vieron como prioritario actualizar ni prever las fallas relacionadas con este sistema obsoleto. (Ruiz, E., 2019).

Tan solo el 7% de las empresas cuentan con protecciones basadas en prevención para poder hacer frente a amenazas de nueva generación. Y esto se debe a que las áreas de ciberseguridad de las empresas siguen creando estrategias basadas en un esquema de detección y reacción (firewalls, antivirus, IPS, etc.). Las herramientas basadas en tecnologías de detección son necesarias ya que protegen la red y los componentes de esta contra las amenazas que actualmente se conocen. Aunque no pueden actuar solas ya que son ineficientes a la hora de enfrentarse a ataques desconocidos o de "día cero. (Ruiz, E., 2019).

"Para facilitar esto, es necesario inculcar una cultura de seguridad de la información en la organización. Sin embargo, se plantean las siguientes preguntas: "¿Qué es la cultura de seguridad de la información?" y "¿Cómo inculca una organización la cultura de seguridad de la información?" Para responder a

estas preguntas, es necesario definir el concepto de cultura de seguridad de la información. Luego se propone un modelo y un enfoque de evaluación, que una organización podría utilizar para inculcar una cultura de seguridad de la información. Por último, se discute un estudio de caso en el que se utilizó un enfoque de evaluación para evaluar la cultura de seguridad de la información de una organización." (Martins, A., & Elofe, J.,2002).

Todo esto junto con la falta de preocupación por el mantenimiento del equipo puede dar oportunidades de que un atacante con *ransomware* pueda entrar a los sistemas. El poder sembrar una cultura de seguridad en las organizaciones no es tarea fácil ya que puede tomar años el inculcar los hábitos correctos en el personal, además de tratar con las políticas de seguridad, la tarea de concientización sobre riesgos al personal, además del cuidado de los activos de la empresa y sus equipos. El enfoque empresarial debe ser considerado en tres niveles: "Organizacional", que es el nivel donde se implementan las políticas de seguridad que rigen el comportamiento dentro del ambiente laboral, "Grupal" el cual incluye a todos los ejecutivos y supervisores a cargo de áreas y grupos de la organización, e "Individual" el cual considera a los empleados a un nivel personal, dándoles apoyo y alentándolos a informarse sobre los temas de seguridad. La seguridad en estos tres niveles debe ser considerado cuando se necesita una correcta implementación de una cultura de protección de los datos. (Martins, A., & Elofe, J.,2002).

4. Justificación

Observando las consecuencias catastróficas que conlleva la ausencia de una cultura de seguridad con bases sólidas en la conciencia sobre riesgos y lleve un nivel de conocimiento hacia todos los niveles de una organización, se convierte en un tema crítico el dar las herramientas y el conocimiento necesarios para que tanto el ambiente empresarial como el individual de sus empleados crezcan hacia un estado elevado y bien organizado de madurez dentro de sus programas de seguridad.

En esta investigación se documentan los ataques por ransomware de manera que se pueda apreciar de forma sencilla el comportamiento, y el modo de operar que se llevan a cabo los procedimientos ofensivos de los mismos y sus objetivos más comunes,

así como las posibles repercusiones que se pueden tener al ser víctima de uno de estos secuestros de datos, esto con el propósito de hacer conciencia sobre el peligro que conlleva este tipo de ataques y tener un antecedente reciente como base para fortalecer los esfuerzos de protección de datos y de los activos importantes de un ambiente digital.

El conjunto de diversas recomendaciones y tácticas defensivas aporta en las áreas de conciencia y cultura de las empresas, dando una guía inicial para la fundación de programas de seguridad que prevengan incidentes de forma efectiva y que a su vez contengan la información y los protocolos adecuados para afrontar un incidente en caso de que la primera línea de defensa falle.

Con el progreso de los programas de conciencia y el aumento de madurez dentro de las empresas se prevé que la cultura de las personas cambie positivamente, pasando estas enseñanzas de individuo a individuo y que se deje en un estado impermeable la mayor parte del espacio laboral y personal. Esto también influye en las áreas administrativas, aumentando la calidad de la gestión por parte de los diferentes líderes y su visión sobre los temas de seguridad.

5. Objetivos

A. Objetivo General

- Documentar y estudiar sobre los ataques de ransomware más relevantes de los últimos cinco años. Analizar la cultura de seguridad dentro de empresas según estudios recientes, así como presentar recomendaciones reconocidas internacionalmente para evitar incidentes y manejarlos en caso de que se esté bajo ataque.

B. Objetivos Específicos

i. Informar sobre los últimos ataques con relevancia en cuanto al objetivo afectado con *ransomware* en últimos 5 años y las características del incidente.
ii. Analizar los reportes sobre cultura de la seguridad respecto a concientización de personal y dedicación a estas que se tienen las empresas.

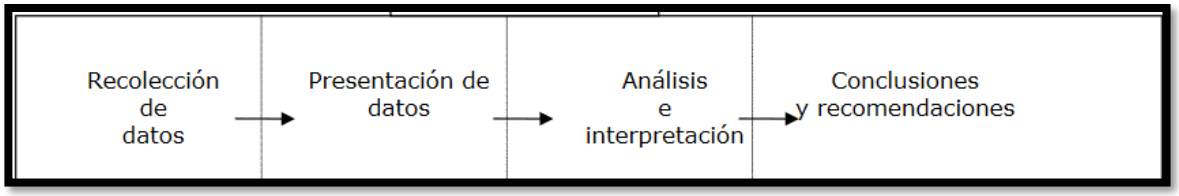
iii. Analizar las recomendaciones más usadas internacionalmente, como las emitidas por agencias de seguridad internacionales para evitar un incidente de *ransomware* y el cómo manejarlo si se encuentra bajo ataque.
iv. Desglosar los planes y recomendaciones de seguridad para mejorar la cultura de seguridad dentro del ecosistema empresarial y fomentar la concientización del personal.

6. Marco Metodológico

Se usará el método cuantitativo mencionado por Nelly López e Irma Sandoval (López, N., & Sandoval, I., 2016) para la búsqueda y clasificación de documentación sobre los ataques de *ransomware* del último lustro, poder procesar los datos extraídos de los informes y reportes de manera imparcial y estadística; así como para el análisis de las políticas de seguridad, las recomendaciones internacionales y los gráficos estadísticos presentados ya que este método permite la recolección y análisis de datos de forma lógica y previamente indexada para su extracción. Con esto se puede realizar una clara presentación de los hechos en un enfoque generalizado y poder resaltar las tendencias de ataques a nivel global e internacional.

Así mismo se usará el método cualitativo mencionado en la misma investigación de Nelly López e Irma Sandoval para poder expresar las opiniones y observaciones que van generando conforme la investigación es realizada y partiendo de las pautas de los datos poder realizar un estudio flexible pero exhaustivo para poder comprender las raíces de los informes de seguridad más allá del aspecto técnico, y entender el comportamiento humano detrás de las diferentes culturas, hábitos y modelos de negocio internacionalmente.

Figura 3: Marco del proceso de información de la investigación.



Fuente: López, N., & Sandoval, I. (2016).

La recolección de información se llevará a acabo de medios públicos oficiales que representen las estadísticas y detalles de las políticas y métodos de concientización de las empresas nacionales. También la consulta a boletines emitidos por entidades federativas de México, Estados Unidos y la Unión Europea sobre el cuidado y prevención de ataques informáticos independientes o de grupos de hackers. Y se va a analizar la información extraída con el concepto y método de análisis de documentos expuesto por Fernando López Noguero (López Noguero, F. ,2002) para poder comparar los diferentes resultados de la investigación.

II. EL RANSOMWARE Y SU CORRELACIÓN CON LA CULTURA DE SEGUUIRDAD

1. Los ataques de ransomware más relevantes dentro del lustro

Para poder entender y visualizar mejor el progreso del *ransomware* en los últimos años, se verá que incidentes fueron los que más resaltaron del 2016 al año presente 2021 por su capacidad destructiva, su víctima objetivo e impacto a la organización o redes afectadas. Esto con el propósito de documentar los métodos que usaron y como han evolucionado, así como el denotar las fallas que se tuvieron de parte de las víctimas para haber sucumbido ante el ataque criminal.

A. WannaCry atacando al mundo

En mayo del 2017 se lanzó un ataque masivo alrededor del mundo, afectando aproximadamente 150 países. El virus enfocaba su ataque en el sistema operativo de Windows, entrando por una de las vulnerabilidades del sistema que existían en ese año,

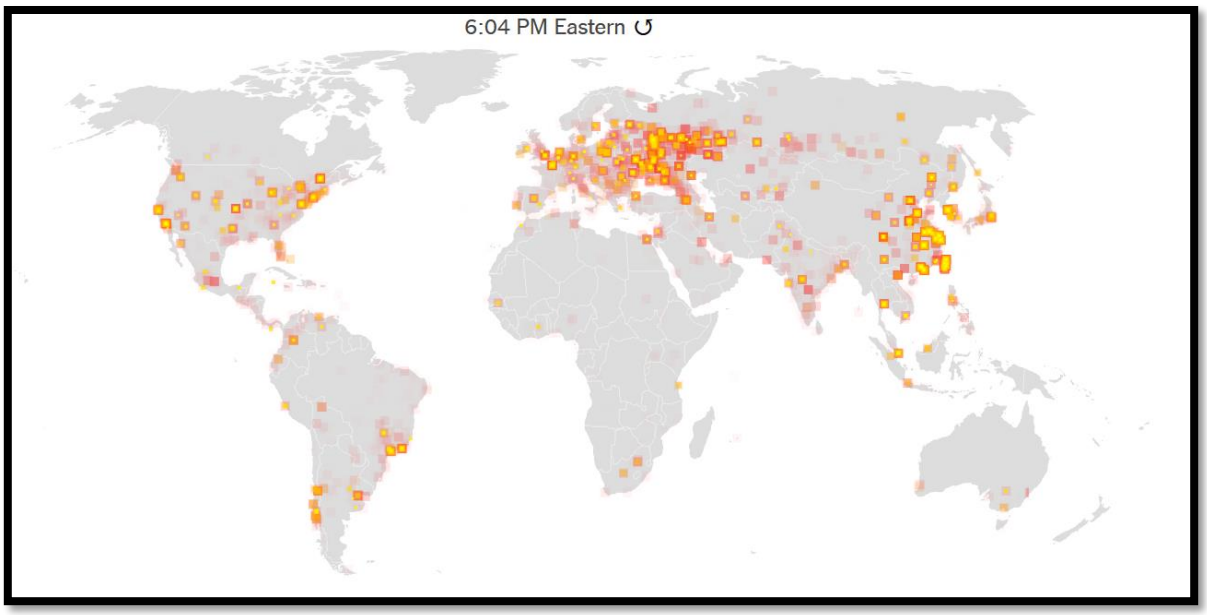
la cual consistía en un protocolo que fallaba del SMB (*Server Message Block*) del sistema. (Chen, Q. & Bridges A.R. 2017).

Wannacry en vez de usar el método de correo electrónico infectado, se infiltró en redes públicas y escaneaba por sistemas que tuvieran el puerto TCP 445 abierto, el cual pertenecía al SMB (Sahi, S. K. 2017). Al entrar al sistema comienza a analizar los archivos y sus contenidos. Aísla al antivirus de sus operaciones para evitar ser detectado. En cuanto termina su análisis el virus encripta con un algoritmo todas las carpetas y archivos ocultándolos del usuario, dejando un mensaje de que la computadora fue infectada y se requiere un pago en criptomonedas para poder tener la contraseña y desencriptar la computadora. (Savita Mohurle, M. P. 2017, mayo).

Después de secuestrar al sistema, buscaba formas de expandir su infección por medio de la misma red donde se conectó o por medio de internet. Según los análisis del antivirus “eScan” la India fue de los países más afectados por este ataque con más del 50% de las maquinas afectadas concentrándose dentro de las regiones del país, siendo la región de Madhya la que tuvo mayor concentración de víctimas con un 32.63% de los ataques siendo reportados desde esa locación. (Savita Mohurle, M. P. 2017, mayo).

Algunas compañías ferrocarrileras en Alemania y Rusia, empresas como FedEx, Nissan, así como departamentos gubernamentales en el Reino Unido fueron gravemente afectadas. Muchas computadoras personales fueron afectadas en escuelas en China. Muchos datos personales e información de las empresas fueron robados o eliminados en el ataque, afectando a las empresas por millones de dolarés. (Savita Mohurle, M. P. 2017, mayo).

Figura 4: Mapa de los ataques registrados sobre Wannacry



Fuente: Jeremy Ashkenas, A. P. (2017).

B. SamSam y la batalla por Atlanta

En el año 2018 la ciudad de Atlanta recibió un paro de actividades repentino. En pocas horas los sistemas administrativos de las diferentes oficinas del ayuntamiento y varios departamentos fueron completamente deshabilitadas por un ataque de *ransomware* ejecutado por el virus SamSam. Los oficiales de policía tenían que organizar su papelería y emitir órdenes a mano y la plataforma de trabajo de la ciudad estaba sin responder. Años de datos acumulados fueron denegados. La nota dejada por el virus pedía cincuenta y un mil dólares para restaurar los sistemas completamente. (Kraszewski, K. 2019, May).

El ayuntamiento solicito ayuda del buró federal de investigación y se le fue recomendado el no pagar el rescate. La ciudad de Atlanta hizo caso a las recomendaciones y prefirió restablecer los sistemas desde cero. Por cinco días la ciudad se quedó sin los servicios previamente mencionados y los costos por la recuperación y reconstrucción de los sistemas rondan alrededor de los doce millones de dólares pudiendo poner a la ciudad de nuevo en labores después de un mes. (James, K. 2019, Jun)

A diferencia de otras formas de *ransomware*, SamSam es dirigido intencionalmente contra un gobierno o sistema de salud como hospitales. Su servicio no se vende en el mercado negro o en foros donde frecuentan los grupos criminales, separándolo de muchos de los *ransomware* más usados. Este programa es resguardado de forma muy íntima por sus creadores, el grupo Gold Lowell. Además, suele ser actualizado frecuentemente para poder pasar desapercibido por los antivirus. (Kraszewski, K. 2019, May).

Su método de ataque ha ido evolucionando con el tiempo. En sus inicios SamSam buscaba vulnerabilidades de versiones desactualizadas de Java. Después cambio a infiltrarse por los protocolos IIS de Microsoft y su transferencia de archivos. Usó también los protocolos de escritorio remoto para poder transferirse sin tener que pasar por el usuario víctima.

Después el grupo se centró en acceder a las redes a través de protocolos de acceso externo por redes privadas virtuales o VPN. La tarifa que se cobraba para descifrar un sistema se establece en alrededor de diez mil dólares, mientras que todos los sistemas en la red se pueden descifrar por cincuenta mil dólares.

El grupo incluso se ofrecía el descifrar un sistema no esencial de forma gratuita para demostrar su capacidad y voluntad de divulgar los datos si se cumplen sus demandas como demostración de que los archivos no estaban perdidos permanentemente y que tenían la posibilidad de recuperarlos. Esto también jugando un papel importante en la manipulación psicológica en contra de la víctima para crear la ilusión de confianza en el grupo criminal. (Kraszewski, K. 2019, May).

C. Baltimore contra RobinHood

Los ataques a sistemas gubernamentales crecieron en uso en los últimos años. Siguiendo el ataque en Atlanta, en mayo del 2019 el *ransomware* conocido como Robinhood atacó la ciudad de Baltimore (Nithya, T., Vijaya, K., Subramanian, D., Balamurugan, E., & Shanmugavel, K, 2020). La oficina de tecnología de la información tuvo que volver a crear alrededor de diez mil credenciales para empleados en turnos dobles diurnos y nocturnos. La red se reestableció solo cuando se reiniciaron los sistemas de uno en uno manualmente. (James, K. 2019, Jun).

Mientras no había datos los residentes no podían realizar operaciones administrativas vía internet y los recibos de los servicios básicos estaban congelados, así como el sistema de multas y cámaras de tránsito. Muchas de las operaciones tenían que realizarse a mano y se guardaron archivos en papel y legajos. (James, K. 2019, Jun).

El FBI volvió a emitir recomendaciones de no pagar el rescate e ignorar las exigencias de los criminales ya que pagando la primera cantidad no hay ninguna garantía de que el grupo no pida más dinero o vuelva a bloquear los sistemas en un futuro. (BBC-News, 2019).

La demanda para el rescate del sistema se estableció en los setenta mil dólares, pero está no fue acatada y se ignoró por parte de la ciudad. Se estima que inicialmente el ataque a la ciudad le costó ocho millones de dólares para poder recuperarse, más la cantidad aumentó a los dieciocho millones de dólares para poder restablecer los sistemas locales. (BBC-News, 2019, James, K. 2019, Jun).

D. Fujifilm bajo ataque de Qbot

Fujifilm es un grupo multinacional enfocado en el desarrollo de diferentes productos médicos de alta tecnología con sede en Japón. El primero de junio del 2021 lanzó un comunicado advirtiendo que habían detectado una entrada no autorizada a uno de sus servidores. Al tomar acciones de emergencia, desconectaron sus servidores y parte de la red que estaba infectada. Esto dejó a múltiples aparatos de la marca sin comunicación ni soporte en hospitales alrededor del mundo, además de dejar a la compañía sin formatos de comunicación ni correos electrónicos aislando a sus empleados y administrativos. (Valdeolmillos, C. 2021).

Un estudio desde la empresa Bleeping Computer, apuntó a que los servidores de Fujifilm fueron atacados con el *ransomware* Qbot y señalaron que el punto de entrada de la infección se dio por un correo malicioso que contenía un mensaje construido con ingeniería social, el cual al engañar a uno de los empleados pudo descargar el virus dentro de la red de la compañía y comenzar a escanear la red y encriptar los archivos iniciales para copiarlos y enviarlos hacia los criminales. (Abrams, L., 2021)

La extracción de datos funciona también como una amenaza a la organización ya que además de bloquear el acceso a ellos para sus empleados puede revelar secretos corporativos o información sensible al público. Afortunadamente la detección fue rápida y se pudo aislar el ataque a las oficinas de Tokio y cortar la comunicación del virus disminuyendo grandemente su funcionalidad ya que no tenía forma de ser controlado o de relegar la información robada. (Fujifilmm, 2021).

Fujifilm no dio ningún comentario sobre si el rescate fue pagado o no, más por la pronta acción que se tomó y lo aislado del incidente, puede ser especulado que ningún recate se pagó y los sistemas fueron reiniciados manualmente. El 4 de junio la empresa pudo restaurar sus redes, servidores y equipo de tecnología médica. Durante el fin de semana pudieron cerrar los demás agujeros de seguridad y el 7 de junio del 2020 finalmente los sistemas administrativos fueron restaurados y la empresa emitió un mensaje sobre sus operaciones volviendo a la normalidad. (Fujifilmm, 2021).

E. El Ministerio del trabajo español

España sufrió una racha de ataques cibernéticos en 2021, habiendo sido afectada por varios frentes. A inicios de marzo se realizó un ataque hacia el servicio público de empleo estatal o SEPE, paralizando por semanas sus sistemas y actividades sin ningún precedente de ese tipo. El mes siguiente a mediados de abril, varios ministerios incluyendo los de justicia, educación, economía y al instituto nacional de estadística fueron infectados y deshabilitados. No hubo datos extraídos y el objetivo principal de los ataques parecía ser el crear daños y caos entre los diferentes ministerios españoles. Los ataques duraron poco más de 12 horas pudiendo reestablecer los servicios al día siguiente. (Otero, C., 2021).

El 9 de junio del mismo año el ministerio del trabajo y economía social fue afectado por un *ransomware* que tuvo un objetivo más concreto que los ataques anteriores. Además de dejar inhabilitado la red y los sistemas, el ministerio dio a conocer por medio de redes sociales que descubrieron una brecha de seguridad importante, una puerta trasera fue abierta, aparentemente por la interacción de un correo malicioso, y dentro del sistema tenía acceso a datos privados, económicos y tenía acceso a tramites del ayuntamiento de los ciudadanos españoles, estos siendo robados para su posterior venta en el mercado negro. (Otero, C., 2021).

A nivel interno el ataque fue categorizado como crítico y se pudo confirmar que el *ransomware* responsable del ataque es el que fue llamado “Ryuk”, virus responsable por ataques en Alemania, China, Argelia y la India. (PandaSecurity, 2020). Aunque el ministerio no declaró si se pagó un rescate, los sistemas volvieron a funcionar en las siguientes 24 horas (Otero, C., 2021).

2. Factores clave para que los ataques se llevaran a cabo con éxito

Leyendo detenidamente los sucesos de los ataques previamente documentados, se pueden destacar un par de prácticas recurrentes. Las maneras en las que los atacantes tuvieron acceso a los sistemas fueron por explotación de vulnerabilidades de los programas o redes de las empresas o por manipulación vía ingeniería social para que les concedieran entrada directa. Por lo tanto, se puede denotar una falta de cultura en las empresas afectadas por parte de la administración y sus empleados.

Un ejemplo muy claro sobre la falta de conciencia y de prevención se puede ver por parte de las compañías en el ataque de Wannacry a nivel global. La agencia de ciberseguridad, infraestructura y seguridad de los Estados Unidos de América había estado siguiendo un rastro sobre el potencial ataque que se realizaría ese mismo año. En su apartado de "Actividad reciente" el cual detalla las vulnerabilidades que están siendo más usadas globalmente por campañas hacktivistas y los descubrimientos más recientes sobre planes de ataques dirigidos o generales, detalló meses antes del ataque como poder protegerse. (Cybersecurity & Infrastructure Security Agency, 2017).

El 16 de enero del 2017, se publicó un boletín titulado "SMB Security Best Practices" o Mejores prácticas para la seguridad del SMB, siendo este el servicio que, si se consultan los detalles del ataque de Wannacry en el tema anterior, se usó para entrar a los sistemas y tomar control de las computadoras. (Cybersecurity & Infrastructure Security Agency, 2017).

En este boletín se detalla que el servicio de SMB está disponible en todos los sistemas Windows y que las versiones de legacía podían permitir a los atacantes realizar infiltraciones maliciosas. Dentro de la sección de recomendaciones se pedía:

- Deshabilitar el SMBv1.
- Bloquear todas las versiones del SMB en la red haciendo un bloqueo directo en los puertos 139 y 445 del servicio TCP, así como los puertos 137 y 138 de UDP, excluyéndolos de todos los dispositivos.

Se advirtió que el realizar estos pasos preventivos podían alzarse problemas como la obstrucción de los servicios de archivos compartidos, acceso a datos entre la red y el control remoto de las computadoras, pero se alentó a las compañías que se evaluará la perdida de esa red o sistema a cambio de la obstrucción de esas características. (Cybersecurity & Infrastructure Security Agency, 2017).

Después de los eventos sucedidos con Wannacry se puede observar que la mayoría de las empresas y organizaciones no estuvieron al pendiente de este boletín o en caso de haberlo consultado, no acataron las recomendaciones por motivos diferentes. La importancia de la consulta sobre el estado actual de amenazas globales es extremadamente grande, ya que los departamentos de seguridad pueden predecir ataques dirigidos a las empresas o campañas masivas que son realizadas en masa.

Ahora el departamento de seguridad de cada empresa es solo el inicio de la cadena de acción de prevención, algo que se verá más adelante en las recomendaciones para la prevención y reacción sobre ataques de *ransomware*. El ecosistema empresarial y organizacional es uno muy complejo, que conforma interacciones individuales realizadas por los empleados y administrativos que residen dentro de él.

En el caso del ataque al ministerio del trabajo en España y de la compañía Fujifilm la infiltración fue provocada por empleados siendo engañados por correos maliciosos e interactuando con ellos. Si los empleados y trabajadores dentro de una organización no conocen los peligros y los métodos de ataques que usan los criminales, estos están expuestos a caer fácilmente en provocaciones o invitaciones falsas dando el acceso a la red, y permitiendo que el atacante pueda robar la identidad del usuario o pueda ejecutar una escala de permisos y comenzar a explorar las ubicaciones de gran importancia.

La falta de conocimiento de las amenazas también puede desembocar en que la víctima no reconozca alguna actividad sospechosa de su computadora o de la red en general, y que no se generé un reporte a tiempo para que pueda ser analizado por el departamento de seguridad o una autoridad competente dándole el tiempo necesario al atacante de planear sus movimientos u ocultar sus rastros.

Parte de la falta de conciencia dentro de la organización va más allá de los empleados, alcanzando niveles altos en las empresas dónde hay puestos administrativos, los cuales pueden dañar la cadena de mando completamente al ignorar reportes importantes por no considerarlos una amenaza o de actividad sospechosa.

Estos puestos, como la gerencia, los líderes de departamentos y los administrativos encargados de la organización suelen ser necesarios para la consulta y la aprobación de actualización de equipo como veremos más adelante. Al no tener participación constante o al no estar bien informada la persona a cargo se pueden tener proyectos e iniciativas frenadas, que pudieron haber detenido un ataque inminente o reducido grandemente las consecuencias y perdidas posteriores al incidente.

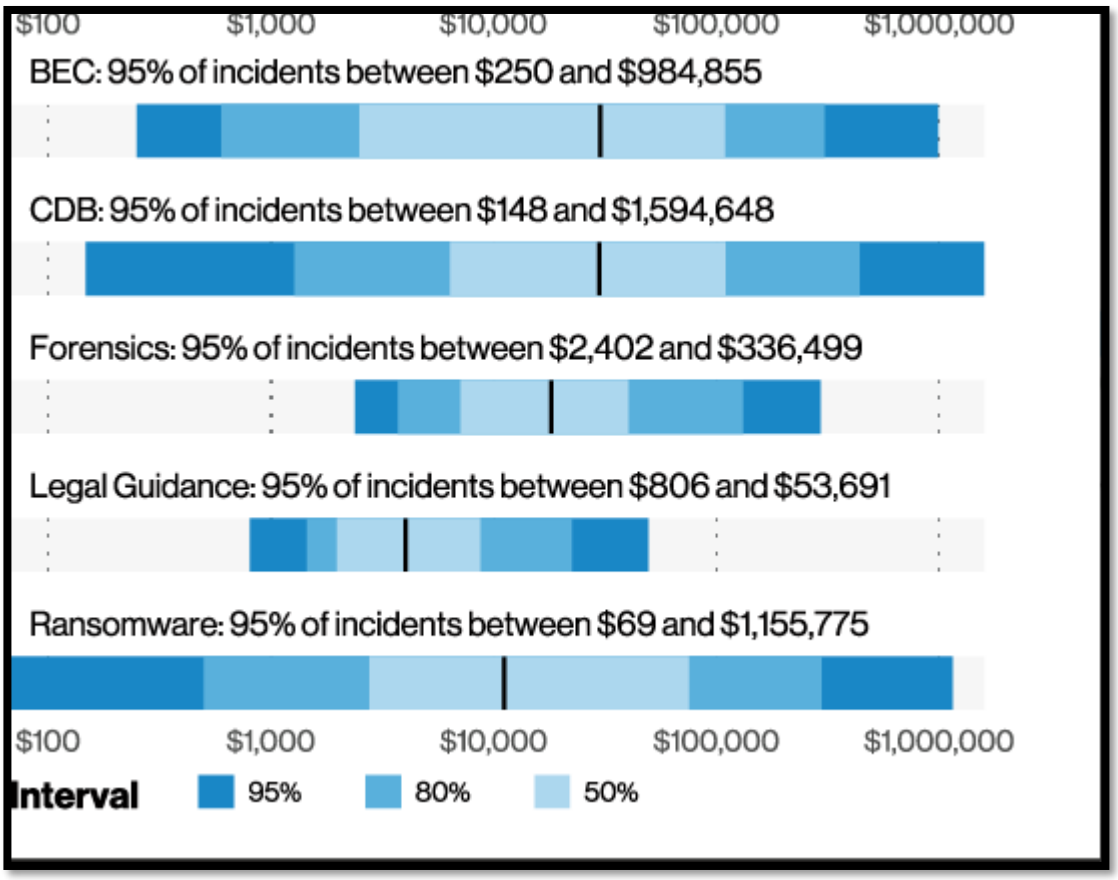
Más de diez por ciento de la actividad criminal y las violaciones de datos fueron por causa de *ransomware* en el año 2020, siendo solo superadas por los ataques efectuados puramente por ingeniería social y siendo el de los más usados los ataques *DDoS* los cuales son de saturación de tráfico para alentar sistemas y sobrecargar

servidores. Siendo el porcentaje de ese año correspondiente al *ransomware* el doble del año que le antecede en el 2019, dando un salto significativo en número y dando indicios de tener una expansión exponencial. (Ikeda, 2021).

Según el informe sobre las violaciones de datos de Verizon, hubo una importante subida en el porcentaje de ataques de *ransomware* usando ingeniería social, aumentando del veinticinco por ciento en el 2019 a un preocupante treinta y seis por ciento en el año del 2020 (Verizon, 2021). Se esperaba esté aumento de ataques combinados de *ransomware* con phishing (ingeniería social manipuladora) por los esquemas de trabajo en casa que se comenzaron por causa de la pandemia del COVID-19. (Ikeda, 2021).

El informe de Verizon también encuentra que el costo medio de la violación es de veintiún mil dólares en promedio, pero se espera que la mayoría de las organizaciones aumenten el costo de la reposición de los ataques hasta aproximadamente seiscientos cincuenta mil dólares yendo de la mano con el aumento de los ataques. (Ikeda, 2021).

Figura 5: Intervalos de costos sobre incidentes.



Fuente: Verizon, (2021).

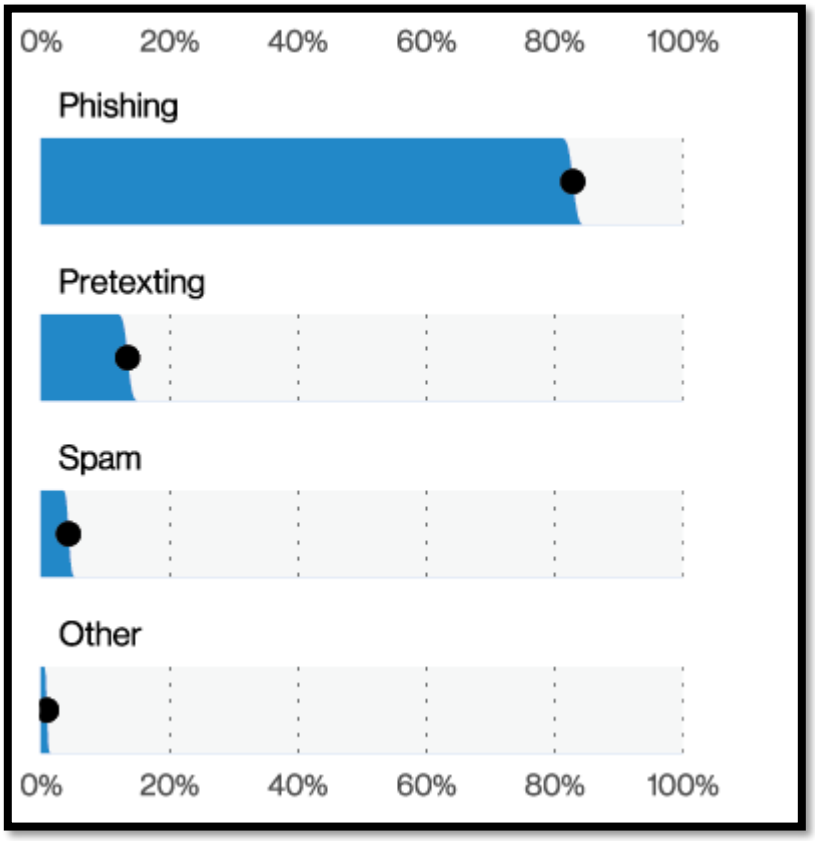
Los intentos de ingeniería social han ido en aumento desde 2017, estos ataques generalmente son impulsados por *botnets*, las cuales son redes de programas que automáticamente mandan y administran correos maliciosos y las organizaciones pueden esperar entre cientos y miles de millones de este tipo de intentos cada año, dependiendo de qué tan interesantes sean el objetivo para los delincuentes. (Ikeda, 2021).

Los ciberdelincuentes están desarrollando sus ataques de ingeniería social a través de medios creativos y esto es particularmente enfocado en la categoría de *ransomware*.

El 99% de los ataques de *ransomware* observados por el informe fueron clasificados como "complejos" por el equipo de DBIR, lo que significa principalmente que involucraron programas maliciosos hechos específicamente para el objetivo o ataques no automatizados, donde el atacante estaba personalmente monitoreando y realizando comandos. Este es un cambio importante con respecto a los patrones originales de *ransomware*, donde se utilizó un enfoque de esparcir masivamente sin objetivos claros para observar resultados extensos, pero con pocos que caían en las trampas impulsado por las redes de *bots*. (Ikeda, 2021).

Las bandas de *ransomware* ahora se enfocan más cuidadosamente en objetivos que creen que tienen la capacidad y la voluntad de realizar grandes pagos y que no tienen la seguridad cibernética o cultura de seguridad adecuadas. Su éxito continuo en la extorsión de víctimas en todo el mundo ha proporcionado a estas operaciones criminales presupuestos superiores a la mayoría de las organizaciones a las que atacan, superando defensas antiguas o programas obsoletos, Incluso yendo mano a mano con las defensas automáticas y pudiendo sostener los ataques por largos periodos de tiempo intentando por diferentes medios (Verizon, 2021). (Ikeda, 2021).

Figura 6: Métodos más usados de ingeniería social.



Fuente: Verizon (2021).

También se señala que diferentes industrias están viendo diferentes patrones de intentos. Por ejemplo, el sector de la educación es un blanco desproporcionado de estafas de ingeniería social que tienen como objetivo final transferencias fraudulentas de fondos. La administración pública también ve una cantidad desproporcionada de intentos de ingeniería social, pero la mayoría de ellos involucran un correo electrónico de phishing directo. Y, como lo ilustró el incidente de Colonial Pipelines que se vio con anterioridad, la minería y los servicios públicos se están convirtiendo rápidamente en un objetivo principal para los grupos de *ransomware*. Todo esto sugiere que los atacantes se están

volviendo mucho más discriminatorios y centrados en objetivos particulares (Krauss, 2021). (Verizon, 2021).

III. EL ESTADO DE CULTURA Y CONCIENCIA EMPRESARIAL

1. La cultura de la seguridad.

Como se vio en el capítulo anterior, un factor crucial para la seguridad de cualquier sistema o red por más automatizado que se encuentre es el factor humano. El ecosistema empresarial y la cultura que tiene dentro de él es un elemento base que desprende de sus raíces los comportamientos principales que siguen los empleados en su día de trabajo y en su encuentro con las amenazas que rodean el ambiente.

El factor humano representa a la parte más débil dentro de la seguridad informática, se dice que las personas pueden no seguir instrucciones o recomendaciones tal y como fueron dictadas, esto se suma a las malas prácticas que se emplean, tales como dejar contraseñas a la vista pública, en notas físicas o de fácil acceso en el ordenador y dejar las credenciales por defecto de los programas y cuentas utilizados (muchos de ellos de conocimiento público en la red como las contraseñas y usuarios predeterminados de los enrutadores). Además de esto pueden llevar a cabo acciones que puedan facilitar los ataques de los hackers hacia sus redes, por ejemplo, pueden realizar una instalación de un software malicioso en el ordenador, en donde pueden ingresar a información sensible de la empresa.

Sabemos que podemos contar con soluciones inteligentes como son las herramientas diseñadas especialmente para salvaguardar información de la empresa en caso de incidentes, con esto tenemos cubierto gran parte de las vulnerabilidades que se puedan presentar inesperadamente, pero no siempre se cuenta con personal capacitado para manejar dichas herramientas o los recursos y el apoyo para obtenerlas. Con esto podemos resaltar que existe una parte critica dentro de la seguridad de la empresa y eso son nuestro capital humano.

Aunque se cuente con ambientes laborales exóticos donde la presencia humana es reducida, siempre hay un elemento humano a cargo de algún puesto o responsabilidad. Este elemento humano puede encontrarse proporcionando soporte, mantenimiento o

administración a los trabajos y herramientas digitales que se usan en las organizaciones hoy en día.

Una herramienta muy común que se encuentra en las organizaciones y empresas es la computadora, es un elemento que se ha convertido en un cimiento para los modelos de negocio actuales y que es muy usado en todo tipo de ámbitos además de ser el punto de control en la interacción personal de un empleado con la información de la organización. Tomando en cuenta la pandemia de COVID-19 del año 2020, el uso de la red local del hogar, así como de herramientas adicionales a la computadora como dispositivos móviles personales aumentó en gran manera, ya que el modelo de trabajo en casa da la oportunidad de integrar esto a las actividades del personal de la empresa.

Una de las mayores amenazas que se presentan hoy en día es el ataque por medio de redes sociales, una vez que infectan a una víctima los hackers bloquean las aplicaciones, secuestran la información y acceden a las cuentas personales de correo electrónico y redes sociales, robando la identidad del usuario y usando eso para enviar mensajes con ligas o archivos maliciosos a sus contactos.

Los atacantes saben poner trampas de ingeniería social a los usuarios que se olvidan de proteger sus ordenadores, móviles y tabletas. Se dice que la mayoría de los usuarios utilizan dispositivos móviles de la empresa para acceder a su correo, los cuales también usan para acceder a redes sociales, compartiendo en un dispositivo las credenciales de su ambiente personal y laboral. Sabemos que la mayoría de las personas no acostumbran a proteger sus dispositivos móviles por ser un ambiente no tan comúnmente conocido por ser atacado entre los usuarios, siendo esto algo falso ya que son dispositivos extremadamente vulnerables ante los ataques e infecciones de *malware*. Esta falta de conocimiento los hace más vulnerables antes cualquier ataque.

Considerando que los empleados son el primer nivel de interacción entre la empresa y sus activos digitales, estos se convierten en el objetivo principal de cualquier ataque, ya que la forma más simple de obtener acceso a una red o sistema es obteniéndolo directamente de la persona que ya se encuentra conectada a él o que tiene conocimientos de sus credenciales. Esto evita que el hacker o grupo criminal inviertan muchos recursos en intentar burlar la seguridad que se tenga implementada.

Es importante para las empresas, como se menciona en el capítulo anterior, que sus empleados tengan un conocimiento de las buenas prácticas y una conciencia sobre las amenazas que rodean su área de trabajo y de la organización. Para poder entender mejor como se encuentra la cultura en las empresas en un ámbito internacional se consultó el “Reporte de conciencia de seguridad de la SANS”.

El reporte indica que los programas de concientización de seguridad han evolucionado de tener un nivel bajo de competencia a ser una parte clave de la habilidad que puede tener una empresa para administrar sus recursos humanos ante un riesgo cibernético. Aún y con este aumento significativo de importancia sobre los programas internos, hay muchos retos que aún no se han conseguido superar para poder logar que este tipo de cultura sea implementada correctamente en las empresas. (SANS Security Awareness, 2021).

Según los datos reportados, más del setenta y cinco por ciento de los profesionales de la conciencia de seguridad dedican menos de la mitad de su tiempo a desarrollar e implementar sus programas de concientización, lo que implica que la conciencia es a menudo menos que una prioridad para estos profesionales. Las organizaciones que informan un éxito que va más allá del cambio de comportamiento y que logra impactar en la cultura de sus empleados, informan que tienen al menos tres personales especializados dedicados a la concientización de seguridad. (SANS Security Awareness, 2021)

La clave para gestionar los riesgos del factor humano no es la cantidad de presupuesto puramente que se les da a los esfuerzos de concientización en sí. Es mucho más efectivo si se hacen inversiones a largo plazo hacia los profesionales y los empleados en general, así como se hacen inversiones en administración de vulnerabilidades o lo centros de operaciones de seguridad. (SANS Security Awareness, 2021)

La mayoría de los líderes de conciencia de seguridad muy comúnmente tienen un historial de preparación técnico y carecen de habilidades sociales como comunicaciones y publicidad, solo muy pocos individuos (alrededor de un veinte por ciento) tienen una preparación no técnica como recursos humanos o en departamento legal, lo que limita la capacidad de las organizaciones para involucrar eficazmente a su fuerza laboral a los

programas de concientización con términos simples y fáciles de entender para los empleados que no tienen esa preparación técnica. (SANS Security Awareness, 2021)

Figura 7: Mapa de los países participantes en los análisis SANS.

Fuente: SANS Security Awareness (2021).

2. El modelo de madurez de la conciencia de seguridad

Establecido en 2011 a través del esfuerzo concertado de más de 200 oficiales de concientización, el "*Security Perception Maturity Model* ™" permite a las organizaciones identificar y evaluar la madurez actual de su programa de conciencia y cultura. su conciencia de seguridad e identificar vías de mejora. Los programas de concienciación sobre seguridad más exitosos y maduros no solo cambian el comportamiento y la cultura, sino que también pueden medir y demostrar su valor a través de un marco de medición. (SANS Security Awareness, 2021).

La mayoría de las empresas sí cuentan con un programa de seguridad, y tienen planes para prevención de incidentes, pero hay una gran cantidad de organizaciones que tienen esos programas mal configurados o paneados, ya que las herramientas

digitales pueden ser instaladas con parámetros por defecto, sin cumplir con las necesidades y riesgos que enfrentan, muchas de ellas dejándose sin mantenimiento o en sistemas desactualizados.

Muchas soluciones de seguridad digitales están obsoletas en lo que respecta detección de incidentes y dejan de ser útiles en contraste de los programas maliciosos que siguen evolucionando para encontrar vulnerabilidades y nuevas formar de afectar a sus víctimas.

Los planes de seguridad y conciencia, por falta de conocimiento pueden ignorar también las verdaderas necesidades de sus empleados y de sus organizaciones, dejando una mala impresión y rechazo de parte del demográfico objetivo. Por eso el modelo de percepción de madurez de la seguridad describe los siguientes niveles del programa de concientización ya que con el mismo se puede tener una evaluación detallada del estado actual de la seguridad y su cultura dentro de la empresa:

i. **Inexistente**: No existe un programa de concientización sobre seguridad en ningún nivel ni capacidad. Los empleados no tienen idea de que son un objetivo potencial a alguna amenaza o que sus acciones tienen un impacto directo en la seguridad de la organización. No conocen ni siguen las políticas de la organización y fácilmente son víctimas de ataques e ingeniería social. (SANS Security Awareness, 2021).
ii. **Enfocado en cumplimiento**: El programa está diseñado principalmente para cumplir con requisitos específicos de una auditoría, requerimiento gubernamental u organizacional. La formación se limita a ser enseñada anualmente o según las previas necesidades. Los empleados no están seguros o no entienden de las políticas de la organización y / o de su papel en la protección de los activos de información de su organización. (SANS Security Awareness, 2021).
iii. **Promoción de la conciencia y el cambio de comportamiento**: El programa identifica los grupos críticos para la empresa y los temas de capacitación que tienen el mayor impacto en la administración del riesgo humano y, en última instancia, en el avance a la misión de la organización al mismo tiempo. El programa va más allá de la capacitación anual e incluye un refuerzo continuo

durante todo el año, así como dinámicas y actividades regulares. El contenido se comunica de una manera atractiva y positiva que fomenta el cambio de comportamiento y hábitos. Como resultado, las personas comprenden y siguen las políticas de la organización y reconocen, previenen e informan activamente los incidentes entre ellos y a sus superiores. (SANS Security Awareness, 2021).

iv. **Sostenibilidad a largo plazo y cambio de cultura**: El programa cuenta con los procesos, los recursos y el apoyo completo de la administración para un ciclo de vida a largo plazo, que incluye como base una revisión y actualización anual del programa. El programa es una parte establecida de la cultura de la organización siendo actual y atractivo para sus empleados. El programa ha ido más allá de cambiar el comportamiento y está cambiando las creencias, actitudes y percepciones de seguridad de las personas creando una cultura saludable de conciencia dentro de la organización. (SANS Security Awareness, 2021).

v. **Marco de métricas**: El programa que se ha creado tienen un marco de métricas sólido, bien implementado y claro hacia todos los perfiles de personas, además de estar alineado con la misión de la organización. Este programa cumple con un objetivo de rastrear el progreso y medir el impacto periódicamente. Como producto de todo esto, el programa mejora continuamente y puede demostrar resultados devolviendo la inversión de la empresa y el nivel administrativo. Las métricas son una parte importante de cada etapa, y este nivel simplemente refuerza la idea de que, para tener un programa realmente maduro, debe poder demostrar valor y seguridad a la organización.

La mitad de las organizaciones internacionales encuestadas (con un cincuenta y tres por ciento) responden que su empresa queda exactamente en el nivel medio, el de promover conciencia y cambio del comportamiento (SANS Security Awareness, 2021). Esto revela que la mayoría de las empresas todavía están bajo el proceso de educar a las personas dentro de ellas, aunque su programa acaba de alcanzar una madurez mediana que ya hace más sencillo el poder transmitir la información de seguridad y las buenas prácticas, todavía se considera en formación de la cultura y no algo completamente permanente que aún necesita trabajarse.

Considerando que de los encuestados solo el treinta por ciento se considera (tomando la opinión de la empresa) por encima del tercer nivel de madurez, esto deja alrededor de un preocupante veinte por ciento de empresas internacionales que están por debajo de un nivel que promueve una cultura de seguridad y la hace parte de su ecosistema laboral, lo que afecta directamente las oportunidades que tienen las campañas criminales cibernéticas de tener éxito.

Dentro de este nivel de madurez bajo, se refleja la falta de atención y recursos por parte de las empresas hacia el tema de seguridad, omitiendo roles empresariales que den mantenimiento y auditoria a los programas y teniendo una falta de políticas que ayuden al mantenimiento del ecosistema empresarial y la continuidad de sus operaciones junto con la integridad de sus activos, así también como la de sus empleados. Las políticas, dictan la forma de actuar y son la estructura base para que haya una guía desde el nivel administrativo y gerencial hacia dentro de sus propias áreas y del ambiente adyacente a ellas.

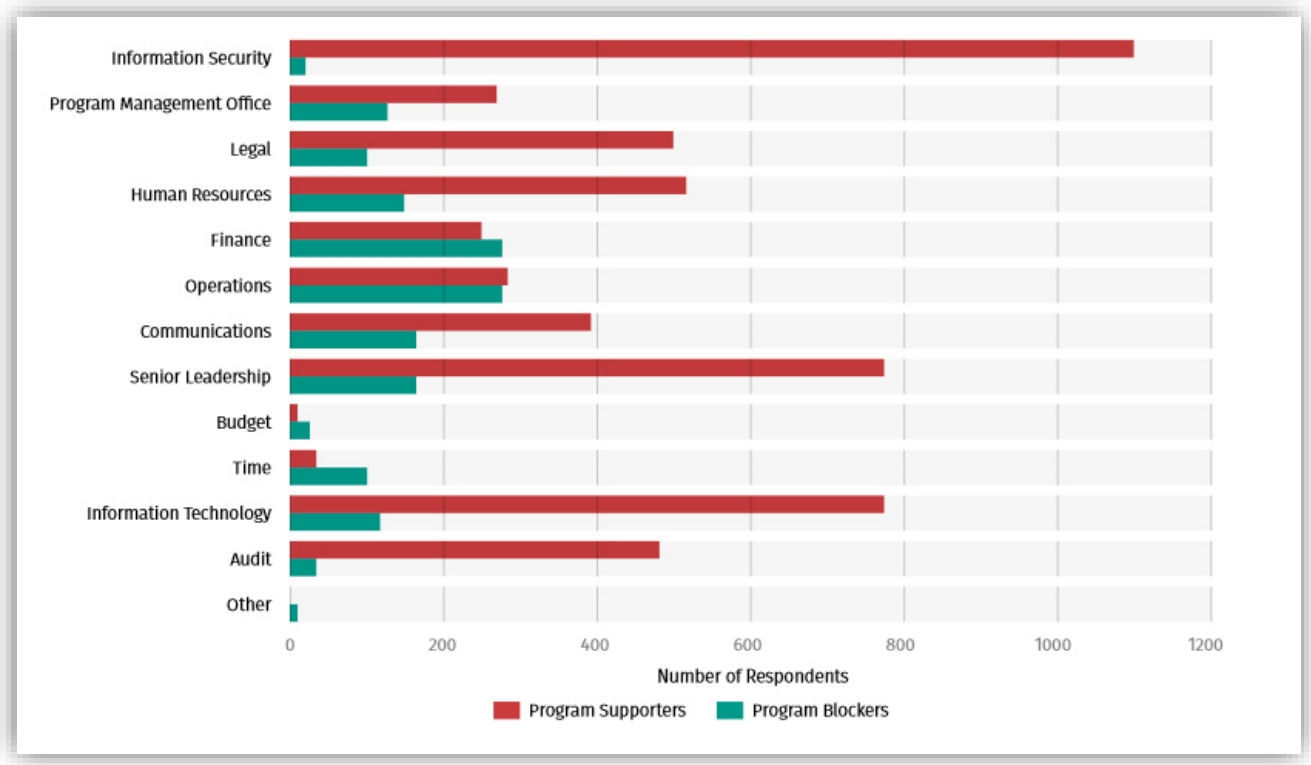
3. Apoyo empresarial y dedicación a la cultura

Un factor clave del éxito para un programa de concientización con nivel de madurez alto es una convivencia interna sólida y una relación de trabajo en equipo entre departamentos críticos dentro de la organización. Los programas de concientización generalmente reciben un fuerte apoyo de los departamentos como seguridad, tecnología de la Información, recursos humanos y auditoría, así como de la alta dirección. Estos diferentes departamentos y áreas a menudo proporcionan apoyo, aprobación o recursos para permitir la ejecución del programa de conciencia y su ciclo de vida, así como su renovación. Normalmente la alta dirección suele ser un desafío para los equipos encargados del programa de conciencia, ya que al ser personas que no están acostumbradas a ver ese tipo de conceptos y temas no pueden comprender la mayoría del tiempo la gravedad de las advertencias o la importancia de las peticiones sobre la mejora de la cultura. (SANS Security Awareness, 2021).

En contraste, los programas de concientización también deben trabajar con departamentos que restringen su capacidad de ejecución, a los que el reporte llama como bloqueadores. Muchos programas informaron que los departamentos de

operaciones y finanzas son bloqueadores comunes. Debido a que la mayoría de los programas de concientización tienen un impacto presupuestario y operativo significativo a corto plazo, así que suelen oponerse a los cambios más radicales, aunque sean necesarios, ya sea por falta de comunicación clara de parte de los equipos y departamentos a cargo de presentar y construir el programa; por falta de la propia concientización o cultura dentro de los bloqueadores o por agendas empresariales estrictas que se oponen al plan propuesto. (SANS Security Awareness, 2021).

Figura 8: Bloqueadores comunes.

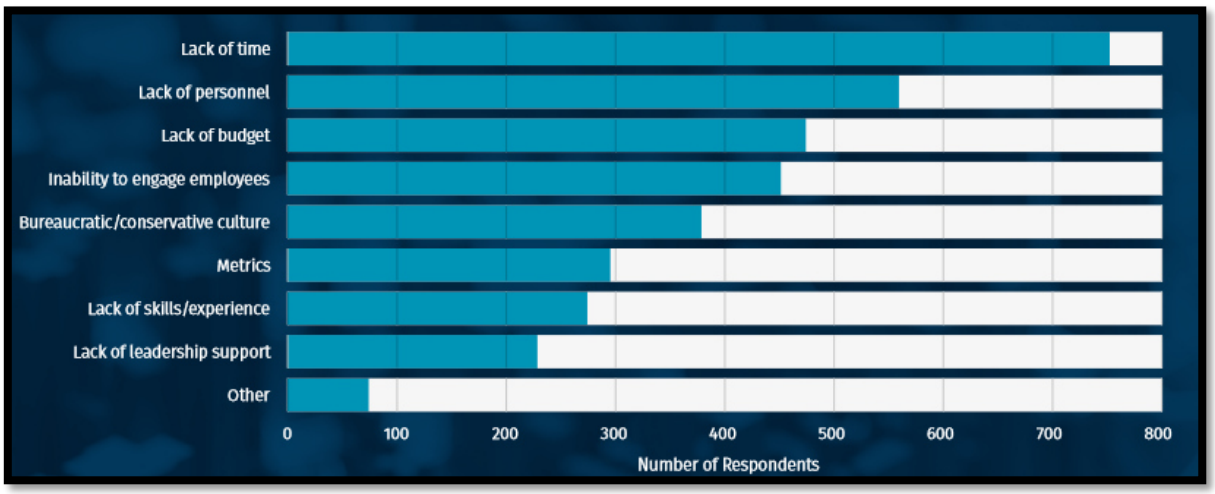


Fuente: SANS Security Awareness (2021).

4. Problemas con el tiempo de conciencia

Los dos principales desafíos reportados para construir un programa de concientización maduro por parte de la administración y los altos mandos fueron la falta de tiempo para administrar el programa y la falta de personal para trabajar e implementarlo. Otros factores entraron como elementos que perjudican los esfuerzos de los programas tales como la falta recursos y el poco interés de los empleados hacia los mismos, este último reflejando la falta de conciencia que se tiene dentro de la empresa. En cuanto a los desafíos principales más del ochenta por ciento de los profesionales de la conciencia de la seguridad informaron que dedican la mitad o menos de su tiempo al desarrollo de conciencia de la empresa, lo que indica que con demasiada frecuencia la conciencia de la seguridad es un esfuerzo de medio tiempo.

Figura 9: Desafíos principales para desarrollar programas de conciencia.



Fuente: SANS Security Awareness (2021).

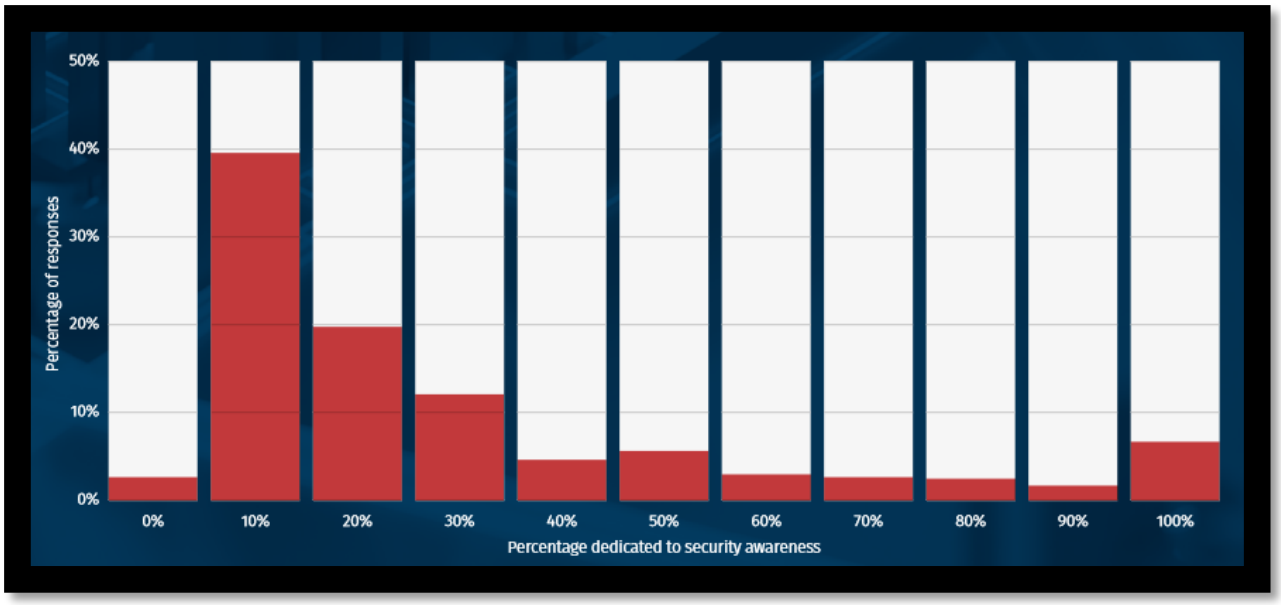
Para tener una mejor comprensión de cuántas personas se necesitan para construir y mantener un programa de concientización maduro, en el reporten utilizaron

“Equivalentes de tiempo completo” (FTE) como medidas. Un FTE equivale a la unidad de tiempo que una persona le dedica a una actividad, por ejemplo, si tiene tres personas que dedican la mitad de su tiempo (un cincuenta por ciento de su tiempo total) a su programa de concientización, eso equivaldría a “punto cinco” multiplicado por tres, lo que totalizará uno punto cinco de FTE dedicados a su programa de concientización.

Los datos de la encuesta revelaron una fuerte correlación entre la cantidad de personas dedicadas a ejecutar un programa de concientización y la madurez del programa en sí e indicaron una relación lineal entre los dos. Hacer crecer un programa maduro más allá del tercer nivel, el cual describe el cumplimiento de reglamentos de seguridad nacionales e internacionales sin una cierta cantidad de personal a tiempo completo es una tarea muy complicada que suele dejar programas inconclusos y muchas veces rezagándose a un nivel de madurez inferior, por lo que se debe considerar aumentar la dotación de personal y su tiempo, alineándolos con los objetivos de madurez.

La cantidad de FTE requeridos suele variar, no solo con el tamaño de la fuerza laboral, sino también con la complejidad y diversidad de un programa de concientización, esto siendo construido desde las necesidades de la empresa. Si bien un programa de concientización básico que cubra la capacitación esencial para una gran empresa puede requerir más personal a medida que crece el tamaño de la organización, las empresas que cuenten con diversas necesidades de capacitación, los programas de concientización regional que involucran múltiples unidades de negocios y centros de trabajo, idiomas, etc., van a requerir de mucho más personal y tiempo.

Figura 10: Tiempo dedicado a la conciencia y cultura de seguridad.



Fuente: SANS Security Awareness (2021).

Los datos indican que las organizaciones más grandes tienen más FTEs, llegando a los cuatro y medio FTE de tiempo en las empresas con más de doscientos cincuenta empleados, y no solo por tener la mayor fuerza laboral, sino porque a menudo están haciendo más cambios dentro de su programa, como esfuerzos de participación más diversos, informes de métricas avanzadas, ejercer múltiples eventos de conciencia de seguridad y programas de embajadores donde hay intercambios de información entre empresas.

Se puede observar de los datos anteriores que hubo un incremento ligero en la madurez de las empresas a nivel internacional, esto no logra ser suficiente con la velocidad a la que evolucionan los métodos y la escala de los ataques cibernéticos en el mundo. Las empresas comienzan a tener incrementos de personal o crecimiento patrimonial y no enfocan sus esfuerzos en blindar ese crecimiento dado. El tiempo y los métodos que se deben de invertir en dar conciencia y voz a las personas dentro de la

organización, así como el mantenimiento de los programas y sus máquinas debe de seguir un crecimiento exponencial dependiendo del tamaño y de las operaciones de la empresa. Se verá en el siguiente capítulo como se puede actuar y prevenir los ataques de ingeniería social junto con los virus *ransomware* e incrementar el nivel de conciencia, mantenimiento y seguridad en un ecosistema laboral.

IV. LOS ESFUERZOS GLOBALES CONTRA LA INSEGURIDAD Y EL FORTALECIMIENTO DE LA CULTURA

1. Prevención contra el ransomware

Alrededor del mundo las agencias y departamentos de inteligencia de la seguridad han estado trabajando arduamente para el tener bajo vigilancia el ambiente cibernético, esto para poder prevenir cualquier ataque o movimiento sospechoso de parte de los grupos criminales reuniendo información de descubrimientos recientes e historial previo sobre los incidentes que se han dado. Desde que el *ransomware* comenzó a tener popularidad diferentes organismos han comenzado a estudiar el modo de operar de este programa malicioso y han dado recomendaciones técnicas y culturales sobre cómo se puede actuar parar evitar la infección de los sistemas, así como las acciones para poder salir de un incidente de *ransomware* de forma segura.

Entonces ¿Qué debe hacer si las computadoras de la empresa muestran un reloj de cuenta regresiva y un mensaje amenazante que indica que los archivos han sido encriptados y que se perderán permanentemente a menos que un rescate sea pagado en una fecha y hora específicas? Los datos encriptados son de vital importancia para una pequeña empresa, un hospital, o un gobierno, así que es muy importante el estar preparados para los ataques de *ransomware*. (NIST, 2021).

El seguir constantemente las diferentes firmas de seguridad y las agencias internacionales proporciona un nivel de preparación extenso para poder frenar cualquier riesgo potencial en el futuro cercano y tener información confiable que puede ser usada por los equipos de seguridad y de cultura para armar sus programas de detección, prevención y concientización con mayor efectividad (CISA, 2021).

A. Agencia de Seguridad en Infraestructura y Ciberseguridad

La CISA, por sus siglas en inglés, es una agencia estadounidense que se enfoca en métodos para defender la nación de los ataques cibernéticos y trabaja con el gobierno federal para proporcionar herramientas de seguridad cibernética, servicios de respuesta a incidentes y capacidades de evaluación para salvaguardar las redes con terminación ".gov" que respaldan las operaciones esenciales de los departamentos y agencias asociados del gobierno. Sus actividades cubren desde ayudar a asegurar la cadena de suministro de COVID-19 hasta apoyar elecciones libres y justas. (CISA, 2021).

Se coordinan los esfuerzos de seguridad y resiliencia utilizando asociaciones confiables en los sectores público y privado, y brinda asistencia técnica y evaluaciones a las partes interesadas federales, así como a los propietarios y operadores de infraestructura en todo el país. La CISA también ofrece información sobre evaluaciones relacionadas con las capacidades actuales para identificar brechas de seguridad, que, junto con un examen de las tecnologías emergentes, ayudan a determinar las acciones que se deben de tomar para evitar riesgos futuros. (CISA, 2021).

El Centro Nacional de Gestión de Riesgos (NRMC) se encuentra dentro de la CISA y este actúa como un centro de planificación, análisis y colaboración que trabaja para identificar y abordar los riesgos más importantes para la infraestructura crítica de las operaciones nacionales. También se trabaja en estrecha coordinación con el sector privado y otras partes interesadas clave en la comunidad de infraestructura crítica para identificar, analizar, priorizar y gestionar los riesgos más estratégicos del país

La CISA constantemente realiza seguimiento del comportamiento del ecosistema cibernético y sus amenazas, publicando sus estudios y descubrimientos sobre el *ransomware*. Se tiene un catálogo extenso sobre las modas actuales de los grupos de criminales cibernéticos y sus agendas así de como poder evitar sus campañas de hackeo o como estar preparado para su llegada. (CISA, 2021).

Figura 11: Sección de alertas y consejos sobre *ransomware* de la CISA.

RANSOMWARE ALERTS AND TIPS

- Current Activity: Update to CISA-FBI Joint Cybersecurity Advisory on DarkSide Ransomware
  - On May 19, a downloadable STIX file of indicators of compromise (IOCs) was added to the advisory to help network defenders find and mitigate activity associated with DarkSide ransomware.
- Alert (AA21-131A): DarkSide Ransomware
  - CISA and FBI are aware of a ransomware attack affecting a critical infrastructure (Cl) entity-a pipeline company-in the United States. Malicious cyber actors deployed DarkSide ransomware, a ransomware-as-a-service (RaaS) variant, against the pipeline company's information technology (IT) network. This joint advisory provides technical details on the DarkSide actors, some of their known tactics and preferred targets, and recommended best practices for preventing business disruption from ransomware attacks.
- Analysis Report (AR21-126A): FiveHands Ransomware
  - Recently, threat actors successfully launched a cyberattack against an organization using a new ransomware variant, which CISA refers to as FiveHands. The actors used publicly available penetration testing and exploitation tools, FiveHands ransomware, and SombRAT remote access trojan (RAT), to steal information, access credentials, obscure files, and demand a ransom from the victim. In addition to mitigation recommendations, this report provides the tactics, techniques, and procedures the threat actors used as well as indicators of compromise (IOCs).
- Alert (AA21-076A): TrickBot Malware
  - CISA and FBI have observed continued sophisticated spearphishing campaigns using TrickBot malware in North America. Cybercrime actors are luring victims, via phishing emails, with a traffic infringement phishing scheme to download TrickBot, a Trojan first identified in 2016. Attackers can use TrickBot to drop other malware, such as Ryuk and Conti ransomware, or serve as an Emotet downloader.
- Current Activity: SMB Security Best Practices
  - In response to public reporting of a potential Server Message Block (SMB) vulnerability, US-CERT is providing known best practices related to SMB. This service is universally available for Windows systems, and legacy versions of SMB ·otocols could allow a remote attacker to obtain sensitive information from affected systems. The Current Activity ·les recommendations for users and administrators.

Fuente: CISA (2021)

Esta organización ha establecido varias recomendaciones para ayudar a complementar y mejorar la cultura de seguridad en las empresas, así como para fortalecer sus redes y estaciones de trabajo. La CISA y el FBI apoyan varios tipos diferentes de protección para reducir el riesgo de que los ataques de *ransomware* y que estos sean exitosos. (CISA, 2021).

El uso de la autenticación multifactor para el acceso remoto a redes y equipo de trabajo agrega una capa adicional al proceso de ingreso de credenciales. La

autenticación multifactor puede enviar peticiones de confirmaciones a los dispositivos que hayan sido configurados para que en caso de que se intente un ingreso de credenciales se mande un mensaje de aprobación hacia el usuario que tenga el dispositivo físico y evitar el acceso desde otra unidad digital. (CISA, 2021).

El habilitar filtros de spam, estos detectan títulos y contenido sospechosos dentro de los correos e implementarlo en los servicios de correo electrónico de la empresa puede evitar que los correos de suplantación de identidad y phishing lleguen a los empleados y administradores. Se pueden filtrar correos maliciosos que contienen archivos ejecutables o de otro tipo de extensión como las de Office, para lo cual se puede deshabilitar la ejecución de macros. Estos filtros pueden dejar los correos para que sean analizados por separado y el personal pueda interactuar con los archivos correctos. (CISA, 2021).

Se recomienda implementar un programa de capacitación de usuarios y ataques simulados para disuadir a los usuarios de visitar sitios maliciosos o abrir archivos adjuntos que sean sospechosos, así como reforzar las respuestas apropiadas de los usuarios a los correos electrónicos de ingeniería social y manipulación personalizada. (FBI, 2019)

Una implementación de alcance mayor dentro de la empresa es la filtración del tráfico de la red para prohibir las comunicaciones de entrada y salida de las direcciones IP maliciosas que sean conocidas por la empresa o por alguna firma de seguridad. Esto puede funcionar complementariamente con un conjunto de políticas de seguridad que ayuden a los usuarios a evitar el acceder a sitios maliciosos dentro de internet mediante la implementación de listas de bloqueo y listas de permisos de URL y DNS. (CISA, 2021).

Como se pudo observar en los casos de ataques que aprovechan las explotaciones de programas desactualizados, el dejar mucho tiempo el equipo de la empresa y su software obsoleto es un riesgo muy grande que puede desembocar en ataques agresivos. Se debe actualizar constantemente los sistemas operativos, las aplicaciones y el firmware de los activos de la red dentro de la organización, de manera constante y periódica. La CISA junto con el FBI recomiendan el uso de sistemas de administración de parches centralizados, estos pueden ayudar a administrar y calendarizar las actualizaciones de drivers y otros programas. (CISA, 2021).

La correcta configuración de los programas antivirus es importante para realizar análisis periódicos de los activos de la red de utilizando firmas de *malware* actualizadas. Las licencias de estos programas antivirus deben conservarse activa y renovarse de forma inmediata, ya que estos programas pueden dejar de funcionar completamente al dejarse con versiones de prueba. Una consideración útil, es usar el software "Office Viewer" para abrir archivos de Microsoft Office transmitidos por correo electrónico en lugar de descargarlos y abrirlos en las aplicaciones de Office de escritorio. (CISA, 2021).

En conjunto con las listas de IP permitidas, la implementación de listas de permisos de aplicaciones, que solo permiten a los sistemas ejecutar programas conocidos y autorizados por políticas de seguridad ya establecidas (como las listas de restricción SRP) pueden evitar que los programas se ejecuten desde ubicaciones comunes usadas por programas *ransomware*, como carpetas temporales dentro de los programas de navegación de internet o programas de compresión como los ZIP, así como carpetas comúnmente usadas, incluida la carpeta "AppData". (CISA, 2021).

Una de las recomendaciones más efectiva es la de realizar respaldos de seguridad de la información crítica de los sistemas. Las copias de seguridad pueden ayudar a restaurar datos cruciales para seguir las operaciones ininterrumpidamente, así como también pueden minimizar la pérdida neta de información en caso de un ataque *ransomware* (FBI, 2019). Estas copias deben ser probadas periódicamente para que se asegure su funcionamiento, ya que los respaldos pueden ser corrompidos inesperadamente. El tener un respaldo que no esté conectado a la red o directamente dentro de la computadora o sistema es imperativo ya que muchos programas de *ransomware* pueden encriptar todos los dispositivos de almacenamiento que encuentren dentro de su alcance. (CISA, 2021).

Además de tener respaldos listos para ser activados se debe tener un plan de continuación de negocio bien elaborado para que las operaciones de la organización no sean afectadas por los métodos de recuperación en caso de un incidente. Esto en conjunto con un horario de cambio de credenciales, así como periódicamente administrar un cambio de las contraseñas y el evitar su repetición entre cuentas ayuda a que cualquier información que haya sido robada por el ataque pueda quedar inutilizada si no

se usa rápidamente lo cual pone en un lugar vulnerable a los atacantes ya que no tienen tiempo de explorar y cubrir sus huellas. (CISA, 2020).

Las auditorias de las cuentas de usuario con privilegios administrativos, así como el uso y roles que desarrollan da información importante para saber en qué estado se encuentra la información de sus credenciales y el riesgo que pueden tener al ser objetivos de un ataque. Las cuentas y sus permisos trabajan de manera más efectiva y segura siguiendo la regla de "*least privilege*" o privilegios mínimos, la cual toma en cuenta que permisos son completamente necesarios para los roles de una cuenta y otorgarlos estrictamente sin ningún otro permiso adicional. (CISA, 2020).

Las auditorias deben también incluir los registros de cuentas que existen en el tiempo de la revisión, asegurando que todos los roles y usuarios son legítimos, ya que muchos primeros pasos de ataques cibernéticos se centran en crear cuentas nuevas con privilegios administrativos. El revisar que los datos estén segmentados en los servidores es algo importante de auditar también ya que se debe separar la información sensible de los datos más comunes con los que se trabaja en el ambiente de trabajo. (NIST, 2021).

Con las prevenciones adecuadas, la ventana para un ataque exitoso se reduce en gran cantidad, dejando a la empresa con un buen plan de acción en caso de detectar un ataque y protegiendo a sus activos en caso de cualquier incidente exitoso. Esto ahorra dinero, tiempo y recursos humanos valiosos que ayudan al crecimiento de las operaciones y resguardan los intereses y objetivos de la organización.

B. Recomendaciones al ser atacado por ransomware de la CISA y el FBI

El tener los activos anteriores de preparación y una fuerte cultura de seguridad son factores que reducen en gran parte el riesgo de estar bajo ataque de un programa malicioso de *ransomware*, sin embargo, aún existe la posibilidad de que un intento de ataque sea exitoso y la empresa se encuentre en peligro. Para esto, se tienen recomendaciones de seguridad que son efectiva en reducir el impacto y la efectividad del ataque en curso. (CISA, 2021).

Tan pronto como se dé el aviso de que un *ransomware* ha tomado control de un sistema se tiene que aislar el sistema infectado lo más rápido como se pueda posible, para evitar la propagación del ataque a otras redes o equipos. Hay que desasociar el

sistema infectado de todas las redes que tienen contactos y desactivar la conexión inalámbrica WIFI, Bluetooth o cualquier otro medio por el cual la computadora pueda comunicarse fuera de su entorno. Se tiene que asegurar que las unidades compartidas y en red estén desconectadas, ya sean cableadas o inalámbricas. (FBI, 2019).

También es imperativo el apagar otras computadoras y dispositivos que hayan estado en conexión con el sistema que fue infectado inicialmente. Una vez que los dispositivos han sido apagados y desconectados, el reunirlos en una ubicación central con etiquetas claras de cuáles han sido encriptados por el *ransomware* y que otros estaban en las cercanías puede ayudar a el tratamiento e investigaciones consecuentes realizadas por los especialistas. (CISA, 2021).

Figura 12: Recomendaciones de la NIST ante la amenaza de *ransomware*

Fuente: NIST (2021)

Durante estos ataques las copias de seguridad que se tienen de los sistemas críticos entran en un rol importante. Hay que asegurar que todas las copias estaban fuera

de línea y del alcance del atacante, y tener los datos de respaldo en lugares seguros para ponerlos en línea tan pronto se pueda. Antes de que estos respaldos puedan estar activos se necesita el revisarlos con programas antivirus, y que se pueda comprobar que estos con contienen el programa malicioso ya instalado. (CISA, 2021).

El FBI otras agencias de seguridad no aconsejan el pago de un rescate en respuesta al ataque de *ransomware*. Ya que pagar ese rescate no garantiza que la organización recupere ningún dato ni sistema infectado, así como tampoco garantiza que el ataque no se repita, esto también alienta a los perpetradores a tener conexiones a más víctimas y ofrece da incentivo para que otros se involucren en este tipo de actividad ilegal. (FBI, 2019).

Lo importante al tener un incidente de *ransomware* es guardar la calma y no realizar ninguna acción o movimiento con desesperación. El guardar la calma y planear el siguiente paso es imperativo para proteger los activos de la organización, los datos de sus usuarios y empleados. Siguiendo las recomendaciones de las agencias de seguridad, se puede cortar el intento de encriptación o incluso restaurar los datos antes de que cualquier perdida ocurra. Todo esto puede lograrse sin pausar las operaciones de la empresa y dejando a los usuarios finales protegidos.

C. El fortalecimiento de la cultura y la conciencia en seguridad

Como se pudo documentar en capítulos pasados la ausencia de una fuerte cultura de seguridad y la falta de conciencia pueden dar raíz a muchos problemas dentro de la empresa y abren potenciales riesgos críticos. Para poder fortalecer ambos pilares y que se puedan combinar con los esfuerzos de seguridad, se debe tener un entendimiento profundo del ecosistema de la empresa y las necesidades de esta. También el tener conocimiento de las necesidades de los empleados y su nivel de conocimiento da información detallada para comenzar a planear las acciones necesarias.

Hay que conocer de forma completa los perfiles que se tiene de los integrantes de los equipos que conforman la empresa. Si el perfil de un empleado es muy técnico o tiene un conocimiento sólido de seguridad, hay que asegurarse de trabajar con otros empleados o incluirlo en capacitaciones para mejorar sus habilidades de comunicación no técnica y social. Uno de los mayores desafíos a los que se enfrentan los profesionales

de la seguridad es simplificar la información de seguridad para sus empleados, siendo esta normalmente de naturaleza puramente técnica y presentada de forma profesional, evadiendo la compresión de los demás empelados. El simplificar la información para que pueda ser entendida por todas las personas que se encuentran en la organización es muy importante.

La comunicación clara es un elemento clave en la presentación de la información de forma simple y sencilla para poder adquirir las aptitudes correctas y tener una clara vía de comunicación. Para lograr esto se puede capacitar a un miembro del equipo de seguridad, asociar a los departamentos de comunicaciones o marketing, o incluso incorporar a uno de los miembros de esos equipos al propio de concienciación sobre seguridad. Incluso aquellos sin experiencia en seguridad o ingeniería pueden entrar a capacitarse en los campos de la seguridad para obtener una mejor comprensión de la terminología, las tecnologías y los desafíos involucrados.

Uno de los problemas que se encontraron en las encuestas de la SANS era la falta de apoyo por parte de los niveles administrativos de la empresa. El analizar los costos que tienen las infracciones por incidentes de seguridad, los costos de las fallas al cumplimiento de los requisitos de seguridad de socios, proveedores y gobiernos locales e internacionales. Presentar una comparación de todos esos gastos eso contra el costo del programa de concientización sobre la seguridad ayuda a demostrar que se puede reducir significativamente la perdida de activos e ingresos invirtiendo en la concientización y la cultura de la seguridad.

Para poder tener una base de información de riesgos para poder informar eficientemente a los empleados y usuarios se debe medir y analizar el ambiente de riesgo que se tiene en la organización. Los informes de seguridad, los datos críticos y las estadísticas ayudan a demostrar a los líderes y a las áreas administrativas la necesidad de abordar el riesgo humano y cómo otras organizaciones están aprovechando activamente los programas de concientización para gestionar eficazmente su cultura. Uno de esos informes es el DBIR de Verizon, que identifica al elemento humano como el factor más importante tanto para los incidentes como para las infracciones a nivel mundial y esta información puede alentar a la cooperación de parte de los departamentos involucrados que no tengan perfil técnico.

Como un esfuerzo paralelo al de tener la información adecuada y la comunicación clara de esta misma, se debe invertir fuertemente en el personal que administra y maneja las áreas de conciencia y cultura de la seguridad. El tener formas eficientes de ahorrar tiempo en los procedimientos de seguridad como la generación de boletines informativos, en cuentas a los empleados, procesamiento de información ayuda a tener una mayor flexibilidad para administrar los recursos y ahorrar en estos mismos. Una manera de poder realizar esto es tener personal delegado y especializado sobre las áreas que necesiten atención, el unificar los procedimientos es importante ya que, si se tienen muchos programas independientes, licencias entre otras maneras de gestión se puede perder mucho dinero y tiempo de la organización.

El tener asociaciones con otros departamentos, como por ejemplo el equipo de diseño gráfico, comunicaciones o incluso el equipo de seguridad de operaciones ayuda a expandir el alcance de las actividades del equipo de cultura y aclara la visibilidad de las necesidades y acontecimientos en el ecosistema de la empresa, así como adoptar comportamientos positivos que se observen dentro de estos departamentos y fomentarlos para los demás.

La sostenibilidad y el cambio de cultura a largo plazo se logrará con la consistencia y la perseverancia de los programas desarrollados a partir de las recomendaciones y prevenciones que se tomaron en cuenta por los equipos de concientización y seguridad. Hay que asegurar que el programa tenga los procesos, recursos y apoyo de liderazgo necesarios para una vida a largo plazo. Se debe incluir un plan de mejora continua, estableciendo un ciclo que incluya como bases mínimas una revisión anual y una actualización del programa que se mantenga al día con las amenazas globales y locales que se frecuentan en el ambiente empresarial, esto también con el propósito de revisar los incidentes que hayan ocurrido en los periodos anteriores o descubrimientos importantes reportados por los equipos, todo con el propósito de mejorar las operaciones de la empresa y protegerla. Como resultado, el programa logra ser una parte bien establecida de la cultura de la organización y se vuelve algo moderno y atractivo para cualquier empleado y líder que sea parte de él. Con los resultados a largo plazo el programa de cultura y conciencia cambia el comportamiento, las creencias, actitudes y percepciones de seguridad de las personas.

I. Como un listado compacto podemos ver las recomendaciones de la siguiente forma:

- **Contar con las personas adecuadas**: Se necesita el personal adecuado dedicando e invirtiendo el tiempo para comenzar a cambiar los comportamientos organizacionales. El número de FTE como se había visto en capítulos anteriores puede variar según el tamaño, la estructura y los requisitos de la organización.
- **Asegurar el apoyo del liderazgo**: El demostrar claramente el riesgo y sus consecuencias a nivel empresarial es una de las formas más efectivas de obtener el apoyo del liderazgo. Explicar el cómo otras organizaciones de la industria tienen programas de extensión maduros y como continúan invirtiendo en ellos también alienta a implementar uno propio de la organización.
- **Fomentar las alianzas**: Establecer asociaciones y colaboraciones con otros departamentos y empleados de la organización para una mayor claridad y efectividad de las operaciones. Involucrar a los departamentos críticos en el proceso de planificación desde el principio es importante para un buen planeamiento.
- **Conseguir tiempo**: Si se tiene el presupuesto, hay que invertirlo para ahorrar tiempo y recursos. Por ejemplo, contratar a un especialista o comprar un programa de administración unificado en vez de invertir en la programación de uno o de licencias separadas.
- **Conocer los perfiles**: La experiencia y los conocimientos son una ventaja siempre que puedan ser compartidos de forma clara para los demás y que puede contribuir en el apoyo de la conciencia y al crecimiento del programa.
- **Realizar capacitación en seguridad**: El desarrollar un programa de capacitación, conciencia y entrenamiento de la seguridad, generaliza y esparce el conocimiento sobre riesgos y sobre como mitigarlos, el combinarlo con los lenguajes simplificados y los profesionales los hace efectivos.

Una nueva recomendación que se agregó este año por parte de la SANS, orientada a las empresas con programas de cultura, es que la mayoría de los equipos de concientización sobre seguridad deben reportar directamente al “Director de Seguridad de la Información” si es posible dentro de la estructura de la empresa, y que la información recibida sea responsabilidad del equipo de seguridad y no de otro departamento. Se busca proporcionar información completa y digerible, así como también pasos prácticos que se puedan tomar para administrar mejor el riesgo que se genera por las personas y su desconocimiento.

VI. CONCLUSIONES

Se puede observar que en los últimos años la tecnología ha tomado un papel fundamental en las actividades básicas de todos los niveles de comercio y administración empresarial, de forma que su camino ha tomado un crecimiento exponencial que apunta a conservar esa tendencia con él desarrollo de las nuevas formas de trabajo en casa y comunicaciones a distancia.

Esto provoca que las actividades criminales crezcan paralelamente con estos avances tecnológicos. Las tecnologías, así como herramientas que nos dan utilidad y protección en el presente, pueden en un futuro que se conviertan en programas con el propósito de usarse en una carrera armamentista entre los grupos criminales y los gobiernos en conjunto con las empresas de seguridad por la superioridad y control en el mercado. Probando que estas mismas herramientas pueden convertirse en amenazas constantes dentro del ecosistema laboral que tienen las empresas si se dejan desatendidas y sin ningún medio de control o conocimiento para quienes las operan.

La ventaja que podemos tener para combatir estas nuevas amenazas es la enseñanza y el inculcar la curiosidad, el hambre por el conocimiento de la cultura de seguridad y de las buenas prácticas que se pueden desarrollar dentro de las empresas, así como los roles que desarrollan los empleados individualmente dentro del ambiente y ecosistema de trabajo, el factor humano es la primera y última línea de defensa de un sistema digital y la empresa que lo administra.

El construir lazos entre los departamentos de inteligencia de ciberseguridad y los departamentos que conducen operaciones diferentes o adyacentes dentro de la empresa va a resultar en una red de comunicación altamente efectiva dando apoyo al análisis y monitoreo de datos y las amenazas que se puedan presentar, así como la preparación oportuna ante incidentes globales entre otros factores de riesgo que rodean las operaciones del día a día. A parte de la concientización de seguridad, el trabajo en equipo y el profesionalismo de deben inculcar, yendo de la mano con la seguridad, así fortaleciendo la confianza entre miembros de los diferentes equipos.

Con el panorama global de la seguridad llevando esta variable constante de crecimiento, el poder contar con este tipo de red de información y comunicación dentro

de los ambientes laborales, ayuda a una evolución conjunta que se expande dentro de la región local de los usuarios y empleados, terminando de desarrollarse de manera nacional, y que ayuda a entender las formas en las que los programas maliciosos y las criminales pueden explotar a los empleados y las mismas herramientas digitales que usan. Esto al final es algo de vital importancia a la hora de defender los activos más críticos y valiosos de una empresa o de una organización: La vida humana y el capital que la mantiene.

Observando la forma en la que los programas de ransomware entre otros tipos de programas maliciosos contagian los sistemas para infectarse, el tener un personal bien informado y que practique buenos hábitos de seguridad y cultura puede prevenir e incluso desmantelar amenazas completas antes de que puedan intervenir en las operaciones de la empresa o en los sistemas individuales de los usuarios. E incluso se puede aportar al avance de creación de programas de seguridad documentados e interconectados, que puedan analizar el progreso de los intentos de ataque e infiltración hacia el ecosistema laboral y con esta información blindarse entre departamentos, sucursales e incluso entre empresas. Trabajando en conjunto, las empresas locales, nacionales e internacionales de la mano con los departamentos de inteligencia, se puede llevar a cabo la implementación de plataformas de monitoreo y análisis de datos para el estudio de los movimientos de los grupos hostiles alrededor del mundo, pudiendo implementar la mejora continua como cultura en todos los niveles sociales y la creación de planes de acción, prevención y reacción ante cualquier incidente y los riesgos que se puedan detectar.

VII. REFERENCIAS BIBLIOGRÁFICAS

Abrams, L. (02 de junio de 2021). *Bleepingcomputer.* Obtenido de https://www.bleepingcomputer.com/news/security/fujifilm-shuts-down-network-after-suspected-*ransomware*-attack/

Aisvector. (Abril de 2018). *shutterstock.* Obtenido de https://www.shutterstock.com/es/image-vector/computer-infected-by-malware-*ransomware*-wannacry-641338786?irclickid=S7WTV9QJ%3AxyLTitwUx0Mo3b%3AUkBwoWxf7T8jRs0&irgwc=1&utm_medium=Affiliate&utm_campaign=TinEye&utm_source=77643&utm_term=&c3ch=Affiliate&c3nid=

Alshaikh, H., Ramadan, N., & Hefny, H. A. Ransomware Prevention and Mitigation Techniques. International Journal of Computer Applications, 975, 8887.

BBC-News 2019, Baltimore government held hostage by hackers' *ransomware*, https://www.bbc.com/news/world-us-canada-48371476

BBC-News 2019, Baltimore *ransomware* attack: NSA faces questions, BBC-News, https://www.bbc.com/news/technology-48423954

Chen, Q. & Bridges A.R. (2017) Automated Behavioral Analysis of Malware A Case Study of WannaCry Ransomware. Obtenido de https://arxiv.org/pdf/1709.08753.pdf

CISA. (08 de julio de 2021). *Cybersecurity & IInfrastructure Security agency.* Obtenido de https://us-cert.cisa.gov/ncas/alerts/aa21-131a

CISA. (s.f.). *CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY.* Obtenido de https://www.cisa.gov/

Cybersecurity & Infrastructure Security Agency. (16 de enero de 2017). *CISA.* Obtenido de https://us-cert.cisa.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices

Federal Bureau of Investigation. (2019). *FBI.* Obtenido de Scam and Safety.

Fujifilm. (07 de junio de 2021). *FUJIFILM.* Obtenido de https://www.fujifilm.com/uk/en/news/statement-on-june-2021-*ransomware*-attack#

Groot, J. D. (1 de Diciembre de 2020). *Digital Guardian.* Obtenido de https://digitalguardian.com/blog/history-*ransomware*-attacks-biggest-and-worst-*ransomware*-attacks-all-time

Ikeda, S. (19 de mayo de 2021). *CPO Magazine.* Obtenido de https://www.cpomagazine.com/cyber-security/verizon-data-breach-report-2021-pandemic-has-caused-major-surge-in-phishing-*ransomware*-and-web-app-attacks/

James, K. (2019, Jun) Protecting Local Governments from Ransomware Attacks. http://www.infosecwriters.com/Papers/kjames_governments_*ransomware*.pdf

Jeremy Ashkenas, A. P. (12 de mayo de 2017). *NewYork Times.* Obtenido de https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-*ransomware*-map.html

Kim, A. (06 de Marzo de 2016). *MacRumors.* Obtenido de https://www.macrumors.com/2016/03/06/mac-*ransomware*-transmission/

Kraszewski, K. (2019, May). SamSam and the Silent Battle of Atlanta. In 2019 11th international conference on cyber conflict (CyCon) (Vol. 900, pp. 1-16). IEEE.

Krauss, C. (11 de mayo de 2021). *The New York Times.* Obtenido de https://www.nytimes.com/es/2021/05/11/espanol/colonial-pipeline-*ransomware*.html

López Noguero, F. (2002). El análisis de contenido como método de investigación.

López, N., & Sandoval, I. (2016). Métodos y técnicas de investigación cuantitativa y cualitativa.

Lovelace, R. (13 de mayo de 2021). *The Washington Times.* Obtenido de https://www.washingtontimes.com/news/2021/may/13/darkside-seek-robin-hood-image-*ransomware*-attacks/

Martins, A., & Elofe, J. (2002). Information security culture. In Security in the information society (pp. 203-214). Springer, Boston, MA.

Nadir, I., & Bakhshi, T. (2018, March). Contemporary cybercrime: A taxonomy of *ransomware* threats & mitigation techniques. In 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-7). IEEE.

NIST. (mayo de 2021). *National Institute of Standards and Technology.* Obtenido de https://csrc.nist.gov/Projects/*ransomware*-protection-and-response

Nithya, T., Vijaya, K., Subramanian, D., Balamurugan, E., & Shanmugavel, K. Ransomware Deployment and Analysis. http://ijrad.com/docs/v4n2/A87.pdf

Otero, C. (09 de junio de 2021). *betecch.* Obtenido de https://as.com/meristation/2021/06/09/betech/1623236920_691793.html

PandaSecurity. (15 de abril de 2020). *PandaSecurity.* Obtenido de https://www.pandasecurity.com/es/mediacenter/malware/ryuk-*ransomware*-empresas/

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. Inf. Secur. J. A Glob. Perspect., 14(2), 37-49.

Redacción APD. (6 de julio de 2018). *apd.es.* Obtenido de https://www.apd.es/empresas-afectadas-por-ciberataques/

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10.

Ruiz, E. (28 de noviembre de 2019). *Forbes.* Obtenido de https://www.forbes.com.mx/las-consecuencias-de-un-ciberataque-caso-pemex/

Sahi, S. K. (2017). A study of wannacry *ransomware* attack. International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), 4(9), 5-7.

SANS Security Awareness. (Marzo de 2021). *SANS.* Obtenido de https://www.sans.org/security-awareness-training/resources/reports/sareport-2021/

Savage, K., Coogan, P., & Lau, H. (2015). The evolution of *ransomware*. Symantec, Mountain View.

Savita Mohurle, M. P. (mayo de 2017). *sbgsMedia.* Obtenido de https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf

Valdeolmillos, C. (04 de junio de 2021). *MuycomputerPro.* Obtenido de https://www.muycomputerpro.com/2021/06/04/fujifilm-ataque-*ransomware*
Verizon. (2021). *Verizon.* Obtenido de https://www.verizon.com/business/resources/reports/dbir/