TRABAJO DE GRADO

# CONSTRUCCIÓN DE GUÍAS DE HARDENING QUE ELEVEN LOS NIVELES DE SEGURIDAD PARA LOS FUNCIONARIOS DE ENTIDADES FINANCIERAS QUE LABORAN DESDE LA MODALIDAD DEL TELETRABAJO.

CAMILO ALEJANDRO IBAÑEZ NARANJO

LUIS FELIPE RODRIGUEZ VARON

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2020

TRABAJO DE GRADO

# CONSTRUCCIÓN DE GUÍAS DE HARDENING QUE ELEVEN LOS NIVELES DE SEGURIDAD PARA LOS FUNCIONARIOS DE ENTIDADES FINANCIERAS QUE LABORAN DESDE LA MODALIDAD DEL TELETRABAJO.

CAMILO ALEJANDRO IBAÑEZ NARANJO

LUIS FELIPE RODRIGUEZ VARON

Trabajo de grado para optar al título de Especialista en Seguridad de la Información

Docente

M.SC. DIEGO OSORIO REINA

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2020

## DEDICATORIA

En primer lugar, queremos agradecer a Dios por habernos permitido llegar a este punto de nuestras vidas y de nuestras carreras profesionales, también queremos agradecer mucho a nuestros padres que nos brindaron su apoyo durante nuestro proceso de formación académica en la Universidad Católica de Colombia que sin su apoyo y sus concejos no hubiese llegado hasta este punto como especialista en seguridad de la información.

También queremos agradecer mucho a los ingenieros y profesores de la universidad católica de Colombia, al ingeniero Diego Osorio Reina que gracias a sus conocimientos y paciencia, estuvo fielmente siempre con nosotros durante todo proceso de la especialización y del proyecto, a la ingeniera Sandra Milena Bernate que desde un principio nos dio ese apoyo de formación educativa y concejos, y al resto de profesores de la especialización que compartieron sus experiencias y enseñanzas en todo el proceso educativo.

## TABLA DE CONTENIDO

**Pág.**


1. Introducción 22
2. Generalidades 23
   2.1. Línea de Investigación 23
   2.2. Planteamiento del Problema 23
      2.2.1. Antecedentes del problema 25
      2.2.2. Pregunta de investigación 29
      2.2.3. Variables del problema 30
   2.3. Justificación 30
3. Objetivos 33
   3.1. Objetivo general 33
   3.2. Objetivos específicos 33
4. Marcos de referencia 34
   4.1. Marco conceptual 36
   4.2. Marco teórico 38
   4.3. Marco jurídico 39
   4.4. Marco geográfico 41
   4.5. Estado del arte 41
5. Metodología 45
   5.1. Fases del trabajo de grado 45
   5.2. Instrumentos o herramientas utilizadas 47
   5.3. Población y muestra 48
   5.4. Alcances y limitaciones 48
6. Productos a entregar 50
7. Entrega de resultados esperados e impactos 51
   7.1. Documento Análisis Threat Intelligence 51
      7.1.1. Introducción 51
      7.1.2. Alcance 51
      7.1.3. El impacto del covid-19 y aumento de las ciberamenazas en las organizaciones financieras 52
      7.1.4. Linea de tiempo 42
      7.1.5. Análisis de amenazas 44
      7.1.6. Herramientas de ataque, técnicas y procedimientos 44

7.1.7. Grupos de amenazas 47
7.1.7.1. Grupo APT-C-36 47
7.1.7.2. Grupo APT38 50
7.1.7.3. Grupo APT19 53
7.1.8. Mapa de Threat Intelligence 58
7.1.9. Resultados obtenidos de la inteligencia anterior 59
7.1.10. Conclusiones de la Threat Intelligence 59
7.2. Guia de Hardening 60
7.3. Prueba de concepto 62
8. Conclusiones 67
9. Bibliografia 68

## LISTA DE FIGURAS

**Pág.**


FIGURA 1. LIBRO BLANCO DE TELETRABAJO EN COLOMBIA - VERSIÓN 3.0, PÁG. 85 ..... 44
FIGURA 2. FASES DEL TRABAJO DE GRADO, ELABORACIÓN PROPIA. ..... 45
FIGURA 3. MAPA CONCEPTUAL INITIAL ACCESS - MITRE ATT&CK ..... 47
FIGURA 4. LÍNEA DE TIEMPO, ATAQUES ENTIDADES FINANCIERAS – ELABORACIÓN PROPIA. .... 42
FIGURA 5. LÍNEA DE TIEMPO, ATAQUES ENTIDADES FINANCIERAS – ELABORACIÓN PROPIA. .... 43
FIGURA 6. CICLO DE VIDA, GRUPO APT-C-36 – MITRE ATT&CK. ..... 47
FIGURA 7. CICLO DE VIDA, GRUPO APT38 - MITRE ATT&CK. ..... 51
FIGURA 8. CICLO DE VIDA, GRUPO APT19 - MITRE ATT&CK. ..... 54
FIGURA 9. MAPA CONCEPTUAL DE THREAT INTELLIGENCE - MITRE ATT&CK. ..... 58
FIGURA 10. GUÍA DE HARDENING. ..... 60
FIGURA 11. RECOMENDACIONES DE SEGURIDAD PARA USUARIO EN TELETRABAJO. ..... 61
FIGURA 12. RECOMENDACIONES DE SEGURIDAD PARA EL ÁREA DE TECNOLOGÍA. ..... 61
FIGURA 13. PRUEBA DE CONCEPTO - GUÍAS DE HARDENING. ..... 62
FIGURA 14. MÁQUINAS VIRTUALES. ..... 63
FIGURA 15. CORREO PHISHING. ..... 63
FIGURA 16. PÁGINA WEB PHISHING. ..... 64
FIGURA 17. DESCARGA DEL MALWARE. ..... 64
FIGURA 18. COMPROMISO DEL EQUIPO DEL TRABAJADOR. ..... 65
FIGURA 19. RECOMENDACIONES DE SEGURIDAD. ..... 65
FIGURA 20. BLOQUEO DEL MALWARE POR PARTE DEL ANTIVIRUS. ..... 66

# LISTA DE TABLAS

**Pág.**

TABLA 1. VARIABLES DEL PROBLEMA, ELABORACIÓN PROPIA..... 30

# 1. INTRODUCCIÓN

La incorporación de las nuevas tecnologías de comunicación ha dado parte a nuevas formas de trabajo, que permite al trabajador adaptarse a nuevas condiciones laborales para obtener una armonía entre lo económico y lo social, y es ahí en donde nace el teletrabajo. Esta nueva modalidad de organización, no obstante, se encuentra inmersa en profundos cambios, a los cuales la seguridad informática no se escapa.

Con relación a la información, se debe considerar como el medio sutil de mayor importancia en el teletrabajo, y es necesario que, a fin de impedir cualquier deformidad, se garantice la CIA "confidencialidad integridad y disponibilidad" de la información, tanto de los equipos de la organización, como de los teletrabajadores, ya que estos últimos manipulan numerosos datos en dispositivos electrónicos desde cualquier ubicación.

"*La información que manejamos en nuestras empresas es uno de los activos más importantes que hay que proteger*" [1] "Instituto nacional de Ciberseguridad (INCIBE) ,2017"

El motivo principal en esta investigación es la construcción de guías robustas que minimicen los riesgos de seguridad del teletrabajo, pues las empresas no cuentan con unas políticas de seguridad de la información, ni protocolos que les permitan brindar una seguridad óptima y oportuna de la información.

"*Las organizaciones deberían asumir que los dispositivos cliente de teletrabajo, que se utilizan en una variedad de ubicaciones externas, son particularmente propensos a la pérdida o robo, y estos serán adquiridos por partes maliciosas que intentarán recuperar datos confidenciales de ellos, o aprovechar los dispositivos para obtener acceso a la red empresarial*" [2] "Guido to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, 2016"

Para el desarrollo de este trabajo se analizará el planteamiento del problema, los objetivos a lograr dentro de la investigación y delimitaciones que se tienen, posteriormente el marco legal en Colombia y reflejar los antecedentes de la problemática del teletrabajo; por último, se realizara un análisis documentado de Threat intelligence para conocer las tácticas y técnicas que utilizan los adversarios o grupos que podrían vulneran o afectan un funcionario de una entidad financiera que labora desde casa.

# 2. GENERALIDADES

## 2.1. LÍNEA DE INVESTIGACIÓN

En el programa se trabaja sobre Software Inteligente y Convergencia Tecnológica

## 2.2. PLANTEAMIENTO DEL PROBLEMA

En los últimos años la modalidad del teletrabajo ha crecido exponencialmente en Colombia y Latinoamérica, teniendo a Brasil y argentina como pioneros en esta modalidad que suman casi 16 millones de teletrabajadores, Colombia por su parte ya cuenta con más de 122 mil empleadores vinculados al trabajo remoto permitiendo obtener un nuevo estilo de vida que permite al empleador adaptarse a un nuevo ambiente para obtener una mayor libertad de organizar su tiempo, destacarse en su productividad, mejorar los resultados y emparejar su vida profesional con su vida familiar. [13] “Teletrabajo.gov, 2019”

Sin embargo las personas que trabajan por esta modalidad en muchas ocasiones no tienen conciencia y son muy confiables, utilizan dispositivos (BYOD) sin las herramientas adecuadas de seguridad, en muchas ocasiones son sus computadores de hogar donde lo utilizan toda la familia ingresado a todo tipo de páginas, descargando programas y multimedia, que sin tener conocimiento de los riesgos del mundo cibernético, estarían fácilmente expuestos estos equipos a virus como spam, troyanos, malware y el más frecuente los ransomware. Solamente en el 2019 se registraron en América latina y caribe 85 billones de intentos de ciberataques de las cuales la mayoría tenía como fin obtener información financiera y robar dineros, lo más preocupante es que en los últimos meses ha crecido los ataques y quizás el principal problema es la falta de conciencia. También se presentan riesgos en equipos otorgados por la empresa porque así ofrezca mejor seguridad, las personas pueden ser hackeadas cuando se conectan a redes públicas inseguras o poco confiables y se exponen a hackeos robo de información confidencial de la empresa o cuando reciben emails que contengan phishing, y aun así ante todas estas amenazas y vulnerabilidades que esto genera tanto empleadores como las empresas no se tiene claridad de que protocolos o guías se deba manejar ante estas situaciones de riesgos para mitigar o minimizar un contagio informático a la seguridad de la información cuando se trabaja por la modalidad de teletrabajo. [30] “Hacknoid, 2019.”

No obstante, las corporaciones o pymes para no afectar sus operaciones, su productividad e ingresos, ellos optan por la modalidad del teletrabajo, que consta dejar al trabajador en la casa y conectarse de forma remota a la red interna o a los equipos de infraestructura de TI. Esta modalidad, aunque representa muchas ventajas como mayor productividad, menor infraestructura y menores costos, ven en esta modalidad una plena desconfianza y más para un funcionario de tesorería

que maneja información muy confidencial y sensible como los recursos, datos de empleados y pagos de nóminas de los trabajadores de una empresa, este funcionario estaría laborando desde su casa y la empresa no sabe con plena certeza como se estaría manejando la información confidencial fuera de la empresa. Las malas prácticas de un teletrabajador también son consecuencias que facilitan los ciberataques ya que por falta de conocimiento o una buena guía no toman las medidas adecuadas para evitar los ataques informáticos.

Es importante hablar de otra problemática que afectaría la productividad en una empresa y es que durante varias décadas atrás y actualmente en pleno siglo XXI la sociedad enfrenta uno de los mayores problemas en las grandes ciudades que es la movilidad, los ciudadanos optan por varias opciones para transportarse desde las casas hasta sus trabajos (carros, motos, transportes públicos...etc.) y mientras los números dicen que las ciudades seguirán creciendo de forma exponencial, el sistema de transporte seguirá colapsando y las carreteras no darán basto a la gran cantidad de carros que circularan. Los trabajadores que se desplazan en hora pico pueden durar en un promedio de hasta 1 a 2 horas, los que se desplazan en automóviles se enfrentarían al tráfico por la alta fluencia de carros, los accidentes automovilísticos que generan trancones y el clima que también es un factor importante cuando se presentan lluvias o granizos, todo esto hace que la gente pierda mucho tiempo de sus valiosas vidas en solo desplazamiento al trabajo.

“Según una firma especializada llamada Inrix reveló el medidor de tráfico mundial del 2017, en el que compara la congestión del tráfico en 1.360 ciudades de 38 países de todo el mundo. Colombia es, según Inrix, el tercer país más congestionado del mundo. En promedio las personas pasan 48 horas al año en medio de congestión máxima. Otro punto muy importante a considerar son las horas que las personas gastan en medio de un trancón. Según el informe, los bogotanos pasan en esta situación 75 horas al año, 27 horas menos de las que viven en la ciudad más congestionada del mundo, Los Ángeles (102), pero 17 horas más que Ciudad de México”. [3] “Revista Semana, 2018”

El transporte público tampoco se salva, los ciudadanos en las grandes ciudades ven como el transporte público colapsa cuando hace falta más frecuencia de buses o no dan abasto a la cantidad gente cuando se transporta por este medio, esto hace que se llegue muy tarde a sus empresas. También están presentes los accidentes que retrasan la movilidad, las manifestaciones y el clima que hace colapsar transporte público. Otro factor importante es que están más expuestos a robos y atracos, cuando vuelven a sus casas en las noches no solo afectan su integridad física si no también su moral que no puede ser bueno para la operación de una organización ya que afecta anímicamente al empleador, esto ocurre también se presentan robos de sus pertenencias como portafolios, dispositivos o documentos sensibles que puedan afectar la confidencialidad de una empresa,
Otro problema y mucho más sensible es el que se está viviendo actualmente en esta época y son las pandemias o virus. Ha sucedido mucho en las últimas décadas

como la gripe aviar, el H1N5 y la gripe porcina y actualmente se está viviendo una situación similar. En los inicios del año 2020 en la ciudad de Wuhan se detectó un virus mortal que afecta el sistema respiratorio y puede dar neumonía que si no se tiene cuidado o se trata correctamente las personas podrían morir. Este nuevo virus en una gran ciudad se puede transmitir fácilmente por las vías respiratorias, los ojos y la boca, también se puede expandir trasmitiéndose de persona a persona y si la persona contagiada anda en transportes públicos terrestres o aéreos seguirá contagiando a otros y se puede seguir propagando hasta llegar a otros países. Por eso los gobernadores de todos los países no les queda otra opción de poner en cuarentena a todas las personas teniéndolas encerradas en sus casas esto con el fin de disminuir la línea de contagiados.

Todas estas problemáticas cuando se habla de la falta de seguridad, confianza y falta de conocimiento en el empleador representan un peligro para la empresa poniendo en jaque los tres pilares de la seguridad de la información o cuando se habla de colapsos en el transporte público, trancones y pandemias puede representar perdida de dinero y baja productividad.

### 2.2.1. ANTECEDENTES DEL PROBLEMA

Las investigaciones acerca de las vulnerabilidades y ataques por consecuencia de la falta de políticas de seguridad en la modalidad de teletrabajo se centran en gran medida en la conciencia de no tener los diversos controles de seguridad y políticas robustas, los requisitos de teletrabajo en el entorno actual, aumentan la probabilidad de que los empleados confíen en dispositivos móviles y dispositivos de propiedad personal para llevar a cabo negocios que anteriormente se harían desde sus oficinas, este cambio abre una nueva vulnerabilidad para las empresas.

Debido a que casi todo el acceso remoto ocurre a través de Internet, las organizaciones normalmente no tienen control sobre la seguridad de las redes externas utilizadas por los clientes de teletrabajo. Los sistemas de comunicaciones utilizados para el acceso remoto incluyen redes de banda ancha, como el cable, y mecanismos inalámbricos, como redes celulares, equipos portátiles, tablets. Estos sistemas de comunicaciones son susceptibles de escuchar a escondidas, así como ataques de intermediarios para interceptar y modificar las comunicaciones.

Para Sophos, el RDP (acceso remoto). “Sigue siendo motivo de insomnio para los administradores de sistemas, informa sobre cómo los cibercriminales explotan el RDP desde 2011, y que, en el último año, los grupos de ciberdelincuentes que se encontraban detrás de dos de los mayores ataques de ransomware, como fueron Matrix y SamSam, han abandonado casi por completo el resto de métodos de acceso a las redes en favor del uso del RDP”. [4] “Matt Boddy, Ben Jones, and Mark Stockley Sophos, RDP Exposed - The Threat That's Already at Your Door, 2019”

Una de las formas que se destaca es como los atacantes pueden encontrar

dispositivos habilitados para RDP, para demostrarlo Matt Boddy experto de seguridad de Sophos, demostró que, en tan solo un día, los atacantes intentaron diversos inicios de sesiones en 10 Honeypots (cebos) dispersos geográficamente de baja interacción.

Como resultado del análisis de investigación en su publicación en el año 2019, Sophos identifico el comportamiento que tienen los atacantes a la hora de explotar esa vulnerabilidad.

Perfiles y patrones de ataque.

**El carnero: "**La estrategia de los atacantes es descubrir la contraseña del administrador. En el transcurso de 10 días, un atacante realizó 109.934 intentos de inicio de sesión, utilizando solo tres nombres de usuario.

El atacante realizó 37,623 intentos de inicio de sesión con el nombre de usuario administrador, seguido de otros 37,623 intentos con el nombre de usuario admin y luego 34,688 mil intentos con el nombre de usuario Riarthóir, la palabra irlandesa para administrador.

Si un atacante tiene como objetivo abrir cuentas de administrador, entonces tiene sentido concentrarse en hacer decenas de miles de conjeturas de contraseñas a expensas de una lenta rotación de los nombres de usuario. Es probable que los administradores tengan contraseñas más seguras que los usuarios habituales y una pequeña cantidad de nombres de usuario son muy comunes." [4] "Matt Boddy, Ben Jones, and Mark Stockley Sophos, RDP Exposed - The Threat That's Already at Your Door, 2019"

**El enjambre: "**Este ataque comenzó en el centro de datos de París justo antes de la medianoche del 23 de abril. El atacante prueba el nombre de usuario ABrown nueve veces en el transcurso de 14 minutos. A esto le siguen nueve intentos con el nombre de usuario BBrown, nueve más con CBrown y nueve con DBrown. Cada nombre de usuario se prueba nueve veces a intervalos impredecibles, y cada intervalo dura desde unos pocos segundos hasta decenas de minutos.

El atacante parece estar trabajando a través de una larga lista de nombres de usuario y simplemente incluye nuevos objetivos en su ataque en cualquier punto de la lista de nombres de usuario que han alcanzado. Quizás el ataque no utiliza una lista en absoluto y se basa en un algoritmo para generar una secuencia interminable de nombres de usuario. Sin embargo, funciona, el atacante parece creer que un nombre de usuario es tan probable que produzca un resultado como cualquier otro y que, a diferencia de las contraseñas, no hay una mejor primera suposición. este atacante parece pensar que su punto de apoyo más probable en la red de una víctima vendrá a través de un usuario normal con una contraseña deficiente en lugar de un administrador." [4] "Matt Boddy, Ben Jones, and Mark Stockley Sophos, RDP Exposed - The Threat That's Already at Your Door, 2019"

**El erizo**: "Este ataque puntiagudo se caracteriza por estallidos de actividad seguidos de períodos más largos de inactividad. Cada pico es generado por una dirección IP, dura aproximadamente cuatro horas y consta de entre 3,369 y 5,199 conjeturas de

contraseña. Aunque los picos tienen un tamaño y una duración similares, no son del mismo tamaño, y tampoco lo son las pausas entre ellos como habría de esperarse. Esto puede deberse a que el atacante está introduciendo deliberadamente algo de aleatoriedad en su ataque para que no siga un patrón predecible, o tal vez sea un artefacto de alguna restricción que no podemos ver." [4] "Matt Boddy, Ben Jones, and Mark Stockley Sophos, RDP Exposed - The Threat That's Already at Your Door, 2019"

Uno de los lugares donde se concentra el mayor uso que hacemos de Internet es en nuestros hogares, y es allí donde deberíamos comenzar a aplicar algunos mecanismos de seguridad que nos protejan de ataques.

Al uso cotidiano que hacemos en nuestras casas con los equipos de cómputo y teléfonos móviles, se suma el Internet de las cosas (resultando en que muchos más dispositivos estén conectados todo el tiempo a la red), televisores, vehículos, smartwatches, entre algunos ejemplos.

A medida que crecen la infinidad de tareas con el uso de Internet, este nos ofrece más confort a la hora de realizar las labores diarias, como el acceso a la empresa desde cualquier lugar del mundo, y es allí, donde hay que tener en cuenta uno de los valores más importantes de esta, su información. Pues en la Internet nos brinda un acceso en tiempo real de todo lo correspondiente a la organización, a productos, bases de datos, información sus clientes, entre otros, pero también nos abre las puertas diferentes vulnerabilidades, como al robo de información, hackers, virus informáticos, etc.

"Un estudio de ESET, especializada en seguridad informática, pone de manifiesto que más del 80% de los trabajadores consultados utiliza sus ordenadores portátiles o memorias USB de uso personal en el entorno laboral. Y en porcentajes menores, aunque igualmente importantes, los encuestados también afirman servirse de sus "smartphones" (55%) y "tablets" (25%) para desempeñar su trabajo." [5] "Miloš Čermák and Robert Lipovsky, 26 Feb 2020"

En el artículo de Reyes, El virus" Wannacry", nos habla de cómo este virus creado por una persona tiene como fin robar los datos y recopilar información.

Reyes nombra el famoso virus "Virus de la Policía" donde explica la fuente del contagio a causa de los malos hábitos de navegación de algunos usuarios, estos malos hábitos común mente están relacionados a descargas de software pirata y visitar paginas poco confiables y/o seguras.

"Virus de la Policía, Bloquea el sistema operativo, mostrando una pantalla simulando ser el Cuerpo Nacional de Policía. Con la alerta de estar acusando al usuario de haber descargado pornografía infantil." [6] "Reyes, J. F. 2017"

Este tipo común de ataque se ve relacionado al pago por el desbloqueo del equipo,

y en sus diversas variables para sustentar el soborno, el virus, toma una fotografía del usuario habilitando la Webcam y mostrando su imagen en pantalla, esto con el fin de que no se tuviera ninguna duda sobre la identidad del autor y coaccionar aún más a la víctima a realizar el pago. [6] “Reyes, J. F. 2017”

Por ejemplo, un cibercriminal muchas veces utiliza la ingeniería social para convencer a un empleado de que divulgue las contraseñas de la empresa. Luego, el cibercriminal usa estas contraseñas para acceder a las redes corporativas para robar datos e instalar malware en la red de la empresa.

Todo lo que se necesita es un correo electrónico, una llamada telefónica o un mensaje de texto disfrazado de un compañero, amigo o empresa conocida y el cibercriminal ha ganado. El ciberdelincuente puede usar un tono familiar pero urgente para convencer a la víctima de actualizar su información bancaria o decirle a la víctima que para reclamar su premio tienen que proporcionar la información de su tarjeta de crédito.
Para el centro de respuestas ante incidentes cibernéticos de Paraguay, “El ransomware encripta archivos de bases de datos, máquinas virtuales, de código, archivos de correo, etc. Algo muy usual de estas variantes es que además encriptan los directorios compartidos en red a los que el equipo tiene acceso, perjudicando un amplio número de usuarios. Usualmente, el ransomware borra todas las instantáneas de recuperación, de manera que no se pueden utilizar para restaurar los archivos de la víctima” [7] “Ministerio de tecnologías de la información y comunicación, Paraguay”

Por otro lado, algunos factores de comportamiento del ransomware son los siguientes:

> “Se auto elimina del equipo, aunque en otros casos permanece latente en el sistema, de modo a seguir encriptado los nuevos archivos que se crean en la máquina”
>
> “Despliega un mensaje en pantalla y/o como fondo de pantalla, como una "nota de rescate" en la que proporcionan las instrucciones para el pago del rescate y la recuperación de los archivos, los montos para recuperar la información pueden variar entre 500 a 1500 Dólares”
>
> “En muchas de las variantes observadas, los cibercriminales exigen a la víctima que ésta contacte por correo electrónico, a través del cual le proporcionan las instrucciones específicas del pago, incluido el monto”

[7] “Ministerio de tecnologías de la información y comunicación, Paraguay”

Para la firma BDO Colombia, el teletrabajo es una valiosa herramienta estratégica para las organizaciones, pero es una puerta abierta al riesgo cibernético.

El Líder de Auditoría Forense, Javier Arévalo considera que:

“Los dispositivos que trabajan de manera remota pueden convertirse en un verdadero talón de Aquiles para la seguridad de la información corporativa y sobre todo para aquellas empresas que manejan datos sensibles”. [8] “*Leonardo soto lesmes, 2018”*

Para el gobierno de Donald Trump, el implementar el teletrabajo a cientos de miles de trabajadores federales y personal del Congreso, aumentara el riesgo de piratería y amenaza con abrumar los sistemas informáticos gubernamentales obsoletos.

Según el Washingtonpost, El Gobierno Federal y del Congreso de EEUU, se alistan para trabajar desde casa. “El brote de coronavirus puede provocar el mayor experimento de teletrabajo del gobierno federal hasta la fecha”

“El aumento en el teletrabajo marcará la primera prueba de su tipo para el gobierno, que ha luchado por actualizar y asegurar sus sistemas de tecnología arcana después de una serie de violaciones de datos dañinas durante la administración de Obama” [9] “Washingtonpost, 2020”

Greg Touhill, Ex jefe de seguridad de información federal durante la administración de Obama plantea que “Los trabajadores federales también podrían estar utilizando redes Wifi-públicas que no son seguras contra los piratas informáticos. Y serán más vulnerables a correos electrónicos de phishing y textos que parecen legítimos pero que en realidad contienen software malicioso. Por ejemplo, los piratas informáticos podrían fingir ser el jefe o compañero de trabajo de un empleado que está bloqueado de un sistema de correo electrónico del gobierno y en su lugar está utilizando una cuenta personal de Gmail”

Para la agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) del DHS, no está nada claro que los servidores informáticos del gobierno y las redes privadas virtuales, estén preparadas para implementar completamente el Teletrabajo, ya que no cuentan con las últimas actualizaciones de seguridad, pues muchos de sus empleados federales también carecen de computadoras portátiles y teléfonos emitidos por el gobierno, lo que aumenta el espectro de que inicien sesión desde sus hogares o cafeterías con dispositivos que carecen de características básicas de seguridad y no están corregidos contra los últimos errores.

Para Muriel E. Browser, alcalde del Distrito de Columbia. "Esta situación es preocupante y subraya exactamente por qué es tan importante que los miembros y su personal estén bien versados en las mejores prácticas de Ciberseguridad".
[9] “Washingtonpost, 2020”

### 2.2.2. PREGUNTA DE INVESTIGACIÓN

¿Ante la vulnerabilidad de la CIA a través de la modalidad de teletrabajo, qué medidas se pueden adoptar para mejorar los niveles de seguridad?

### 2.2.3. VARIABLES DEL PROBLEMA

Una vez construidas las guías de hardening, las variables identificadas en el problema y justificación tendrán un cambio de mejora una vez estas sean implementadas.

| Variables | Antes | Después |
|---|---|---|
| Fácil acceso y manipulación a los sistemas de información de la organización por medio del equipo de teletrabajo | Alto | Bajo |
| Ingreso, pérdida o robo de dispositivos | Medio | Bajo |
| Engaños basados en ingeniería social | Alto | Bajo |
| No conciencia del respaldo de la información del teletrabajador | Alto | Medio |
| Conexiones a redes inseguras | Alto | Bajo |
| Infección con códigos maliciosos | Medio | Bajo |

*Tabla 1. Variables del problema, Elaboración propia.*

## 2.3. JUSTIFICACIÓN

Hoy en día somos una sociedad hiperconectada donde alrededor del planeta casi 4.540 millones de personas estas conectadas a internet utilizando dispositivos electrónicos que se interconectan y viajan a través por otros medios de dispositivos electrónicos cuya función es transportar y enviar miles de millones de gigabytes por segundo a través de la internet por todo el planeta, donde se comparte información de cualquier tipo como personal, información sensible o confidencial de empresas u gobiernos. Esto hace que el hombre este siempre conectado y en las últimas décadas la experiencia de comunicación a facilitado el acceso y el alcance a otras personas por medio de la internet, algo que no se lograba a lo largo de la historia del hombre. [34] “Jesús Fernández, 2020”

Ahora, a raíz de lo sucedido mundialmente por el COVID-19 los trabajadores están cambiando su estilo de trabajar y cambiaron sus cubículos en la oficina por espacios de trabajo en sus salas, dormitorios o mesas en el hogar lo cual convierte cada espacio en el hogar en una pequeña oficina satelital utilizando su computador para acceder por medio sesión de datos a la empresa que está a una distancia considerable. Este modelo de trabajo ha crecido exponencialmente en muchos países y empresas, pero a la hora de la verdad no se sabe si en realidad estos equipos a distancia que se conectan de forma remota a las empresas estén bien seguras y protegidas contra ciberataques o robo de información confidencial de una organización que pone en jaque los pilares de la seguridad de la información que son la confidencialidad, la integridad y la disponibilidad.

Para que las empresas este bien preparadas, eleven su nivel de seguridad y mitiguen los ciberataques ante la modalidad de teletrabajo se tiene como propósito en este proyecto crear unas guías de hardening para que las empresas, pymes o corporaciones las utilicen y para que la función de las guías cumpla con la necesidad de este tipo de seguridad es indispensable conocer cuáles son los riesgos, amenazas y vulnerabilidades que podrían afectar a un empleador que trabajo desde su casa. De acuerdo a lo anterior se hará una investigación profunda y más importante conocer antecedentes de casos reales en el mundo o empresas que han sido víctimas o extorsionadas por ciberdelincuentes y más cuando el mundo está en una situación de emergencia por pandemia global donde las personas son obligadas a estar en confinamiento por los gobiernos y a laborar desde sus casas, ahí es cuando los hackers aprovechan la situación para para escudriñar y atacar estas oficinas satelitales vulnerables que son una buena entrada para robar información de las empresas.

Si bien las personas se han adaptado fácilmente a los computadores, móviles y programas en esta última década, existe gente que desconoce todavía los peligros reales en el mundo del ciber-espacio. Un gran porcentaje no conoce ni tiene los conocimientos suficientes de prevenir ataques y las consecuencias que esto conlleva, y más para los empleadores que trabajan desde una oficia satelital donde pueden ser blanco de robo de información, hackeos por mal uso del dispositivo en el hogar y navegación de sitios inseguros, y más si no tiene los programas o herramientas adecuadas como buen antivirus, firewall. Las empresas que hoy en día utilizan bastante las herramientas de videoconferencias para las reuniones virtuales no tienen en cuenta los riesgos que estos implica y podría afectar la operación de su organización.

Aunque el objetivo principal es construir unas buenas guías de hardening para mitigar estos ataques y elevar los niveles de seguridad para las personas que utilizan la modalidad de teletrabajo también se quiere recrear un escenario real con usuarios reales de una empresa utilizando una prueba de concepto aplicando el desarrollo de estas guías y ver que pasarías si no se utilizara y un después de ponerse en práctica estas guías, claramente todo el desarrollo de esta investigación no hay que limitarse solamente para las personas o empresas que utilizan el teletrabajo, también se podría utilizar para otros campos de seguridad como buenas prácticas dentro de una organización o para el común diario en la utilización de un computador o un móvil en el hogar.

Este proyecto es muy oportuno por la problemática mundial actual por el covid-19, de acuerdo a la revista science, las empresas estarán en la obligación de seguir utilizando el modelo de teletrabajo “El confinamiento no podría durar solo meses si no años” [33] “Revista Sciencie, 2020”, y a pesar de que tienen las herramientas y capacidades tecnológicas para mandar a sus empleadores a trabajar desde casa, las empresas no cuentan ni tiene la suficiente confianza porque no se tiene una vigilancia

constante de las acciones de sus empleadores y sus equipos en el hogar y un mal uso de este, puede ser una ventana de fácil acceso para los ciberdelincuentes a la información confidencial de las empresas. Por eso este proyecto tendrá una gran ventaja debido a lo sucedido actualmente en el mundo ya que proporcionará una guía formal y robusta para que las empresas tengan una herramienta con buenas prácticas de seguridad para que puedan orientar y capacitar a sus empleadores y lo pongan en práctica cuando estén en la modalidad de teletrabajo.

# 3. OBJETIVOS

## 3.1. OBJETIVO GENERAL

Construir guías de hardening qué eleven los niveles de seguridad en teletrabajo.

## 3.2. OBJETIVOS ESPECÍFICOS

- Identificar las principales amenazas de ciberseguridad a las que se enfrenta las empresas financieras que utilizan la modalidad de teletrabajo a partir de un análisis de inteligencia de amenazas (Threat Intelligence).

- Construir guías de hardening en Teletrabajo.

- Realizar una prueba concepto implementando la guía de hardening, que confirmen una mejora del nivel de seguridad en teletrabajo.

# 4. MARCOS DE REFERENCIA

Basado en los hallazgos de la web se encuentra que muchas empresas están optando por el teletrabajo ya que beneficia en gran medida el rendimiento y la flexibilidad para el trabajador generando mejor calidad de vida. Un estudio revelado indico que el 57% de las empresas nacionales han estado implementando trabajos más flexibles por requerimiento de los mismos empleados. De acuerdo a lo anterior lo que muestran las cifras es que van en aumento, y esto no solo se evidencia en Colombia sino en el mundo también. [13] "Teletrabajo.gov, 2019"

"En Estados Unidos ya existe una compañía en la que todos sus empleados son teletrabajadores. Se trata de Gitlab, un startup cuya valoración está por encima de los 1.000 millones de dólares. Los 789 empleados de Gitlab trabajan desde su casa, y tanto la compañía como los empleados se benefician de las ventajas que tiene trabajar en remoto" [10] "El Tiempo, 2019"

Si bien el teletrabajo ha crecido fuerte en las empresas, todavía falta mucho por crecer ya que la mayor parte de las empresas ya sea pymes o grandes compañías temen que el rendimiento laboral desde la casa sea más bajo que estando presente en la oficina, esto deriva de muchos factores como las distracciones del perro o la familia, no se tiene el control del empleador, el trabajo en equipo se pierde y más importante la seguridad de la información que maneja el empleador fuera de la empresa estaría expuesta a pérdida o robo.

Cuando se creó el ministerio de tecnologías de la información y comunicaciones se tuvo como propósito mejorar la protección de infraestructuras y de información el cual se denominó seguridad informática. Este pensamiento en las tecnologías ha ido evolucionando, en un principio solo se tuvo en cuenta la protección de los equipos de telecomunicaciones físicamente para prevenir daños o robos, luego se hizo un estudio para la protección del acceso a las redes limitándolo y actualmente ya se considera valioso el cuidado y la protección de información confidencial. [33] Mábel Mateus

Para esta nueva modalidad de trabajo se debe garantizar la información que manejan, los dispositivos y la del empleador. De acuerdo a lo anterior estos manejan mucha información sensible generando muchos riesgos que es necesario mitigar y prevenir lo más mínimo posible estableciendo protocolos adecuados de seguridad, para esto se recomiendo tener buen antivirus, respaldo o backups, acceso seguro a través de una VPN y los accesos bien restringidos a aplicaciones, servidores, base de datos y equipos de comunicaciones.

En la Publicación especial del NIST 800-114, se centra específicamente en la seguridad del teletrabajo que implica el uso de acceso a los recursos informáticos no públicos de las organizaciones. Ofrece consejos prácticos y reales para asegurar

los sistemas operativos y las aplicaciones de las computadoras de teletrabajo, así como las redes domésticas. Presenta recomendaciones básicas para asegurar los dispositivos móviles utilizados para el teletrabajo. El documento también presenta consejos sobre la protección de la información almacenada en las computadoras de teletrabajo y los medios extraíbles. [29] "Guide to Telework and Bring Your Own Device (BYOD) Security, NIST Special Publication 800-114, 2016"

"Se considera conveniente que se establezcan patrones de seguridad adecuados con la implementación del teletrabajo contemplando objetivamente tanto las necesidades de la entidad como las del teletrabajador" [11] "Villada Arango, Lizeth Andrea, 2018"

Basado en las mejores prácticas, la ISO 27001 nos describen los controles en su Anexo A, y detallados en ISO 27002 , pueden ayudar a las organizaciones a manejar los riesgos del teletrabajo en varias formas, y la principal es la definición de una política de dispositivos móviles y teletrabajo basada en controla A.6.2.1 (Política de dispositivo móvil) y control A.6.2.2 (Teletrabajo). [31] "Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información, ISO, NTC. IEC 27001, 2013"

A través de esta política, una organización puede establecer las reglas para la implementación de salvaguardas para proteger la información a la que se accede, procesa o almacena fuera de la organización.

En la Publicación especial del NIST 800-46, Esta publicación proporciona información sobre consideraciones de seguridad para varios tipos de soluciones de acceso remoto, y hace recomendaciones para asegurar una variedad de tecnologías de teletrabajo, acceso remoto y BYOD. También da consejos sobre la creación de políticas de seguridad relacionadas. Para mejorar la seguridad de las tecnologías de teletrabajo y acceso remoto de las organizaciones, así como para mitigar mejor los riesgos que plantean las tecnologías controladas por BYOD y por terceros a las redes y sistemas de las empresas. [2] "Guide to Enterprise Telework, Remote Access, and Bring Your Own, Device (BYOD) Security, NIST Special Publication 800-46, 2016"

El aumento del teletrabajo significa que hay un amplio espacio para los ciber atacantes, parte del problema es que muchas personas trabajan de forma remota, incluso cuando pasan la mayor parte del tiempo en la oficina, incluso si no se dan cuenta.

Según un nuevo estudio de CybSafe, un tercio de todas las empresas del Reino Unido han sufrido ciberataques como resultado directo de sus empleados que trabajan de forma remota. "Capacitar al personal para que reconozca y lidie con las amenazas en el trabajo, fuera de casa y en el hogar es importante" [12] "Oz Alashe, CybSafe, 2018"

## 4.1. MARCO CONCEPTUAL

Durante el proceso de investigación se llegó a profundizar en diferentes aspectos y diferentes artículos que son clave para la implementación de las técnicas y guías que ayudaron a la solución para el desarrollo de la seguridad informática en la modalidad del teletrabajo.

### ¿Qué es la seguridad de la información?

La seguridad de la información es la encargada de proteger y reducir los riesgos hasta un punto en que pueda ser aceptable para minimizar las amenazas por robo o modificación en la información. Los activos con información pueden encontrarse en diferentes maneras ya sea en una forma digital, verbal o mensajes escritos y a pesar de que se encuentre en varios formatos esta información tiende a tener la necesidad de tener protecciones adecuadas de acuerdo a su criticidad o importancia y por eso es importante la seguridad de la información.

"la seguridad de la información se sustenta de metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos, que soportan la idea de protección en las distintas facetas de la información; también involucra la aplicación y gestión de medidas de seguridad apropiadas, a través de un enfoque holístico" [36] "Miguel ángel Mendoza, 2015"

### ¿Qué es la ciberseguridad?

La ciberseguridad es la encargada de la protección de activos de información digital, procesada, almacenada y transportada por medio de sistemas informáticos ante amenazas que ponen en riesgo la información.

De acuerdo a la norma ISO27001 este activo de un sistema de información es de gran valor para una empresa ya que estos sistemas trabajan en conjunto e interconectados y en caso latente ante una amenaza podría afectar todo el sistema informático de una organización y generar pérdida de productividad y dinero. La ciberseguridad solo está enfocada a un formato digital. [36] "Miguel ángel Mendoza, 2015"

### ¿Qué es una VPN?

VPN o en por sus siglas "red privada virtual" permite crear redes privadas y locales que se interconectan a otra red privada sin la necesidad que estar físicamente en el mismo lugar, esta conexión funciona a través del internet del proveedor contratado sin embargo se crea un túnel cifrada conectando una punta del mundo a otra sin que el proveedor del internet sepa a que está accediendo. Las ventajas que una red VPN es ofrecer es mayor flexibilidad, seguridad y tu dirección IP no será rastreada ya que es la que te da el servidor de VPN y no la que te da el proveedor de internet. Uno de los usos más frecuentes es la del Teletrabajo y evitar censura o bloqueos a

páginas web en el país local. [14] ”Iván Ramírez,2019”

**¿Qué es un firewall?**

Un firewall o cortafuegos es un software o hardware diseñado para proteger un computador. Actualmente están implementado en todos los ordenadores sin darte cuenta cumpliendo las funciones de protección e integrado con el antivirus.

El firewall en el mundo de la informática es un sistema de seguridad cuya función es bloquear y restringir accesos no autorizados a un sistema informático mientras que para otros servicios si permite accesos de acuerdo al propósito requerido. Los cortafuegos también son utilizados en redes de una empresa, locales o intranets cumpliendo como primera medida de seguridad. Esta medida de protección se empezó a utilizarse con la llegada del internet evitando la intrusión de hacker que violan y se infiltran en sistemas informáticos realizando ataques de malware o robando información. Por eso llego la necesidad de mejorar la seguridad y los desarrolladores en el año 1988 crearon las primeras versiones de cortafuegos y con el tiempo fueron evolucionando con mejoras que ayudaban a analizar el tráfico entrante y saliente evitando posibles amenazas. Actualmente la finalidad sigue siendo la misma de mejorar la seguridad en un ordenados o en redes amplias y seguir estableciendo criterios de seguridad. [15] “Yubal FM, 2019”

**¿Qué es un antivirus?**

Los antivirus son software creados con el único fin de prevenir, bloquear, detectar y eliminar cualquier intrusión o archivo ejecutable que puede comprometer un sistema informático, que son descargados en internet.

Es importante saber la función de un antivirus y para qué sirve ya que es muy importante cuidad un computador y la mejor manera es tener un buen antivirus. Existen programas malintencionados a los que llamamos virus, y su propósito es de dañar o modificar cualquier elemento informático.

Normalmente estos virus son cada vez más sofisticados y difíciles de detectar, con solamente descargar un archivo contaminado por virus, puede este infectar y propagarse por todo un sistema informático de una empresa y perjudicar varios equipos al mismo tiempo a que estos están conectados entre sí,

Cualquier dispositivo electrónico puede ser afectado como tables, teléfonos móviles y por supuesto servidores de datos de una empresa. Actualmente se pueden encontrar muchos tipos de virus creados con diferentes propósitos que representan una amenaza a los sistemas informáticos.

De acuerdo a lo anterior y la gran cantidad de amenazas informáticas que existen y que se crean constantemente, es difícil que encontrar un antivirus que cumpla

totalmente con las funciones y necesidades de protección, por eso los antivirus están en constante actualización ante nuevas amenazas y este sería su fin desde la creación del antivirus. [16] “Vanguardia, 2018”

**¿Diferencias entre puertos UDT/TCP?**

Los puertos UDP y TCP son protocolos de capa de transporte basadas en IP que se utilizan para el transporte de paquetes para la comunicación lógica entre equipos. Ambos protocolos trabajan bajo la capa del internet y la más utilizada es la TCP.

TCP y UDP proporcionan comprobación de servicios sin embargo UDP no es tan confiable ya que no garantiza la integridad porque solo entrega los datos en el proceso a cada host, pero no recibe una confirmación al emisor, a diferencia de TCP este si proporciona una transferencia de datos confiable ya que garantiza que las entregas de mensajes se envíen correctamente sin perdidas, o errores que se presenten en el transcurso de su recorrido. TCP siendo las más utilizada en conexiones de redes ya que ofrece una mejor comunicación, cuando un paquete recibido es corrupto o presenta errores, el protocolo TCP le dice al destinatario que solicite nuevamente al receptor él envió del paquete confirmando una buena recepción. UDP no proporciona este tipo de control de gestión. [17] “Dana Elfenbaum, 2019”

## 4.2. MARCO TEÓRICO

Las empresas hoy en día han encontrado en la tecnológica la mejor herramienta para llevar el trabajo al empleador y no el empleador al trabajo, este ha sido un gran aliado para que las empresas fueran más eficientes. Todo inicio durante la década de los 70 durante la crisis petrolera en un momento de crisis donde la inflación estaba muy por encima, el físico Jack milles considerado el padre del teletrabajo creo el concepto de telecommuting para optimizar los recursos y de esa manera llevar el trabajo al empleador. La idea constaba en crear terminales remotas cerca a las oficinas y así los trabajadores evitaban desplazarte en vehículos derivados del petróleo ahorrando energía. Este experimento fue utilizado primeramente en la empresa Montgomery Ward.

Con la salida de la crisis el teletrabajo presento una gran oportunidad para las empresas permitiendo enviar el trabajo al hogar sin la necesidad de desplazar al trabajador.

“Hacía los años 80, el desarrollo tecnológico conduce a un paso importante en la disposición del teletrabajo en las empresas. Algunos países europeos, deciden adoptar el nuevo modelo para equilibrar las altas tasas de desempleo y fomentar la apropiación de las nuevas tecnologías. Para esto, fue necesario mejorar la infraestructura técnica de telecomunicaciones en las organizaciones, y establecer

metas con los teletrabajadores para la implementación exitosa y sostenible”. [18] “Seguridad, Leonardo, 2016”

Con los avances tecnológicos se empezaron a crear transferencias de archivos por medio del FTP y más adelante aparece la WWW (World wide web), durante la década de los 90 el internet empezaba a crecer y de ahí nacieron todas las plataformas o páginas que actualmente conocemos, también se empezó a masificarse el uso de herramientas portátiles como computadores y móviles.

Algo que impulso a las empresas a implementar más el teletrabajo fue el atentado del 11 de septiembre en estados unidos, con el miedo abundando en los trabajadores en las oficinas y ante el terror que volviera a pasar el teletrabajo se da como plan de choque para que no paren las operaciones trabajando desde los hogares obteniendo resultados positivos.

En la crisis económica entre el año 1998 y 2002 ocurrida en Argentina la tasa de desempleo ascendió hasta superar el 20% lo que genero pensar en nuevas ideas que permitiera disminuir los costos a las empresas y para esto el uso del internet fue un gran aliado lo que permitía que muchos empleados empezaran a trabajar por su propia cuenta utilizando todas las herramientas que ofrecía la web. [32] Ministerio Tic Colombia, 2016.

## 4.3. MARCO JURÍDICO

### LEY 1221 DE 2008

> “Establece el reconocimiento del Teletrabajo en Colombia como modalidad laboral en sus formas de aplicación, las bases para la generación de una política pública de fomento al teletrabajo y una política pública de teletrabajo para la población vulnerable. Crea la Red Nacional de Fomento al Teletrabajo, con el fin de promover y difundir esta práctica en el país e incluye las garantías laborales, sindicales y de seguridad social para los Teletrabajadores.
>
> **ARTÍCULO 1o. OBJETO.** La presente ley tiene por objeto promover y regular el Teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones (TIC).
>
> **ARTÍCULO 2o. DEFINICIONES.** Para la puesta en marcha de la presente ley se tendrán las siguientes definiciones: Teletrabajo. Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo”. [19] “Ministerio de telecomunicaciones, 2008”

## Decreto 884 DE 2012

"Especifica las condiciones laborales que rigen el teletrabajo en relación de dependencia, las relaciones entre empleadores y Teletrabajadores, las obligaciones para entidades públicas y privadas, las ARLS y la Red de Fomento para el teletrabajo. Así mismo establece los principios de voluntariedad, igualdad y reversibilidad que aplican para el modelo.

**ARTÍCULO 5°.** Uso adecuado de equipos y programas informáticos. Para el sector privado el empleador debe incluir en el reglamento interno de trabajo, lo relacionado con el adecuado uso de equipos, programas y manejo de la información, con el fin de permitir y facilitar la implementación del teletrabajo como una forma de organización laboral" [19] "Ministerio de telecomunicaciones, 2008"

## Resolución 2886 de 2012

"El objeto de la presente resolución es definir las entidades que harán parte de la red nacional de fomento al trabajo, las actividades que le compete desarrollar y su funcionamiento

Que una de las acciones de la Red Nacional de Fomento al Teletrabajo, prevista en el numeral 1 del artículo 12 del citado Decreto 0884 de 2012, es convocar la integración de mesas de trabajo considerado para ello aspectos tecnológicos, formativos, organizativos, legales y una mesa especial, sobre población vulnerable, las cuales deberán generar una agenda anual para el desarrollo de la políticas definidas en la Ley 1221 de 2008 en cuanto al fomento del Teletrabajo, generación de incentivos y en la políticas especial de Teletrabajo en la población vulnerable (Ministerio del trabajo. Bogotá)" [20] "Ministerio de trabajo, 2012"

## Proyecto de acuerdo 128 de 2013

"Contexto: El presente Proyecto de Acuerdo tiene como objetivo mejorar las condiciones laborales del trabajador, empleado o colaborador, su calidad de vida, la de su familia y en general la relación con el entorno, además de causar un impacto positivo en la movilidad y en el medio ambiente para Bogotá.

Bajo esta premisa, es pertinente señalar la sentencia C-337 de 2011 de la Corte Constitucional, ya que se constituye en el primer pronunciamiento jurídico, en el cual este Alto Tribunal plantea directamente la figura del teletrabajo, ratificando que se deben garantizar a los teletrabajadores distintos beneficios, entre ellos el subsidio familiar y todas las prerrogativas propias consagradas en la legislación laboral vigente.

Con este normativo, no se intenta promover o permitir formas de explotación o flexibilidad laboral, en perjuicio del trabajador, que deriven en la promoción de algún tipo de informalidad laboral; la práctica del Teletrabajo debe constituirse en apoyo al trabajador y a la promoción del empleo digno en el Distrito Capital". [21] "Alcaldía de Bogotá, 2013"

## 4.4. MARCO GEOGRÁFICO

Hoy la constante y acelerada evolución de la tecnología, así como la relación del acelerado crecimiento en el tráfico capitalino, se ha convertido en un tema de discusión en Colombia. Bogotá considerada como la tercera cuidad con el peor tráfico del mundo y en la que más horas se pasan las personas en el tráfico “272 al año” se ve reflejado en el alto crecimiento demográfico, producto de los procesos económicos, sociales y políticos que tienden hacia la híper - concentración de población, sin embargo en este estudio se abordará el uso de la modalidad de Teletrabajo en las organizaciones, que tiene que ver con el incremento a través de los años de nuevas modalidades de trabajo correlacionadas a temas de movilidad, productividad y reducción de costos.

Esta nueva modalidad ha provocado la expansión de nuevas alternativas de empleo, conciliando la vida personal y laboral, permitiendo gestionar el tiempo al no tener que depender de factores externos, como el desplazamiento a las empresas, o los horarios del transporte público. Los antecedentes se relacionan a la inclusión sociolaboral de la población vulnerable, gracias al desarrollo tecnológico, como son la población en condiciones de discapacidad, aislamiento geográfico y cabezas de familia.

“Recientemente en Colombia se firmó el pacto por el teletrabajo con el sector justicia, el cual diseñará e implementará un plan maestro que permita a la población privada de la libertad capacitarse y posteriormente ser calificada para teletrabajar” [22] “Libro Blanco. El ABC del teletrabajo en Colombia”

## 4.5. ESTADO DEL ARTE

En la actualidad los principales riesgos de seguridad a los que puede estar expuesta una empresa, al no tener en cuenta las vulnerabilidades asociadas ante el uso dispositivos personales (BYOD) en entornos de trabajo, y de mencionar las pocas medidas de seguridad como configuraciones seguras (hardening) que las empresas hoy manejan, estas, se ven preocupadas ya que generalmente al no tener una política de seguridad de acceso, pueden estar potencialmente expuestas al robo de información.

“La probabilidad de pérdida de información y las consecuencias que esto acarrearía para la empresa u organización son una amenaza que no se puede olvidar y desde el campo de la seguridad de la información se debe trabajar en el diseño de un sistema de gestión centrado en la prevención y mitigación de los daños.” [23] “Revista Cintex 20, Pág. 119, 2015”

CSIRT-CV, Centro de Seguridad TIC de Valenciana, en su guía de seguridad estable que antes de implantar una política de BYOD en una organización, es

fundamental realizar un análisis del riesgo y abarcar las siguientes medidas de seguridad.

> “Disponer de un mecanismo de reemplazo de equipos en caso de pérdida o avería de estos, para garantizar que el empleado pueda seguir desempeñando sus tareas habituales”
>
> “Establecer medidas técnicas para garantizar las mismas condiciones de seguridad que tendría la información en caso de estar almacenada en un equipo propio de la organización en lugar del empleado. Para ello se recomiendan cuentas de usuario independientes o incluso el uso de sistemas operativos o máquinas virtuales separadas, además de implantar el resto de los controles habituales (borrado remoto, cifrado, copias de seguridad, control de acceso, etc.)”
>
> “Establecer medidas para evitar el acceso fortuito a información corporativa por otros usuarios del equipo aparte del propio empleado: familiares o similar”

[24] “Guía de seguridad en el Teletrabajo, 2015”

Para Bustos Guáqueta, C. A. (2015), Expone que según el tamaño, necesidad y naturaleza de la empresa se podrán definir las políticas que cubran por lo menos los siguientes ítems:

- Procedimiento de solicitud voluntario y autorización de teletrabajo
- Perfiles de usuarios que podrán optar por el teletrabajo y definir los permisos de acceso remoto.
- Procedimiento de conexión remota alterna en caso de fallos
- Posibilidad de utilizar equipos personales (BYOD) para el teletrabajo y su medida de seguridad.
- Política para el almacenamiento de la información de la empresa equipos personales o medios extraíbles.
- Procedimiento para proteger físicamente los accesos a los equipos de cómputo de la empresa.
- Cláusulas de responsabilidad de la información a custodio por el empleado bajo teletrabajo

[25] “Bustos Guáqueta, C. A. 2015”

En la Publicación especial del NIST 800-46, esta plantea que las organizaciones deberían asumir que los dispositivos cliente de teletrabajo, que se utilizan en una variedad de ubicaciones externas, son particularmente propensos a la pérdida o robo, y estos serán adquiridos por partes maliciosas que intentarán recuperar datos confidenciales de ellos, o aprovechar los dispositivos para obtener acceso a la red

empresarial.

“Desarrolle una política de seguridad de teletrabajo que defina los requisitos de teletrabajo, acceso remoto y BYOD” [2] “Guide to Enterprise Telework, Remote Access, and Bring Your Own, Device (BYOD) Security, NIST Special Publication 800-46, 2016”

En 2017 para España, el Teletrabajo comprendía amplias perspectivas de desarrollo en el futuro, y nuevas maneras de trabajar a distancia. Para aquellas organizaciones españolas, El teletrabajo regulado legalmente tenía que contar documentos previos de seguridad, como políticas de uso de los recursos informáticos, debían definir el ámbito de los controles, así como respetar, en su caso, los principios de protección de datos. Los elementos de seguridad debían incluir guías responsables y respetuosas argumentando los controles empresariales ante del uso de Internet. [26] “Wolters Kluwer España, 2017”

El Instituto nacional de Ciberseguridad (INCIBE) de España, en su publicación, “Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario”, da a conocer los riesgos que se pueden presentar ante el uso de este tipo de dispositivos en las empresas. [1] “Una guía de aproximación para el empresario, 2017”

Argumenta en su guía que tanto los dispositivos móviles personales, como la información corporativa que manejan estos, deben estar protegidos eficazmente, estableciendo medidas de seguridad que contribuyan a reducir todo lo posible los riesgos a los que están expuestos.

“La información que manejamos en nuestras empresas es uno de los activos más importantes que hay que proteger” [1] “Una guía de aproximación para el empresario, 2017”

Leal Cubaque en su artículo “La seguridad de la información en dispositivos móviles personales de uso profesional”, se basa en la ISO 27001 y el cómo reducir los riesgos. Como primera medida expone, se debe identificar los dispositivos críticos que tiene la organización, esto se puede hacer de acuerdo con la clasificación de información que se tenga y al grado de vulnerabilidad, esto con el fin de identificar que controles son necesarios para reducir el riesgo, sustenta el artículo informando la implementación del proceso de Hardening

“Debemos asegurar tanto los dispositivos móviles para uso profesional como los datos de la empresa, realizando hardening de configuración a cada uno de los elementos donde se almacena o transporta la información, sin dejar de lado que estamos trabajando con equipos personales y no podemos restringir todo. El endurecimiento de configuraciones (Hardening), servirá para minimizar algunos riesgos como acceso no autorizado, perdida de dispositivos, y algunos riesgos.”[27] “Leal Cubaque, Edicson Daniel. 2019”

Para COLOMBIA, el Ministerios TIC y del Trabajo, desarrollo una herramienta que fomenta y orienta a las organizaciones a innovar en la modalidad de Teletrabajo, proyectado a entidades públicas y privadas del país. En esta metodología que nos presenta en “Libro Blanco. El ABC del teletrabajo en Colombia” nos define qué, “la política de seguridad debe ser un documento de alto nivel, que deja claro la responsabilidad de la alta dirección con la seguridad de la información, siendo este de obligatorio cumplimiento”

“La revisión periódica de la política de seguridad constituye un proceso de mejora continuo que permite mantenerla vigente ante los constantes cambios del entorno tecnológico y nuevas amenazas.” [22] “Libro Blanco. El ABC del teletrabajo en Colombia”


*Figura 1. Libro Blanco de teletrabajo en Colombia - versión 3.0, Pág. 85*

# 5. METODOLOGÍA

## 5.1. FASES DEL TRABAJO DE GRADO

Para el desarrollo de la construcción de las guías de hardening, se empezará por describir y conocer las características esenciales de la modalidad de teletrabajo y problemática de seguridad que este enmarcaba, los riesgos principales a los que se enfrentan las entidades financieras que no cuentan con una política de seguridad, evidenciando esta problemática en la justificación y los datos recopilados en los antecedentes.

En este, se presentarán los métodos de investigación más adecuados en los que el equipo de trabajo se ha basado para analizar los factores de amenaza que se enfrentan las entidades financieras que implementan la modalidad de teletrabajo. Se aplicarán las técnicas y tácticas basadas en Threat intelligence. Además, se realizarán consultas a fuentes documentales e investigativas, con el fin de analizar las principales amenazas críticas que se presentan en teletrabajo.

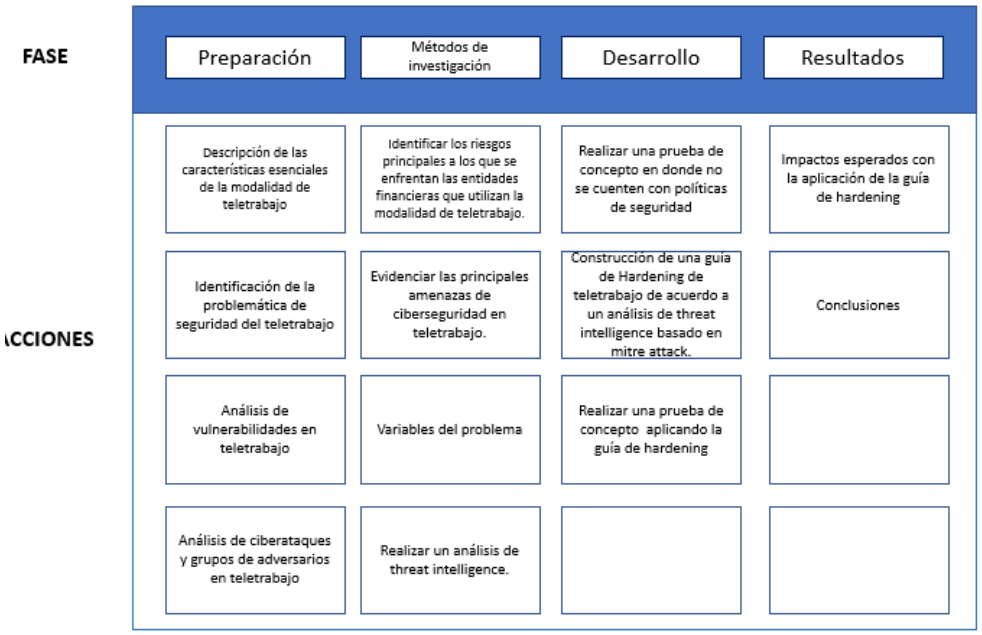


*Figura 2. Fases del trabajo de grado, Elaboración propia.*

Por otro lado, con el objetivo de exponer los resultados del desarrollo de la guía de hardening, se evidenciará la problemática en una prueba concepto y el cómo la guía de hardening, ayudará a aquellas organizaciones a reducir los riesgos y elevar los niveles de seguridad en teletrabajo.

Para lograr la construcción y elaboración de unas guías de teletrabajo para entidades financieras, se realizó un análisis de Threat intelligence basado en mitre att&ck, esta herramienta de mitre att&ck nos ayuda a conocer una gran variedad de técnicas y tácticas de adversarios que actualmente intenta vulnerar y penetrar sistemas informáticos de empresas y organizaciones a nivel mundial. ¿Entonces que es Mitre att&ck?

- Es una base de conocimientos de los comportamientos de un adversario.

- Es un marco que une muchas cosas diversas que hacen los adversarios.

- Es una enciclopedia de diferentes actividades de los malos actores

Mitre att&ck se basa en observaciones del mundo real, en acciones que han realizado adversarios en el pasado o lo que probablemente están haciendo, Mitre att&ck no incluye pruebas teorías o conceptos si no en hechos reales que ha pasado para priorizar esos comportamientos. Mitre att&ck es gratuito, abierto y accesible a nivel mundial, cualquiera lo puede utilizar desde estudiantes hasta corporaciones.

ATT&CK utiliza tabla llamada matriz donde se va recopilando toda la información en tiempo real los distintos ataques orientados a empresas, dispositivos móviles o preataques. En la matriz se podrá observar un conjunto de columnas que contiene las siguientes categorías:

- Acceso inicial
- Ejecución
- Persistencia
- Escalado de privilegios
- Evasión de defensas
- Acceso a credenciales
- Identificación
- Movimiento lateral
- Recolección
- Comando y control
- Exfiltración
- Impacto

Cada una de estas categorías contiene unas subcategorías o tácticas, que son los objetivos técnicos de alto nivel de un atacante. Por cada una de sus tácticas contiene formas más detalladas de cómo se logran estos objetivos de un atacante. Una ejemplo seria la categoría de acceso inicial que contiene una subcategoría llamada Spearphishing Link lo cual consiste en una técnica de ingeniería social dirigidas en su mayoría por correo electrónico con el fin de utilizar métodos

engañosos como un email falso que contiene un link malicioso para contaminar una red corporativa.

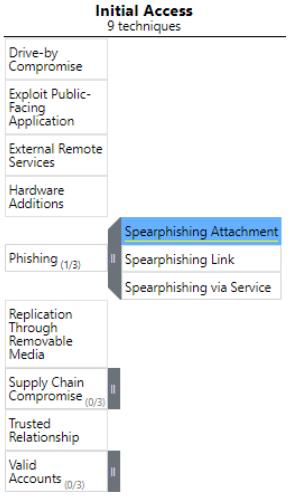


*Figura 3. Mapa conceptual Initial Access - Mitre att&ck*

Detrás de cada una de estas técnicas, hay mucha más información que incluye procedimientos e información relevante de la forma de ataque, para empezar cada técnica contiene una descripción en texto que describe cual es la actividad, por qué el atacante lo estaría haciendo y muestra varios niveles de detalle técnico.

## 5.2. INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

Entre las herramientas de investigación aplicadas como instrumentos de apoyo al presente trabajo se encuentran las siguientes:

La observación: esta técnica se fundamenta, y encuentra contexto en el tipo de problemática descrito en este, y se realizará desde la perspectiva de la necesidad evidenciada por la llegada de la pandemia COVID-19, y de todos los sectores de la economía, en seguir desarrollando sus actividades laborales mediante el teletrabajo y/o trabajo remoto, sin tener en cuenta los factores de inseguridad que representa aplicar este tipo de organización.

Revisión conceptual de teletrabajo y seguridad: como situación previa a la técnica anteriormente mencionada, se hará necesario la revisión bibliográfica de los conceptos asociados a teletrabajo, los diferentes modelos de seguridad, y la seguridad aplicada al teletrabajo, apoyados a partir de la revisión en libros, normas técnicas, y dimensiones nacionales e internacionales, los cuales han sido punto

clave para el tipo de investigación.

Revisión documental: se abordará inicialmente toda la documentación relacionada a incidentes y vulnerabilidades en teletrabajo utilizando threat intelligence, antecedentes y características especiales de inseguridad que presentan las entidades financieras, consulta a tesis de grados, libros y revistas científicas, permitiendo así, hacerse a la idea de cómo desarrollar el proyecto y dar solución a la problemática abordada.

Prueba de Concepto: para este proceso, se llevará a cabo realizar pruebas de contaminación de phishing en una maquina utilizando las herramientas aprendidas en lo que llevamos cursado de la especialización, simulando un ambiente de teletrabajo con el objetivo de mostrar los impactos generados sin y con la aplicación de las guías.

## 5.3. POBLACIÓN Y MUESTRA

Nuestro proyecto va enfocado en una población específica que son los funcionarios de entidades financieras que trabajan por medio del teletrabajo, sin embargo a nivel general ya que no contamos con cifras exactas de este tipo de funcionarios podemos decir que el teletrabajo en los últimos 4 años en Colombia el crecimiento de esta nueva modalidad ha crecido en un 287% y los que más aplican este modelo son las pymes. “Unos de los estudios indican que desde el 2012 al 2018 los teletrabajadores pasaron de 31.553 a 122.278 trabajadores, así mismo durante este mismo periodo las empresas que implementaron este modelo también aumento de un 4.292 a 12.912 empresas”. Según indica un experto en tecnología con el desarrollo de las nuevas tecnologías y el pasar de los años este modelo seguirá en crecimiento dando como oportunidad a las empresas de reducir costos. “En relación con esto último, en el informe también indica que las ciudades en las que más se teletrabaja sea en las más grandes y en las de mayor congestión vehicular. En primer lugar, está Bogotá, con 63.995 teletrabajadores; de segunda está Medellín, con 29.751, y en tercera posición está Cali, con 13.379”. Aunque todavía no existe un informe preciso actual del uso del teletrabajo en el país, es muy cierto que desde que inicio el confinamiento por el covid-19 este modelo ha crecido también exponencialmente durante los inicios del año 2020. [28] “La república, 2018”

## 5.4. ALCANCES Y LIMITACIONES

### Alcance

En el alcance del desarrollo del proyecto se contempla conocer e identificar las amenazas y vulnerabilidades para las entidades financieras y donde los usuarios trabajan desde la modalidad de teletrabajo, al igual desarrollar unas guías de

hardening de seguridad para minimizar el impacto de amenazas para este tipo de teletrabajador. También se quiere determinar el uso de estas guías por medio de una prueba de concepto, sin el uso de las guías y después con el uso de las guías con el fin de mostrar resultados positivos. De acuerdo a lo anterior este sería el alcance del proyecto.

**Limitaciones**

Nuestra limitación en este proyecto será en la fase de las pruebas de concepto, donde nos limitaremos solamente a realizar el escaneo de vulnerabilidades o pentesting utilizando los programas aprendidos en el transcurso de la especialización en máquinas de pruebas, simulando un ambiente de teletrabajo, mostrando los resultados.

# 6. PRODUCTOS A ENTREGAR

Este trabajo de grado se relaciona en el contexto del objetivo general y específicos, los productos a entregar son:

- Documento Análisis de Threat Intelligence: Para este punto se presenta el análisis realizado de una Inteligencia de amenazas “Threat Intelligence”, para conocer que grupos de adversarios están interesados en atacar a las entidades financieras y como desde sus técnicas y tácticas podrían vulnerar un funcionario que labora desde su casa.

- La Guía de Hardening: Se presentará las consideraciones técnicas de seguridad sobre cómo reducir y mitigar los ataques vistos en el documento de análisis de Threat Intelligence. **Guía de Hardening- Anexo A.**

- Prueba de Concepto: Se presenta una prueba de concepto, en donde se demuestra la efectividad de la guía de hardening reduciendo el riesgo y evitando el cumplimiento del objetivo de los diferentes grupos de amenazas. **Prueba de Concepto - Anexo B.**

- Articulo IEEE: Se presentará artículo realizando el desarrollo y muestra del análisis de Threat Intelligence con el fin de conocer los diferentes grupos de amenazas que están atacando a las organizaciones financieras en teletrabajo. **Articulo IEEE - Anexo C.**

# 7. ENTREGA DE RESULTADOS ESPERADOS E IMPACTOS

## 7.1. DOCUMENTO ANÁLISIS THREAT INTELLIGENCE

### 7.1.1. INTRODUCCIÓN

A medida que el mundo se une y utiliza todos los recursos disponibles para contener la pandemia mundial del COVID-19, esta creó un cambio radical en la forma en que trabajamos y vivimos, y desafortunadamente agregó una chispa detonante para el crecimiento exponencial de ciberataques y habrá quienes intentaran aprovechar la crisis con propósitos nefastos.
A medida que las organizaciones continúan impulsando las prácticas comerciales a través de la transformación digital, los desafíos que enfrentan también evolucionan, con un gran número de empleados y estudiantes que trabajan desde casa, las empresas se enfrentan a un riesgo cada vez mayor de convertirse en víctimas del ciberdelito.
En nuestro informe de Threat intelligence, identificamos los desafíos únicos que enfrentan las organizaciones financieras que implementaron la modalidad de teletrabajo, y las consideraciones operativas, tácticas y estratégicas que las organizaciones deben aprovechar para administrar el riesgo.
Así también identificamos tres grupos de amenazas de Mitre att&ck los cuales utilizan como vector de ataque, las tácticas de acceso inicial y de ejecución para comprometer y vulnerar una entidad financiera por teletrabajo.
Con esta composición de conocimiento, los líderes de ciberseguridad obtendrán una mayor conciencia de la situación, lo que les permitirá orientar procesos y respaldar las decisiones para ayudar a mejorar su postura en seguridad.
Además, los defensores de la ciberseguridad deben aprovechar esta información para evaluar las amenazas identificadas frente a su propio perfil de riesgo y huella tecnológica para reforzar la detección de amenazas específicas y los esfuerzos en respuestas.

### 7.1.2. ALCANCE

El alcance para este documento es identificar las amenazas y vulnerabilidades a las que se enfrentan las entidades financieras, hacer un análisis de inteligencia de amenaza para conocer que tácticas y técnicas utilizan los adversarios o grupos de amenazas para afectar la integridad, disponibilidad y confidencialidad de un funcionario de una entidad financiera que laborar desde casa y también mostrar como poder mitigar o defenderse de estos ataques.

### 7.1.3. EL IMPACTO DEL COVID-19 Y AUMENTO DE LAS CIBERAMENAZAS EN LAS ORGANIZACIONES FINANCIERAS

El COVID-19 está afectando todos los aspectos de la sociedad y alterando vidas, así como las operaciones comerciales.

Muchas empresas se han visto afectadas por el brote; algunas han cerrado y otras probablemente no podrán recuperarse; algunas están prosperando debido a la mayor demanda de COVID-19 y han puesto un negocio particular.

Pero incluso esas organizaciones están cambiando la forma en que operan a un nivel muy básico. Las organizaciones están participando en las operaciones de trabajo desde casa y apoyando el aislamiento físico para ayudar a proteger a su personal. En este entorno, las organizaciones necesitan aprender a seguir operando mientras gestionan el bienestar de su gente, junto con las cambiantes demandas del mercado.

Algo comprensible, la gestión de cambios inesperados a menudo significa que la "seguridad" pasa a un segundo plano, mientras que las empresas se centran en "hacer las cosas". Eso significa que se vuelve aún más importante para los gerentes y grupos de seguridad enforcarse en los aspectos de seguridad que están diseñados para permitir que las empresas, "hacer las cosas de manera segura", permitan operaciones seguras y protegidas de una manera que no puede de lo contrario sería posible.

El sector financiero está ligado en la vida diaria de las personas de todo el mundo y es el núcleo mismo de las economías globales. Las entidades financieras permiten a los ciudadanos y las organizaciones de todo el mundo a administrar las finanzas, el comercio y operar de diferentes maneras.

En consecuencia, los actores de amenazas tienen mucho que beneficiarse de un ciberataque exitoso contra cualquier institución financiera, y los adversarios ya se han dado cuenta de este hecho.

Esta amenaza no solo se aplica a los bancos, sino también a las bolsas, administradores activos, proveedores de tecnológica, aseguradoras, cajas de compensación y liquidación, así como a las cadenas de suministros de las instituciones de gobierno.

Como resumen de los eventos que llevaron a la realización de este informe, la siguiente línea de tiempo nos cuenta los diferentes ciberataques realizados a entidades financieras en este año 2020.

## 7.1.4. LINEA DE TIEMPO


*Figura 4. Línea de tiempo, ataques entidades financieras – Elaboración propia.*


*Figura 5. Línea de tiempo, ataques entidades financieras – Elaboración propia.*

### 7.1.5. ANÁLISIS DE AMENAZAS

En este informe, las amenazas cibernéticas al sector financiero se han divido en tres categorías predominantes basadas en las motivaciones de los atacantes, para ayudar a las instituciones financieras a comprender mejor las amenazas que son relevantes para ellos:

- Robo de datos.
- Integridad de datos y sabotaje.
- Robo financiero directo.

A continuación, evidenciamos las técnicas y herramientas que utilizan tres grupos de amenazas enfocados en utilizar las tácticas de acceso inicial y de ejecución, como vector de ataque en teletrabajo.
Presentaremos una breve descripción de cada grupo, su ciclo de vida del ataque, que técnica utiliza para vulnerar un teletrabajador y adicional como podemos mitigar o defendernos de estos ataques.

### 7.1.6. HERRAMIENTAS DE ATAQUE, TÉCNICAS Y PROCEDIMIENTOS

**Spearphishing Attachment**

Los adversarios pueden usar un accesorio de spearphishing, una variante del spearphishing “Phishing”, como una forma de ataque de ingeniería social contra objetivos específicos. Los archivos adjuntos de spearphishing son diferentes de otras formas de spearphishing en que emplean malware adjunto a un correo electrónico. Todas las formas de spearphishing se envían electrónicamente y se dirigen a un individuo, empresa o industria específica. En este escenario, los adversarios adjuntan un archivo al correo electrónico de spearphishing y generalmente dependen de la ejecución del usuario para obtener ejecución y acceso.

**¿Como Funciona?**

**Etapa 1**

Los atacantes determinan su objetivo final con el fin de, robo de identidad, robo de datos confidenciales o propiedad intelectual, chantaje o sabotaje, o puede ser para sentar las bases para un futuro ataque más sofisticado.

**Etapa 2**

Los atacantes investigan sus objetivos, pueden haber realizado un ataque previo para ingresar a la red y monitorear el tráfico de correo electrónico. En ese ataque, es posible que hayan estado buscando identificar qué personas de la organización

tienen acceso a los datos confidenciales que desean robar o quién tiene una relación comercial con alguien cuyas credenciales desean.
Los atacantes también pueden aprender sobre las funciones diarias del rol o del negocio para comprender qué tipos de mensajes recibe el individuo objetivo en un día normal, de modo que el atacante pueda crear un mensaje de phishing que pasará desapercibido.

**Etapa 3**

Los atacantes crean un correo electrónico que parece legítimo a simple vista . Una mirada más cercana revelaría que una O mayúscula en la dirección del remitente es en realidad un cero, o que una L minúscula es una I mayúscula. Esto se llama "falsificación de correo electrónico".
El correo electrónico contendrá un enlace o archivo adjunto malicioso. Si se hace clic en un enlace, llevará al usuario objetivo a una página web, como un portal de recursos humanos, beneficios o financiero, que parece ser auténtica. Cuando el usuario intenta iniciar sesión, sus credenciales se envían al atacante.
Si el correo electrónico incluye un archivo adjunto, puede estar alojado en un servicio legítimo de intercambio de archivos, como Dropbox o Google Drive, para evitar ser bloqueado por los filtros de spam de la empresa objetivo.

**Etapa 4**

Ahora los atacantes cosechan las recompensas de los esfuerzos realizados. Una vez ejecutado el enlace o archivo malicioso, los atacantes pueden lanzar un ataque APT, con el fin de robar datos confidenciales, robo de dinero, datos confidenciales o propiedad intelectual, o simplemente causando caos.

**Drive-by Compromise**

Los adversarios pueden obtener acceso a un sistema a través de un usuario que visita un sitio web durante el curso normal de navegación. Con esta técnica, el navegador web del usuario suele ser objeto de explotación, pero los adversarios también pueden utilizar sitios web comprometidos para un comportamiento que no sea de explotación, como adquirir un token de acceso a la aplicación.

**¿Cómo se ejecutan los ataques de Drive-by Compromise?**

- Los atacantes alojan contenido malicioso en un sitio web vulnerable que visitan los usuarios, mientras los usuarios visitan estos sitios web, se les puede persuadir para que habiliten las secuencias de comandos en el navegador o instalen extensiones de terceros.
- Los scripts maliciosos luego escanean los navegadores de los usuarios visitantes en busca de vulnerabilidades. La mayoría de estas

vulnerabilidades son conocidas. Algunos son previamente desconocidos y se conocen como días cero.

- Una vez que se descubren las vulnerabilidades, el malware presente en el sitio web comprometido explota el navegador del objetivo.
- Una vez que el exploit se haya ejecutado, permitirá al atacante ejecutar el código de forma remota en la máquina de destino.

Los adversarios también pueden usar sitios web comprometidos para enviar a un usuario a una aplicación maliciosa diseñada para robar tokens de acceso a aplicaciones, como tokens de autenticación, para obtener acceso a aplicaciones e información protegidas. Estas aplicaciones maliciosas se han distribuido a través de ventanas emergentes en sitios web legítimos.

**Replication Through Removable Media**

Los adversarios pueden pasar a los sistemas, posiblemente a los de redes desconectadas o con espacios abiertos, copiando malware en medios extraíbles y aprovechando las funciones de ejecución automática cuando el medio se inserta en un sistema y se ejecuta. En el caso del movimiento lateral, esto puede ocurrir mediante la modificación de archivos ejecutables almacenados en medios extraíbles o al copiar malware y cambiarle el nombre para que parezca un archivo legítimo para engañar a los usuarios para que lo ejecuten en un sistema separado. En el caso del acceso inicial, esto puede ocurrir mediante la manipulación manual de los medios, la modificación de los sistemas utilizados para formatear inicialmente los medios o la modificación del firmware del medio en sí.

Las herramientas de uso frecuentemente incluyen:

**H1N1**

Es una variante de malware que se ha distribuido a través de una campaña que utiliza macros VBA para infectar a las víctimas. Aunque inicialmente solo tenía capacidades de cargador, ha evolucionado para incluir la funcionalidad de robo de información.

**Ramsay**

Es un marco de malware de robo de información diseñado para recopilar y exfiltrar documentos confidenciales, potencialmente de sistemas con espacios vacíos.

**Ursnif**

Es un troyano bancario y una variante del malware Gozi que se ha observado que se propaga a través de varios kits de explotación automatizados, archivos adjuntos

de phishing y enlaces maliciosos, se asocia principalmente con el robo de datos, pero las variantes también incluyen componentes (puertas traseras, software espía, inyectores de archivos, etc.) capaces de una amplia variedad de comportamientos.

### 7.1.7. GRUPOS DE AMENAZAS

#### 7.1.7.1. GRUPO APT-C-36

Creado en 05 mayo 2020
Última modificación: 07 de mayo de 2020

Es un presunto grupo de espionaje de América del Sur que ha estado activo desde al menos 2018. El grupo se dirige principalmente a instituciones del gobierno colombiano, así como a importantes corporaciones del sector financiero, la industria petrolera y la fabricación profesional.

**Ciclo de vida del ataque**

APT-C-36 utiliza señuelos de phishing con archivos adjuntos que contienen malware como vector de infección inicial. El objetivo del grupo APT es establecer una puerta trasera en los objetivos previstos para luego obtener un punto de apoyo y luego moverse lateralmente una vez en una red con fines de reconocimiento. Los correos electrónicos y archivos adjuntos de phishing se adaptan a cada industria o entidad a la que se dirige el grupo para aumentar potencialmente la posibilidad de que un destinatario abra el correo electrónico y el archivo adjunto.

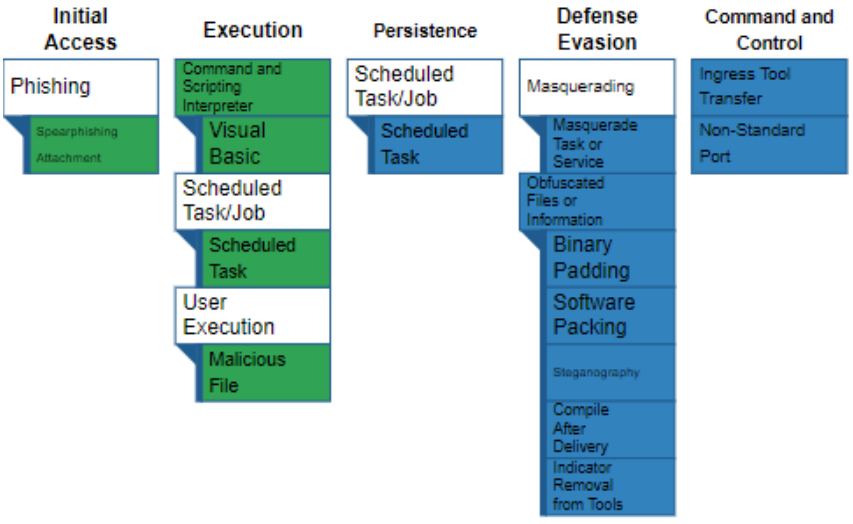


*Figura 6. Ciclo de vida, grupo APT-C-36 – Mitre att&ck.*

**¿Como afectaría este grupo al teletrabajo?**

**Compromiso inicial**

**ID T1566:** Phishing
**Sub-technique T1566.001:** spearphishing Attachment
**Fuentes de datos:** cámara de detonación, puerta de enlace de correo electrónico, supervisión de archivos, servidor de correo, sistema de detección de intrusiones en la red, captura de paquetes.

En este escenario, los adversarios adjuntan un archivo al correo electrónico de spearphishing y, por lo general, dependen de la ejecución del usuario para obtener la ejecución, además los adversarios frecuentemente manipulan las extensiones de archivo y los íconos para hacer que los ejecutables adjuntos parezcan archivos de documentos, o que los archivos que explotan una aplicación parezcan un archivo de otra diferente.

**Ejecución**

**ID T1059:** Command and Scripting Interpreter
**Sub-technique T1059.005:** Visual Basic
**Fuentes de datos:** Supervisión de DLL, supervisión de archivos, DLL cargadas, parámetros de la línea de comandos del proceso, supervisión del proceso

**ID T1053:** Scheduled Task/Job
**Sub-technique T1053.005:** Scheduled Task
**Fuentes de datos:** Monitoreo de archivos, parámetros de la línea de comandos del proceso, monitoreo del proceso, registros de eventos de Windows.

**ID T1204:** User Execution
**Sub-technique T1204.002:** Malicious File
**Fuentes de datos:** Antivirus, parámetros de la línea de comandos del proceso, supervisión del proceso.

Después del compromiso, Su técnica de ejecución para APT-C-36 al hacer clic en el enlace es, redirigir a la víctima a un fichero con la opción de habilitar macros con scripts personalizados basados en Visual Basic. El código de macro ejecuta la carga útil el cual contiene una serie de herramientas personalizadas, las cuales llegan a implantar un RAT y establecer tareas programadas.

**Movimiento lateral**

APT-C-36 facilita el movimiento lateral a través de sus herramientas personalizadas las cuales busca como objetivo ofuscar diferentes aplicaciones para evitar la detección y confundir los análisis mientras realizan algún tipo de monitoreo o envió

de información.

**¿Como mitigarlo?**

**ID T1566:** Phishing
**Sub-technique T1566.001:** spearphishing

- **Antivirus / Antimalware:** El antivirus también puede poner en cuarentena automáticamente los archivos sospechosos.
- **Prevención de intrusiones en la red:** Los sistemas de prevención de intrusiones en la red y los sistemas diseñados para escanear y eliminar archivos adjuntos de correo electrónico maliciosos pueden usarse para bloquear la actividad.
- **Restringir el contenido basado en la web:** Bloquee los archivos adjuntos desconocidos o no utilizados de forma predeterminada que no deben transmitirse por correo electrónico como una mejor práctica para evitar algunos vectores, como .scr, .exe, .pif, .cpl, etc. Algunos dispositivos de escaneo de correo electrónico pueden abrir y analizar comprimidos y cifrados formatos, como zip y rar, que pueden utilizarse para ocultar archivos adjuntos maliciosos.
- **Entrenamiento de usuario:** Los usuarios pueden recibir formación para identificar técnicas de ingeniería social y correos

**ID T1059:** Command and Scripting Interpreter
**Sub-technique T1059.005:** Visual Basic

- **Antivirus / Antimalware:** El antivirus se puede utilizar para poner automáticamente en cuarentena archivos sospechosos.
- **Deshabilitar o quitar función o programa:** Apague o restrinja el acceso a componentes VB innecesarios.
- **Prevención de ejecución:** Utilice el control de la aplicación cuando corresponda.
- **Restringir el contenido basado en la web:** Las extensiones de bloqueo de scripts pueden ayudar a prevenir la ejecución de scripts y archivos HTA que pueden usarse comúnmente durante el proceso de explotación. Para el código malicioso publicado a través de anuncios, los bloqueadores de anuncios pueden ayudar a evitar que ese código se ejecute en primer lugar.

**ID T1053:** Scheduled Task/Job
**Sub-technique T1053.005:** Scheduled Task

- **Auditoría:** Los kits de herramientas como el marco PowerSploit contienen módulos PowerUp que se pueden usar para explorar sistemas en busca de

debilidades de permisos en tareas programadas que podrían usarse para escalar privilegios.

- **Configuración del sistema operativo:** Configure las opciones de las tareas programadas para forzar la ejecución de las tareas en el contexto de la cuenta autenticada en lugar de permitir que se ejecuten como SISTEMA. La clave de registro asociada se encuentra en HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl.
  La configuración se puede configurar a través de GPO: Configuración del equipo> [Políticas]> Configuración de Windows> Configuración de seguridad> Políticas locales> Opciones de seguridad: Controlador de dominio: Permitir que los operadores del servidor programen tareas, establecido en deshabilitado.
- **Gestión de cuentas privilegiadas:** Configure la opción Aumentar la prioridad de programación para permitir solo al grupo de administradores los derechos para programar un proceso de prioridad. Esto se puede configurar a través de GPO: Configuración del equipo> [Políticas]> Configuración de Windows> Configuración de seguridad> Políticas locales> Asignación de derechos de usuario: aumentar la prioridad de programación.
- **Gestión de cuentas de usuario:** Limite los privilegios de las cuentas de usuario y corrija los vectores de escalamiento de privilegios para que solo los administradores autorizados puedan crear tareas programadas en sistemas remotos.

**ID T1204:** User Execution
**Sub-technique T1204.002:** Malicious File

- **Prevención de ejecución:** El control de aplicaciones puede evitar la ejecución de ejecutables disfrazados de otros archivos.
- **Entrenamiento de usuario:** Utilice la formación de los usuarios como una forma de concienciar sobre las técnicas habituales de phishing y spearphishing y cómo generar sospechas de posibles eventos maliciosos.

#### 7.1.7.2. GRUPO APT38

Creado: 29 de enero de 2019
Última modificación: 30 de marzo de 2020

APT38 es un grupo de amenazas con motivaciones financieras que está respaldado por el régimen de Corea del Norte. El grupo se dirige principalmente a bancos e instituciones financieras y se ha dirigido a más de 16 organizaciones en al menos 13 países desde al menos 2014, en Latinoamérica ha afectado a Brasil, Uruguay y chile.

## Ciclo de vida del ataque

Este grupo utiliza diferentes técnicas en un deseo de mantener el acceso a los entornos de las víctimas durante el tiempo que sea necesario para comprender el diseño de la red, los permisos requeridos y las tecnologías del sistema para lograr sus objetivos. APT38 es único en el sentido de que no temen destruir agresivamente las pruebas o las redes de víctimas como parte de sus operaciones.

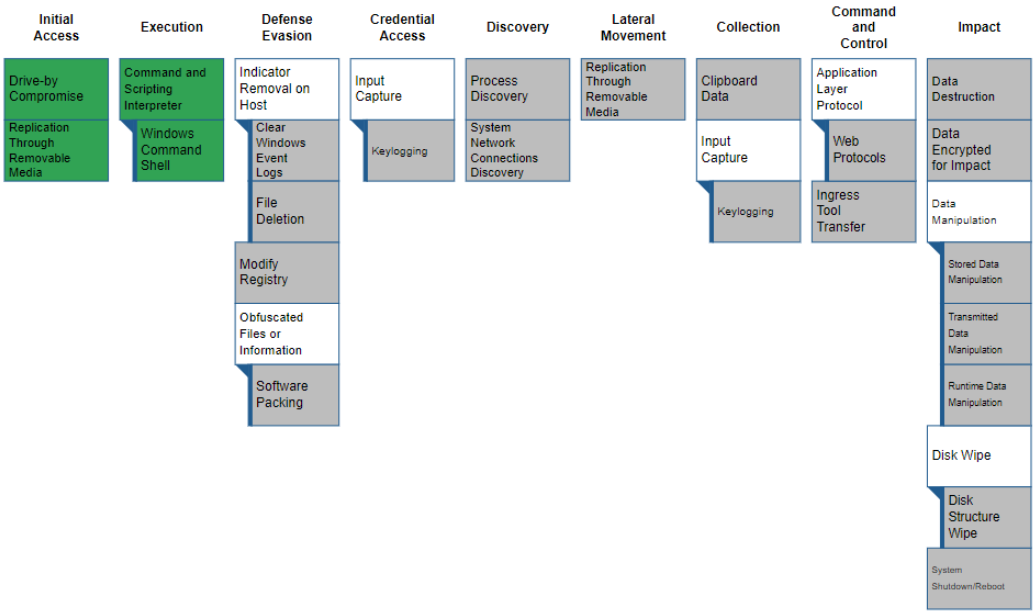


*Figura 7. Ciclo de vida, grupo APT38 - Mitre att&ck.*

## ¿Como afectaría este grupo al teletrabajo?

## Compromiso inicial

**ID T1189, T1456:** Drive-by Compromise
**Fuentes de datos:** Registros de dispositivos de red, sistema de detección de intrusiones en la red, captura de paquetes, uso de procesos de la red, inspección SSL / TLS, proxy web.

En este escenario, el grupo APT38 aplica la tendencia de Watering hole “perfilado de su víctima”, tras observar y realizar un seguimiento acerca de sus hábitos, identifica las páginas que visita habitualmente. Una vez recabada la información necesaria, el hacker aprovechará cualquier posible vulnerabilidad en dicha página e inyectará código malicioso (en los anuncios, en los banners, etc.).
Los usuarios que visita un sitio web durante el curso normal de navegación, suelen ser objeto de explotación, así como el correo electrónico de spearphishing y, por lo

general, dependen de la ejecución del usuario para obtener la ejecución.
**Ejecución**

**ID T1059:** Command and Scripting Interpreter
**Sub-technique T1059.003:** Windows Command Shell
**Fuentes de datos:** Parámetros de la línea de comandos del proceso, supervisión del proceso, registros de eventos de Windows.

Después del compromiso, el usuario visita un sitio web que normalmente ingresa, y es ahí donde suelen ser objeto de explotación, ya que al dar clic al anuncio o banner el grupo APT38 planta una carga útil ejecutando un tunelizador de línea de comandos como Nachocheese, con el fin de darles acceso a Shell de la maquina víctima.

**Movimiento lateral**

Una vez el grupo APT38 tiene acceso al Shell de la máquina, despliega diferentes herramientas para empezar escalar privilegios como la toma de acceso a teclas, recopilación de datos de la papelera de reciclaje, así como el monitoreo en los sistemas usados por trasferencias SWIFT para comprender mejor cómo se configuran y se usan. Implementa puertas traseras activas y pasivas en estos sistemas para acceder a sistemas internos segmentados en una organización víctima y evitar la detección. Una vez realizada la transferencia de datos, el grupo elimina los registros del sistema de forma segura, así como ejecutar un malware para el borrado de discos o de encriptación, con el fin cubrir pistas e interrumpir el análisis forense.

**¿Como mitigarlo?**

**ID T1566:** Drive-by Compromise
**Fuentes de datos:** Registros de dispositivos de red, sistema de detección de intrusiones en la red, captura de paquetes, uso de procesos de la red, inspección SSL / TLS, proxy web.

- **Aislamiento de aplicaciones y sandboxing:** Los entornos sandbox del navegador se pueden utilizar para mitigar parte del impacto de la explotación, pero es posible que aún existan escapes de sandbox.
  Otros tipos de virtualización y microsegmentación de aplicaciones también pueden mitigar el impacto de la explotación del lado del cliente. Es posible que aún existan riesgos de vulnerabilidades y debilidades adicionales en la implementación para este tipo de sistemas.
- **Protección contra exploits:** Las aplicaciones de seguridad que buscan el comportamiento utilizado durante la explotación, como Windows Defender Exploit Guard (WDEG) y Enhanced Mitigation Experience Toolkit (EMET), se

pueden utilizar para mitigar algunos comportamientos de explotación. [5] La comprobación de la integridad del flujo de control es otra forma de identificar y detener potencialmente una explotación de software. [6] Muchas de estas protecciones dependen de la arquitectura y el binario de la aplicación de destino para la compatibilidad.

- **Restringir el contenido basado en la web:** Para el código malicioso publicado a través de anuncios, los bloqueadores de anuncios pueden ayudar a evitar que ese código se ejecute en primer lugar.
  Las extensiones de bloqueo de scripts pueden ayudar a prevenir la ejecución de JavaScript que se puede usar comúnmente durante el proceso de explotación.
- **Actualiza el software:** Asegúrese de que todos los navegadores y complementos actualizados puedan ayudar a prevenir la fase de explotación de esta técnica. Utilice navegadores modernos con funciones de seguridad activadas.

**ID T1059:** Command and Scripting Interpreter
**Sub-technique T1059.003:** Windows Command Shell

- **Prevención de ejecución:** Bloquear la ejecución de código en un sistema a través del control de aplicaciones y / o bloqueo de scripts.

#### 7.1.7.3. GRUPO APT19

Creado: 17 octubre 2018
Última modificación: 20 de junio de 2020

Es un grupo de amenazas con sede en China que se ha dirigido a una variedad de industrias, que incluyen defensa, finanzas, energía, farmacéutica, telecomunicaciones, alta tecnología, educación, fabricación y servicios legales.

**Ciclo de vida del ataque**

APT19 agrega el compromiso en la navegación en sitios web a través de anuncios maliciosos los cuales se publican a través de proveedores de anuncios legítimos con el fin de que sus víctimas den clic en los enlaces. APT19 ha utilizado tres técnicas diferentes para intentar comprometer los objetivos. A principios de mayo de 2017, los señuelos de phishing aprovecharon los archivos adjuntos RTF que explotaban la vulnerabilidad de Microsoft Windows descrita en CVE 2017-0199. Hacia fines de 2019, APT19 pasó a utilizar documentos de Microsoft Excel (XLSM) habilitados para macros. Para este año 2020, algunos analistas rastrean a APT19 y Deep Panda como el mismo grupo, pero no está claro a partir de la información de código abierto si los grupos son iguales.

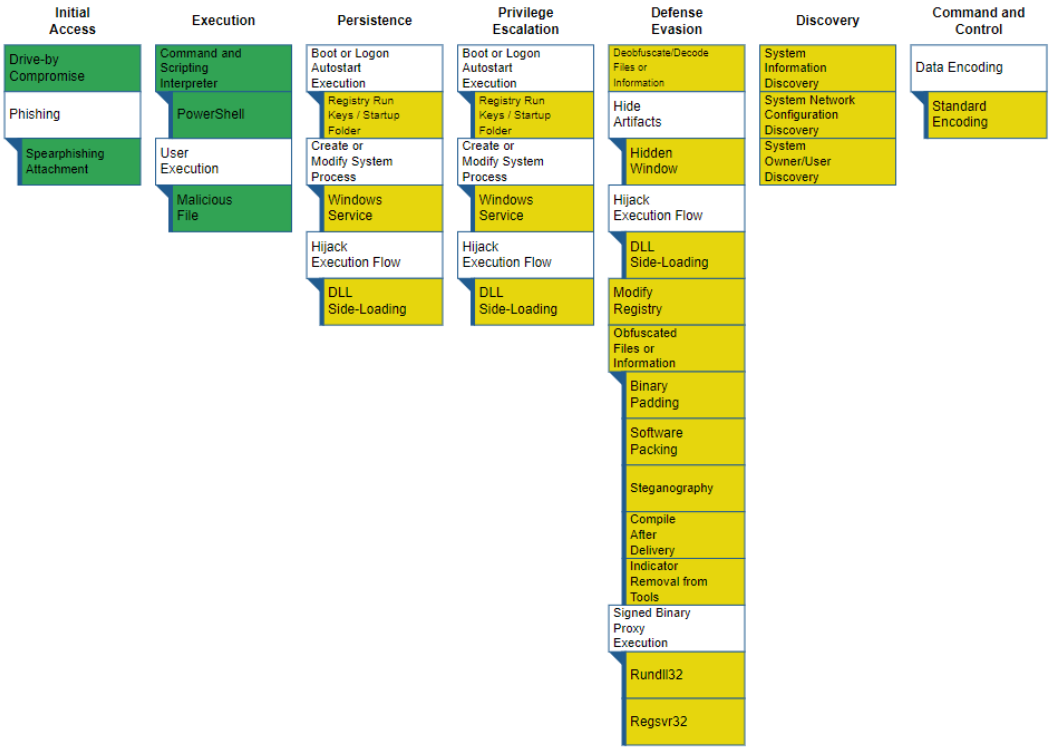


*Figura 8. Ciclo de vida, grupo APT19 - Mitre att&ck.*

**¿Como afectaría este grupo al teletrabajo?**

**Compromiso inicial**

**ID T1566:** Drive-by Compromise
**Fuentes de datos:** Registros de dispositivos de red, sistema de detección de intrusiones en la red, captura de paquetes, uso de procesos de la red, inspección SSL / TLS, proxy web.

**ID T1566:** Phishing
**Sub-technique T1566.001:** spearphishing
**Fuentes de datos:** cámara de detonación, puerta de enlace de correo electrónico, supervisión de archivos, servidor de correo, sistema de detección de intrusiones en la red, captura de paquetes.

En este escenario, los usuarios que visita un sitio web durante el curso normal de navegación, suelen ser objeto de explotación, así como el correo electrónico de spearphishing y, por lo general, dependen de la ejecución del usuario para obtener la ejecución.

**Ejecución**

**ID T1059:** Command and Scripting Interpreter
**Sub-technique T1059.001:** PowerShell
**Fuentes de datos:** Supervisión de DLL, supervisión de archivos, DLL cargadas, registros de PowerShell, parámetros de la línea de comandos de proceso, supervisión de procesos, registros de eventos de Windows.

**ID T1204:** User Execution
**Sub-technique T1204.002:** Malicious File
**Fuentes de datos:** Antivirus, parámetros de la línea de comandos del proceso, supervisión del proceso.

Después del compromiso, Su técnica de ejecución para APT19 es descargar e iniciar un código de comandos de PowerShell oculto en un archivo de ejecución de arranque del equipo y ejecutar cargas útiles.

**Movimiento lateral**

APT19 utiliza las variantes del malware para recopilar información de los usuarios, así como información y características del equipo y enviarlas por un puerto de comunicaciones.

**¿Como mitigarlo?**

**ID T1566:** Drive-by Compromise
**Fuentes de datos:** Registros de dispositivos de red, sistema de detección de intrusiones en la red, captura de paquetes, uso de procesos de la red, inspección SSL / TLS, proxy web.

- **Aislamiento de aplicaciones y sandboxing:** Los entornos sandbox del navegador se pueden utilizar para mitigar parte del impacto de la explotación, pero es posible que aún existan escapes de sandbox.
  Otros tipos de virtualización y microsegmentación de aplicaciones también pueden mitigar el impacto de la explotación del lado del cliente. Es posible que aún existan riesgos de vulnerabilidades y debilidades adicionales en la implementación para este tipo de sistemas.
- **Protección contra exploits:** Las aplicaciones de seguridad que buscan el comportamiento utilizado durante la explotación, como Windows Defender Exploit Guard (WDEG) y Enhanced Mitigation Experience Toolkit (EMET), se pueden utilizar para mitigar algunos comportamientos de explotación. [5] La comprobación de la integridad del flujo de control es otra forma de identificar y detener potencialmente una explotación de software. [6] Muchas de estas

protecciones dependen de la arquitectura y el binario de la aplicación de destino para la compatibilidad.

- **Restringir el contenido basado en la web:** Para el código malicioso publicado a través de anuncios, los bloqueadores de anuncios pueden ayudar a evitar que ese código se ejecute en primer lugar.
  Las extensiones de bloqueo de scripts pueden ayudar a prevenir la ejecución de JavaScript que se puede usar comúnmente durante el proceso de explotación.
- **Actualiza el software:** Asegúrese de que todos los navegadores y complementos actualizados puedan ayudar a prevenir la fase de explotación de esta técnica. Utilice navegadores modernos con funciones de seguridad activadas.

**ID T1566:** Phishing
**Sub-technique T1566.001:** spearphishing

- **Antivirus / Antimalware:** El antivirus también puede poner en cuarentena automáticamente los archivos sospechosos.
- **Prevención de intrusiones en la red:** Los sistemas de prevención de intrusiones en la red y los sistemas diseñados para escanear y eliminar archivos adjuntos de correo electrónico maliciosos pueden usarse para bloquear la actividad.
- **Restringir el contenido basado en la web:** Bloquee los archivos adjuntos desconocidos o no utilizados de forma predeterminada que no deben transmitirse por correo electrónico como una mejor práctica para evitar algunos vectores, como .scr, .exe, .pif, .cpl, etc. Algunos dispositivos de escaneo de correo electrónico pueden abrir y analizar comprimidos y cifrados formatos, como zip y rar, que pueden utilizarse para ocultar archivos adjuntos maliciosos.
- **Entrenamiento de usuario:** Los usuarios pueden recibir formación para identificar técnicas de ingeniería social y correos

**ID T1059:** Command and Scripting Interpreter
**Sub-technique T1059.001:** PowerShell

- **Antivirus / Antimalware:** El antivirus se puede utilizar para poner automáticamente en cuarentena archivos sospechosos.
- **Firma de código:** Configure la política de ejecución de PowerShell para ejecutar solo scripts firmados.
- **Deshabilitar o quitar función o programa:** Puede ser posible eliminar PowerShell de los sistemas cuando no sea necesario, pero se debe realizar una revisión para evaluar el impacto en un entorno, ya que podría estar en uso para muchos propósitos legítimos y funciones administrativas.

Deshabilite / restrinja el servicio WinRM para ayudar a prevenir los usos de PowerShell para la ejecución remota.

- **Gestión de cuentas privilegiadas:** Cuando sea necesario PowerShell, restrinja la política de ejecución de PowerShell a los administradores. Tenga en cuenta que existen métodos para omitir la política de ejecución de PowerShell, según la configuración del entorno.

**ID T1204:** User Execution
**Sub-technique T1204.002:** Malicious File

- **Prevención de ejecución:** El control de aplicaciones puede evitar la ejecución de ejecutables disfrazados de otros archivos.
- **Entrenamiento de usuario:** Utilice la formación de los usuarios como una forma de concienciar sobre las técnicas habituales de phishing y spearphishing y cómo generar sospechas de posibles eventos maliciosos.

## 7.1.8. MAPA DE THREAT INTELLIGENCE

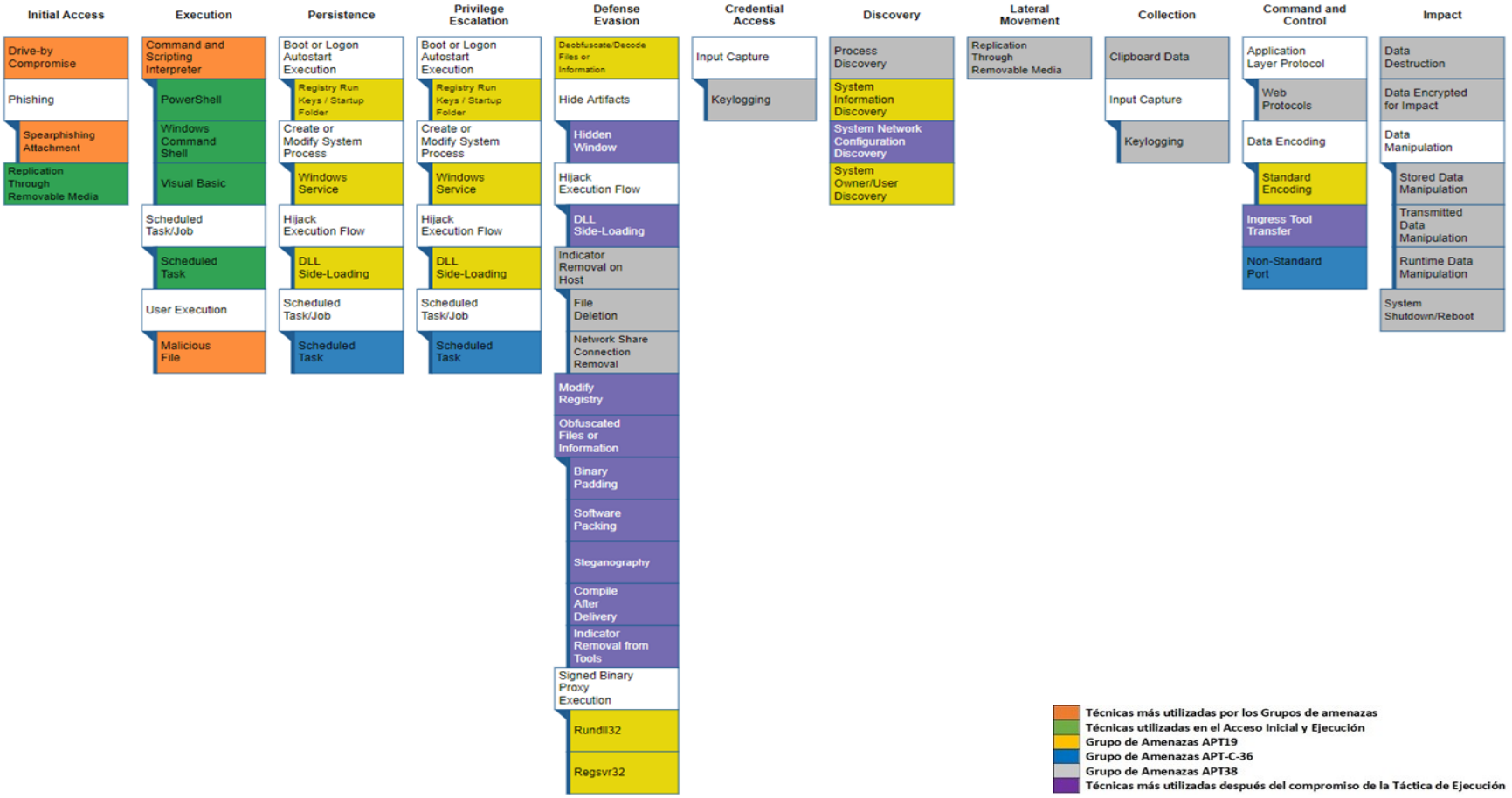


*Figura 9. Mapa conceptual de threat intelligence - Mitre att&ck.*

### 7.1.9. RESULTADOS OBTENIDOS DE LA INTELIGENCIA ANTERIOR

De acuerdo al informe presentado se evidencia los siguientes puntos más importantes a tener en cuenta.

Muchos de los impactos y ataques son de naturaleza similar, pero existen algunas diferencias notables según la industria específica.
Tanto los actores delictivos como los grupos de amenazas se han dirigido al sector financiero para:

- Robar datos personales.
- Seguimiento de las actividades financieras de clientes específicos.
- Robar dinero.

Además de esto, ha habido un cambio general en la popularidad de ciertas técnicas ofensivas, algunas de las cuales simbolizan un aumento en la sofisticación de los ataques.
Estos cambios incluyen el aumento de:

- Phishing
- Watering hole “perfilado de su víctima”
- Ataques de Ransomware dirigidos

A medida que el panorama de amenazas continúa evolucionando, surgen nuevas herramientas y enfoques con regularidad. Pero una cosa permanece constante es el factor humano.

Más que nunca, los ciberdelincuentes dependen de las personas para descargar e instalar malware o enviar fondos e información en su nombre. Y a medida que la vida útil de los exploits automatizados se acorta, el potencial retorno de la inversión de la ingeniería social superará aún más al de los ataques automatizados.

### 7.1.10. CONCLUSIONES DE LA THREAT INTELLIGENCE

Con base al conocimiento de Mitre att&ck y a las observaciones relacionadas en la Threat Intelligence presentadas en este análisis, las organizaciones financieras deben reflexionar y concentrar sus esfuerzos en las siguientes áreas:

- Implementar infraestructura, aplicaciones y operaciones que sean seguras por diseño, lo que significa que incluir la seguridad es una decisión clave y consciente en el enfoque para diseñar soluciones empresariales de principio a fin.
- Evaluar su estado actual de ciberresilencia y definir el estado futuro deseado.

- Utilice la formación de los usuarios como una forma de concienciar sobre las técnicas más habituales de los ciber atacantes y cómo generar sospechas de posibles eventos maliciosos.
- Aproveche la ciberseguridad inteligente en apoyo de la agilidad empresarial y mantener un nivel de riesgo aceptable para la organización.

Aproveche las capacidades de inteligencia de amenazas proactivas para identificar y tomar decisiones rápidamente para administrar el riesgo.

## 7.2. GUIA DE HARDENING

Para la elaboración de la Guía de Hardening y construcción de su contenido, esta se basó en los resultados obtenidos del documento de análisis de Threat Intelligence, en donde se tomaron las técnicas utilizadas por los ciberdelincuentes y se les proporciono las diferentes consideraciones técnicas de seguridad sobre cómo reducir y mitigar los ataques, siendo estos desde la parte del usuario de una entidad financiera que está trabajando desde la casa, como recomendaciones más avanzadas enfocadas al área de tecnología, estas consideraciones de seguridad se basaron en la información publicada por los organismos especializados en seguridad como son la NIST, ISO 27001 y entidades de ciberseguridad europeas. así mismo, se compartió en la publicación de la guía algunas recomendaciones de seguridad propuestas por nosotros como resultado de toda la información aprendida en el transcurso de la especialización.


*Figura 10. Guía de Hardening.*


*Figura 11. Recomendaciones de seguridad para usuario en teletrabajo.*


*Figura 12. Recomendaciones de seguridad para el área de tecnología.*

Para la consulta de la guía remitirse al **Anexo A-Guía de Hardening.**

## 7.3. PRUEBA DE CONCEPTO


*Figura 13. Prueba de Concepto - Guías de Hardening.*

Para la realización de la prueba de concepto, se utilizó el software gratuito Virtual box para simular primero un equipo de un usuario que trabaja desde casa de una entidad financiera, y como segundo equipo se simulara a un adversario con intenciones de atacar y comprometer el equipo del trabajador de la entidad financiera.

- Maquina Windows 7: Equipo del trabajador de una entidad financiera.
- Maquina Kali Linux: Equipo del atacante.

Para este ejercicio, la prueba de concepto esta divida en dos partes, la primera evidenciando el compromiso del equipo del trabajador de la entidad financiera por medio del uso de las técnicas de Spearphishing y Drive-by Compromise, Para la segunda parte del video, se evidenciara el resultado de la aplicación de las guías de hardening en donde se analizará cada punto de las amenazas utilizadas por parte del atacante, y como con el uso de la aplicación de las recomendaciones de la guía se mitigo el ataque del adversario.

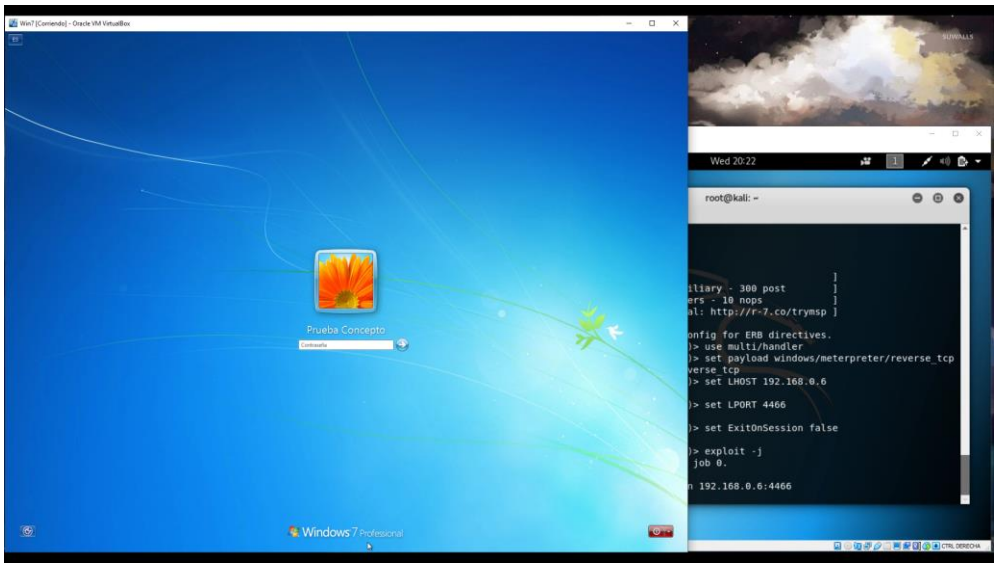


*Figura 14. Máquinas Virtuales.*

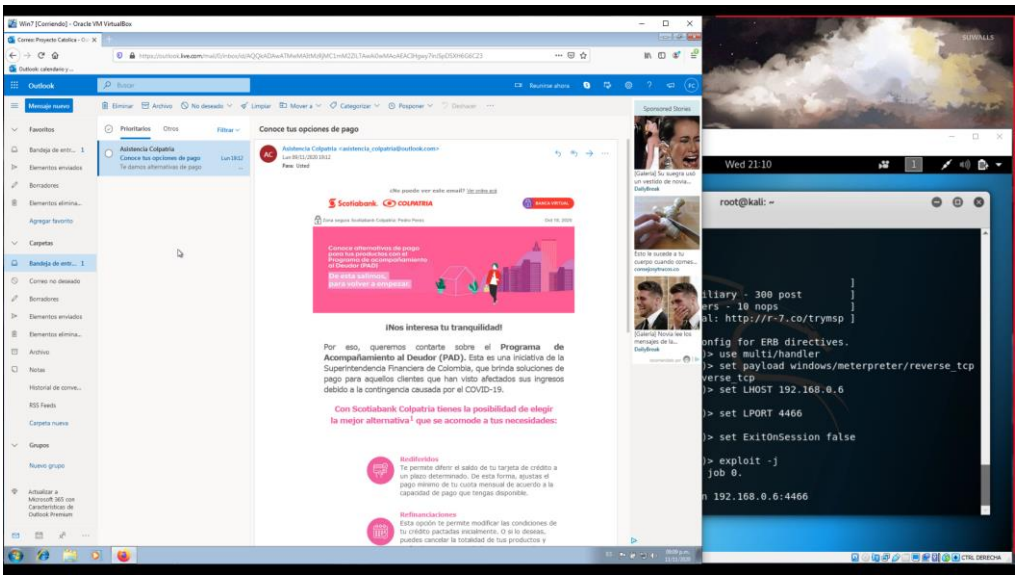


*Figura 15. Correo Phishing.*

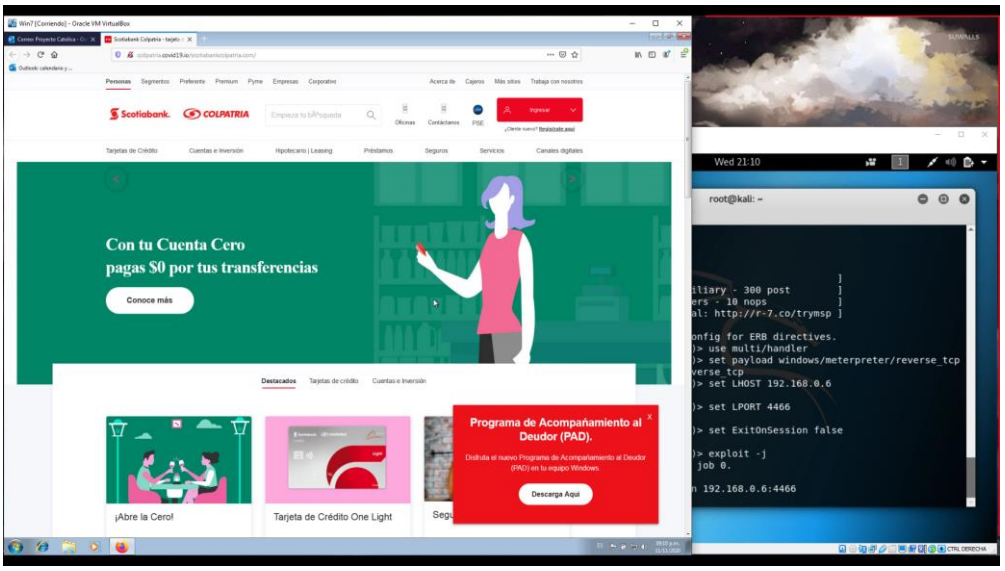


*Figura 16. Página Web phishing.*

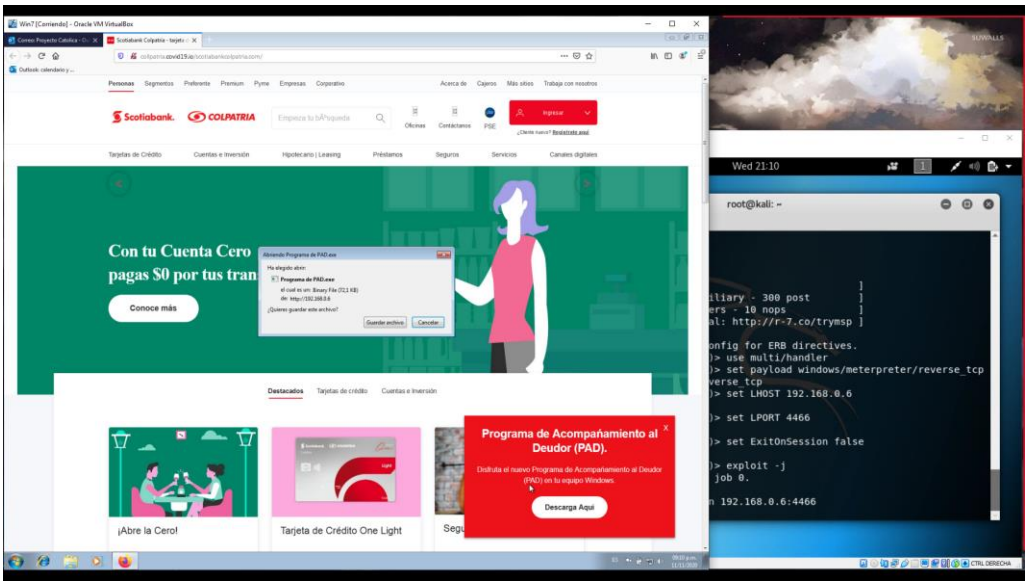


*Figura 17. Descarga del Malware.*

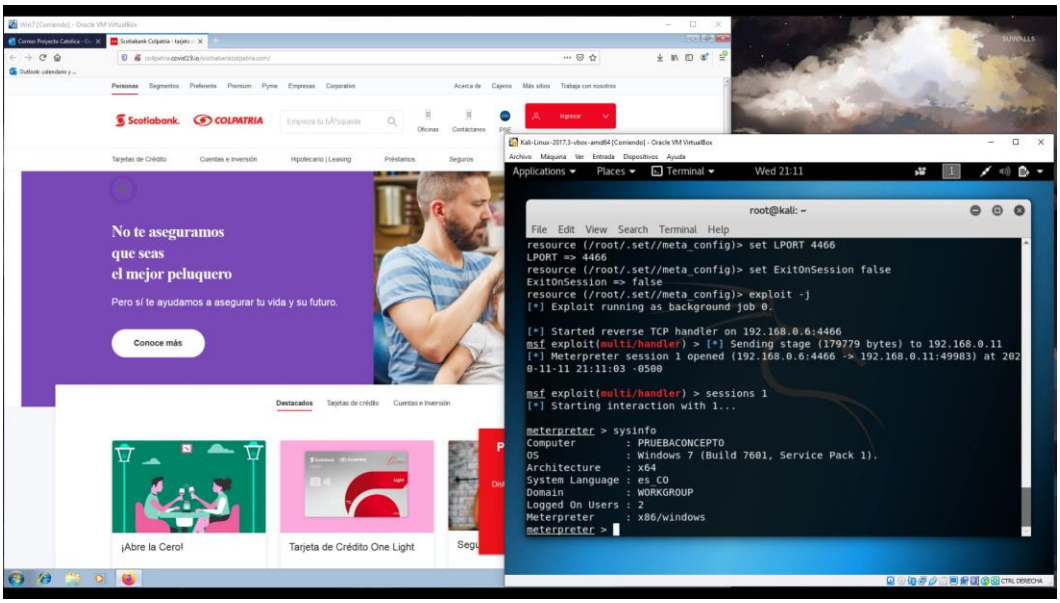


*Figura 18. Compromiso del equipo del trabajador.*

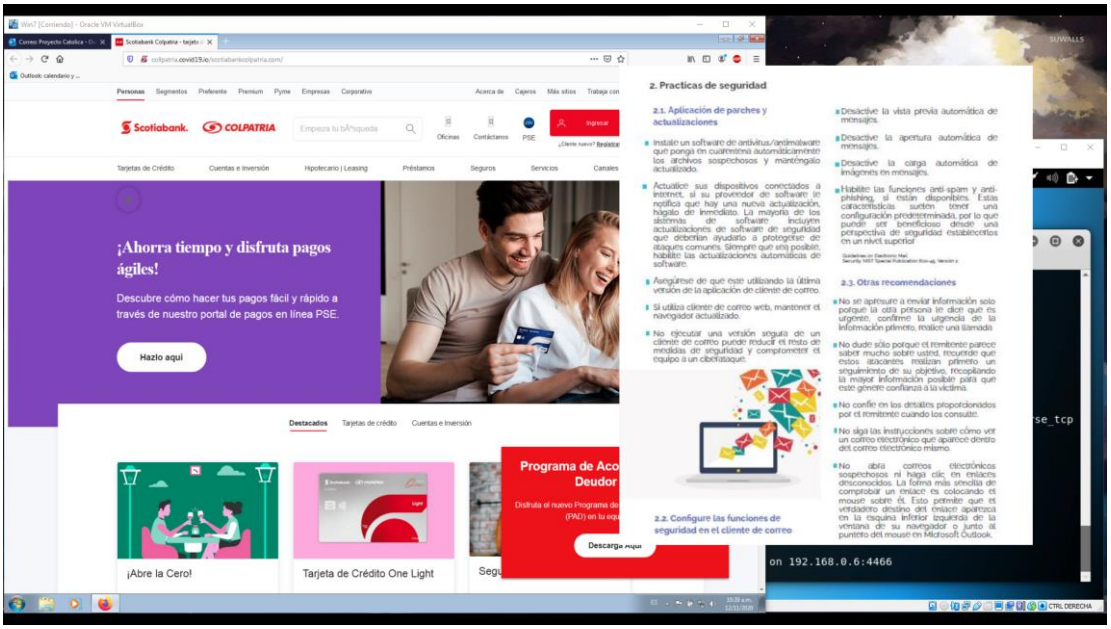


*Figura 1919. Recomendaciones de seguridad.*

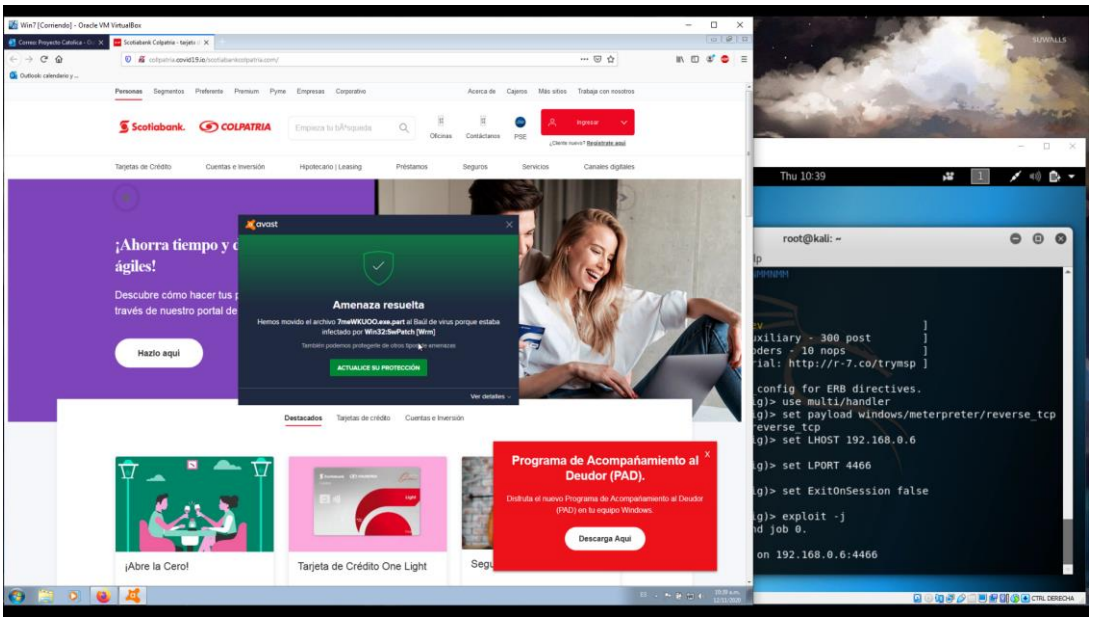


*Figura 200. Bloqueo del malware por parte del Antivirus.*

Para la consulta de la prueba de concepto remitirse al **Anexo B-Prueba de Concepto.**

Cabe resaltar que en la siguiente prueba de concepto expuesta solo evidenciamos la aplicabilidad de las recomendaciones técnicas para el usuario que trabaja desde casa, ya que basados en el análisis visto de Threat Intelligence, los diferentes grupos de amenazas buscan como vector principal atacar la táctica de acceso inicial de un teletrabajador y es ahí donde el primer nivel de seguridad debe estar presente en todos los dispositivos de los usuarios de las entidades financieras.

Por otra parte, el documento de análisis de Threat Intelligence nos presenta las tácticas de ejecución después del compromiso del acceso inicial de un teletrabajador y es ahí donde la guía de hardening nos expone el segundo nivel de seguridad que las organizaciones deben aplicar de la mano del oficial de seguridad, ya que estos son los responsables de los aspectos técnicos de la preparación, organización y aseguramiento de los dispositivos de los clientes.

# 8. CONCLUSIONES

Los funcionarios de entidades financieras que laboran desde su casa, actualmente no cuentan con herramientas o conocimientos que les ayude a mitigar los riesgos a los que están expuestos diariamente, ya que el objetivo que hoy vemos en tiempos de pandemia por los adversarios, es en vulnerar o atacar sus equipos BYOD, por lo cual, este proyecto tenía como fin investigar, analizar y construir una herramienta útil que ayudara a reducir y mitigar todo tipo de ciberataques para los funcionarios, de acuerdo a lo anterior, fue necesario hacer análisis de Threat Intelligence con el apoyo de Mitre Att&ck para conocer que grupos de adversarios están interesados en atacar a las entidades financieras y como desde sus técnicas y tácticas podrían vulnerar un funcionario que labora desde su casa.

El documento de análisis de Threat Intelligence era ese punto de partida para empezar a construir la guía de hardening, ya que era el objetivo principal de este proyecto, gracias a este documento, fue posible encontrar cuales eran los vectores de entrada para un atacante hacia un usuario de teletrabajo, que métodos utilizaban los adversarios, que impactos generaría al vulnerar un teletrabajador y como mitigar o prevenir estos ataques.

Al finalizar el documento de Threat Intelligence y la construcción de la guía, se hizo una demostración en una prueba de concepto que se divido en dos fases, una simulando a un funcionario que trabaja desde casa y que no cuenta con los mínimos niveles de seguridad, y la segunda prueba en donde el funcionario aplica las recomendaciones dadas en la guía de hardening. A través de esta prueba de concepto se pudo evidenciar la efectividad de la guía reduciendo el riesgo y evitando el cumplimiento del objetivo de un atacante.

## 9. BIBLIOGRAFIA


[1] INCIBE, Instituto nacional de Ciberseguridad; Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario, 2017. En https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf

[2] GUIDE TO ENTERPRISE TELEWORK; Remote Access, and Bring Your Own Device (BYOD) Security, NIST Special Publication 800-46 Revisión 2, 2016. En https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

[3] REVISTA SEMANA; El tiempo que los bogotanos pierden al año en trancones, 2018. En https://www.semana.com/Item/ArticleAsync/556386

[4] BODDY, Matt. JONES, Ben and STOCKLEY Mark, Sophos - RDP Exposed - The Threat That's Already at Your Door, 2019".
En https://nakedsecurity.sophos.com/2019/07/17/rdp-exposed-the-wolves-already-at-your-door/

[5] MILOŠ, Čermák, ROBERT, Lipovsky; welivesecurity by eset, 26 Feb 2020.En https://www.welivesecurity.com/2020/02/26/krook-serious-vulnerability-affected-encryption-billion-wifi-devices/

[6] REYES, J. F. Firma invitada; El virus" Wannacry". Quadernos de criminología: revista de criminología y ciencias forenses, 2017, (38), 32-37.

[7] Ministerio de tecnologías de la información y comunicación, Paraguay. En https://cert.gov.py/index.php/noticias/distribucion-de-ransomware-mediante-ataques-de-fuerza-bruta-rdp

[8] LESMES SOTO, Leonardo; Gerente de Auditoría y Aseguramiento, BDO Colombia, Contadores Públicos y Consultores, 15 de junio de 2018.
En http://www.empresariotic.com/software-y-la-nube/107-seguridad/1185-teletrabajo-una-puerta-abierta-a-la-vulnerabilidad-cibernetica-de-las-empresas

[9] WASHINGTONPOST, marzo 13 de 2020.
En: https://www.washingtonpost.com/nation/2020/03/13/federal-employees-may-soon-be-ordered-work-home-that-could-pose-serious-cybersecurity-risks/

[10] EL TIEMPO, ¿Cómo los trabajos se están transformando hacia un entorno digital?, 2019. En https://www.eltiempo.com/economia/empresas/teletrabajo-una-opcion-cada-vez-mas-comun-en-colombia-393214

[11] ARANGO, Lizeth Andrea Villada; Condiciones facilitadoras y obstaculizadoras para la adaptación al teletrabajo en docentes de una IES de Medellín, 2018, 76 pág.

[12] OZ ALASHE, Alashe; Remote working poses significant security risk to uk's sme businesses, new research reveals, CybSafe. En https://www.cybsafe.com/press-releases/remote-working-poses-significant-security-risk-to-uks-sme-businesses-new-research-reveals/

[13] TELETRABAJO, El teletrabajo sigue creciendo en el mundo, 2019. En https://www.teletrabajo.gov.co/622/w3-article-103166.html

[14] RAMIREZ, Iván; ¿Qué es una conexión vpn, para qué sirve y qué ventajas tiene?, 2019. En https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene

[15] YUBAL FM; Firewall: qué es un cortafuegos, para qué sirve y cómo funciona, 2019 en https://www.xataka.com/basics/firewall-que-cortafuegos-sirve-como-funciona

[16] VANGUARDIA; ¿Qué es un antivirus y para qué sirve?, 2018. En https://vanguardia.com.mx/articulo/que-es-un-antivirus-y-para-que-sirve

[17] DANA, Elfenbaum; Cual es la diferencia entre los protocolos TCP y UDP, 2019 en. En https://es.ccm.net/faq/1559-cual-es-la-diferencia-entre-los-protocolos-tcp-y-udp

[18] SEGURIDAD, Leonardo ; en ¿QUIÉN ES JACK NILLES?, 2016 en https://teletrabajoblog.wordpress.com/2016/04/28/quien-es-jack-nilles/

[19] MINISTERIO DE TELECOMUNICACIONES, Ley 1221 de 2008 por la cual se establecen normas para promover y regular el teletrabajo y se dictan otras disposiciones, 2008. En https://www.mintic.gov.co/portal/604/articles-3703_documento.pdf

[20] MINISTERIO DE TRABAJO, Resolución 2886; Por la cual se definen las entidades que harán parte de la red nacional de fomento al teletrabajo y se dictan otras disposiciones, 2012.

[21] ALCALDÍA DE BOGOTÁ; Proyecto de acuerdo 128; Por medio del cual se establece en el distrito capital, la estrategia para la implementación del teletrabajo en Bogotá, 2013.
En https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53426

[22] LIBRO BLANCO; El ABC del teletrabajo en Colombia - versión 3.0, Pág. 97. En https://www.teletrabajo.gov.co/622/articles-8228_archivo_pdf_libro_blanco.pdf

[23] MOJICA, JJ Chaverra; VÉLEZ, H. de J. Restrepo; GARCÍA, JF Pérez. El teletrabajo y la seguridad de la información empresarial. REVISTA CINTEX, 2015, vol. 20.

[24] CSIRT-CV. Centro de seguridad tic de la Comunitat valenciana; Guía de seguridad en el teletrabajo, 2015.

[25] ANDRÉS, Bustos Guáqueta Carlos; Seguridad informática para el teletrabajo en empresas privadas en Colombia. 2015. Tesis de Licenciatura. Universidad Piloto de Colombia.

[26] MÉNDEZ, M; El teletrabajo en España: aspectos teórico-prácticos de interés. Madrid: Wolters Kluwer. En https://ebookcentral.proquest.com/lib/biblioucatolicasp/reader.action?docID=5350366&query=factores+protectores+teletrabajo

[27] LEAL CUBAQUE, Edicson Daniel, La seguridad de la información en dispositivos móviles personales de uso profesional." 2019. En http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4920/00005097.pdf?sequence=1&isAllowed=y

[28] LA REPÚBLICA, Número de teletrabajadores en Colombia creció 287% los últimos cuatro años, 2018. En https://www.larepublica.co/economia/numero-de-teletrabajadores-en-colombia-crecio-287-los-ultimos-cuatro-anos-2753681

[29] GUIDE TO TELEWORK AND BRING YOUR OWN DEVICE (BYOD) SECURITY, NIST Special Publication 800-114 Revisión 1, 2016.
En https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf

[30] HACKNOID, estadísticas de ciberataques en tiempos de covid-19, 2019. En https://hacknoid.com/sin-categorizar/estadisticas-de-ciberataques-en-tiempos-de-covid-19/

[31] TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información, ISO, NTC. IEC 27001, 2013. En https://repository.ucatolica.edu.co/bitstream/10983/14680/1/Proyecto%20Identificar%20el%20GAP%20de%20Seguridad%20de%20la%20Informaci%C3%B3n%20en%20el%20Proceso%20TI%20de%20OMB.pdf

[32] MINISTERIO TIC COLOMBIA, Historia del teletrabajo, 2016. En https://www.youtube.com/watch?v=keKFJUiEQwU

[33] REVISTA SCIENCE, Projecting the transmission dynamics of SARS-CoV-2 through the postpandemic period, 2020. En https://science.sciencemag.org/content/368/6493/860

[34] JESUS FERNANDEZ, El uso de las redes sociales abarca casi la mitad de la población mundial, 2020. En https://wearesocial.com/es/blog/2020/01/digital-2020-el-uso-de-las-redes-sociales-abarca-casi-la-mitad-de-la-poblacion-mundial

[35] MABEL MATEUS, ¡Teletrabaje con seguridad! En https://mintic.gov.co/portal/vivedigital/612/w3-article-5106.html

[36] MIGUEL ANGEL MENDOZA, ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia, 2015. En https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

[37] ATT&CK Training; En https://attack.mitre.org/

[38] MITRE CORPORATION; En https://attack.mitre.org/resources/training/cti/

[39] MITRE CORPORATION; En https://attack.mitre.org/resources/training/cti/

[40] MITRE CORPORATION; Phishing: Spearphishing Attachment. En https://attack.mitre.org/techniques/T1566/001/

[41] MITRE CORPORATION; Drive-by Compromise. En https://attack.mitre.org/techniques/T1189/

[42] MITRE CORPORATION; Replication Through Removable Media. En https://attack.mitre.org/techniques/T1091/

[43] MITRE CORPORATION; Grupo APT-C-36. En https://attack.mitre.org/groups/G0099/

[44] MITRE CORPORATION; APT-C-36. En https://web.archive.org/web/20190625182633if_/https://ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/)

[45] MITRE CORPORATION; Grupo APT38. En https://attack.mitre.org/groups/G0082/

[46] MITRE CORPORATION; Grupo APT19. En https://attack.mitre.org/groups/G0073/

[46] CSIRT-CV; Centre Seguretat TIC de la Comunitat Valenciana, Guía de seguridad en teletrabajo.
En https://concienciat.gva.es/wp-content/uploads/2018/03/infor_guia_de_seguridad_en_el_teletrabajo.pdf

[47] GUIDELINES ON ELECTRONIC MAIL SECURITY; NIST Special Publication 800-45, Versión 2. En
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-45ver2.pdf

[48] SPEARPHISHING A LAW ENFORCEMENT AND CROSS-INDUSTRY PERSPECTIVE, European Cybercrime centre, Europol EC3 2019 En
https://www.europol.europa.eu/sites/default/files/documents/report_on_phishing_-_a_law_enforcement_perspective.pdf

[49] RISK MANAGEMENT FOR REPLICATION DEVICES, NISTIR 8023. En
https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8023.pdf

[50] CYBERSECURITY & INFRAESTRUCTURE SECURITY AGENCY; Security Tip (ST08-001). En https://us-cert.cisa.gov/ncas/tips/ST08-001

[51] PICUSSECURITY; MITRE ATT&CK T1059 Command Line Interface. En
https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1059-command-line-interface

[52] PICUSSECURITY; MITRE ATT&CK T1064 Scripting. En
https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1064-scripting

[53] MICROSOFT; Reduce attack surfaces with attack surface reduction rules. En
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction#block-untrusted-and-unsigned-processes-that-run-from-usb

[54] MICROSOFT; Increase scheduling priority. En
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn221960(v=ws.11)?redirectedfrom=MSDN

[55] MICROSOFT; Domain controller: Allow server operators to schedule tasks. En
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj852168(v=ws.11)?redirectedfrom=MSDN