ANÁLISIS DEL IMPACTO EN LA IMPLEMENTACIÓN DEL TRABAJO REMOTO, RESPECTO DEL AUMENTO DE ATAQUES DE INGENIERÍA SOCIAL EN LAS EMPRESAS DEL SECTOR RETAIL.

DIEGO ARMANDO BELTRAN SAAVEDRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2023

ANÁLISIS DEL IMPACTO EN LA IMPLEMENTACIÓN DEL TRABAJO REMOTO, RESPECTO DEL AUMENTO DE ATAQUES DE INGENIERÍA SOCIAL EN LAS EMPRESAS DEL SECTOR RETAIL.

DIEGO ARMANDO BELTRAN SAAVEDRA

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

EDGARDO MAURICIO LÓPEZ ROJAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2023

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

CIBERDELINCUENTE: Es el vocablo empleado para hacer referencia a "la persona que buscará sacar beneficio de estos problemas o fallos de seguridad utilizando para ello distintas técnicas como es la ingeniería social o el malware."[1]

INGENIERÍA SOCIAL: Se define como "un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados".[2]

MALWARE: Es una expresión utilizada para precisar cualquier tipo de "malicious software (software malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento. Hay muchos tipos de malware y cada uno busca sus objetivos de un modo diferente".[3]

MITIGAR: Este verbo es definido como **"**Moderar, aplacar, disminuir o suavizar algo riguroso o áspero."[4]

SECTOR RETAIL: Es el sector económico que corresponde a "las cadenas de negocios que se caracterizan por vender artículos de consumo masivo en grandes cantidades a muchos clientes. Éstos suelen ser en su gran mayoría los consumidores finales."[5]

---

[1] HACKER VS Ciberdelincuente | INCIBE | INCIBE [Anónimo]. INCIBE | INCIBE [página web]. [Consultado el 9, julio, 2023]. Disponible en Internet: https://www.incibe.es/aprendeciberseguridad/hacker-vs-ciberdelincuente#:~:text=El%20ciberdelincuente%20es%20la%20persona,ingeniería%20social%20o%20el%20malware.&text=If%20playback%20doesn't%20begin%20shortly,%20try%20restarting%20your%20device.

[2] INGENIERÍA SOCIAL: definición [Anónimo]. latam.kaspersky.com [página web]. [Consultado el 9, julio, 2023]. Disponible en Internet: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

[3] BELCIC, Ivan. ¿Qué es el malware y cómo protegerse de los ataques? ¿Qué es el malware y cómo protegerse de los ataques? [página web]. (19, enero, 2023). [Consultado el 9, julio, 2023]. Disponible en Internet: https://www.avast.com/es-es/c-malware

[4] MITIGAR | Diccionario de la lengua española [Anónimo]. «Diccionario de la lengua española» - Edición del Tricentenario [página web]. [Consultado el 13, septiembre, 2023]. Disponible en Internet: https://dle.rae.es/mitigar

[5] ¿QUÉ ES el sector retail? Descubre cómo iniciarte en él con tu ecommerce [Anónimo]. Shopify [página web]. [Consultado el 9, julio, 2023]. Disponible en Internet:

SMISHING: Es un término empleado para referirse a la "técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima -red social, banco, institución pública, etc. -, con el objetivo de robarle información privada o realizarle un cargo económico."[6]

TRABAJO REMOTO: La legislación colombiana ha definido esta modalidad laboral como:

> "Una forma de ejecución del contrato de trabajo en la cual toda la relación laboral, desde su inicio hasta su terminación, se debe realizar de manera remota mediante la utilización de tecnologías de la información y las telecomunicaciones u otro medio o mecanismo, donde el empleador y trabajador, no interactúan físicamente a lo largo de la vinculación contractual. En todo caso, esta forma de ejecución no comparte los elementos constitutivos y regulados para el teletrabajo y/o trabajo en casa y las normas que lo modifiquen."[7]

PHISHING: Es definida como "una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico."[8]

PHARMING: Es una técnica que se encuentra "compuesta por phishing y pharming, es una estafa en línea que consiste en dirigir a las personas a páginas web fraudulentas que imitan páginas auténticas".[9]

---

https://www.shopify.com/es/blog/que-es retail#:~:text=¿Qué%20significa%20retail?,gran%20mayoría%20los%20consumidores%20finales

[6] SMISHING | INCIBE | INCIBE [Anónimo]. INCIBE | INCIBE [página web]. [Consultado el 9, julio, 2023]. Disponible en Internet: https://www.incibe.es/aprendeciberseguridad/smishing

[7] LEY 2121 de 2021 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. [Consultado el 9, julio, 2023]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=167966

[8] PHISHING | INCIBE | INCIBE [Anónimo]. INCIBE | INCIBE [página web]. [Consultado el 9, julio, 2023]. Disponible en Internet: https://www.incibe.es/aprendeciberseguridad/phishing

[9] DIARIO EL DIA DE LA PLATA WWW.ELDIA.COM. Tarjetas de crédito, otro blanco para el ciberdelito. eldia.com [página web]. (3, abril, 2023). [Consultado el 9, julio, 2023]. Disponible en

VISHING: Este tipo de técnica hace referencia a la gestión “realizada por teléfono o a través de un sistema de comunicación por voz. El cibercriminal se pone en contacto con la víctima a través de una llamada, y por ejemplo, haciéndose pasar por un servicio técnico, le pide a la víctima determinados requisitos para resolver la incidencia."[10]

Internet: https://www.eldia.com/nota/2023-4-3-2-12-32-tarjetas-de-credito-otro-blanco-para-el-ciberdelito-policiales

[10] TÉCNICAS DE ingeniería social [Anónimo]. Cloud Computing | Adaptix Networks | Cómputo en la Nube [página web]. [Consultado el 9, julio, 2023]. Disponible en Internet: https://www.adaptixnetworks.com/tecnicas-de-ingenieria-social/

RESUMEN

El presente proyecto de monografía busca abordar el aumento de los ataques de ingeniería social como práctica para obtener información privada, con el impacto que ha tenido la implementación del trabajo remoto en las empresas del sector retail a partir el factor humano y los errores atribuibles al desconocimiento y falta de formación en materia de seguridad informática.

Este enfoque es de vital importancia para la ingeniería, ya que la ciberseguridad ha evolucionado con el tiempo y requiere una comprensión más completa de los riesgos asociados; además de una orientación al análisis de los programas de información por parte de la empresa, se busca abordar de manera integral el tema de la ingeniería social.

Además, se definen las técnicas más utilizadas por los ciberdelincuentes para acceder a la seguridad informática en las empresas del sector retail, poniendo énfasis en las vulnerabilidades que surgen de la implementación del trabajo remoto. Se examinarán detalladamente técnicas como Phishing, Smishing, Pharming y Vishing, y se analizará su impacto en el sector.

Se expone una evaluación de las medidas preventivas que deben implementarse en las empresas del sector retail para contrarrestar los ataques de ingeniería social más comunes, de tal manera que sea posible establecer pautas claras y efectivas para proteger los sistemas informáticos y la información confidencial, teniendo en cuenta las normas establecidas por la NTC.

Finalmente, con este proyecto, se espera contribuir al conocimiento en el campo de la seguridad informática y proporcionar recomendaciones prácticas para mejorar la protección contra los ataques de ingeniería social en el sector retail.

Palabras claves: Mitigación, Trabajo remoto, ingeniería social, sector retail, ciberdelincuentes.

ABSTRACT

This monograph project seeks to address the increase in social engineering attacks as a practice to obtain private information, with the impact that the

implementation of remote work has had on companies in the retail sector based on the human factor and errors attributable to ignorance. and lack of training in computer security.

This approach is of vital importance for engineering, as cybersecurity has evolved over time and requires a more complete understanding of the associated risks; In addition to an orientation to the analysis of information programs by the company, it seeks to comprehensively address the issue of social engineering.

In addition, the techniques most used by cybercriminals to access computer security in companies in the retail sector are defined, placing emphasis on the vulnerabilities that arise from the implementation of remote work. Techniques such as Phishing, Smishing, Pharming and Vishing will be examined in detail and their impact on the industry will be analyzed.

An evaluation of the preventive measures that must be implemented in companies in the retail sector to counteract the most common social engineering attacks is presented, in such a way that it is possible to establish clear and effective guidelines to protect computer systems and confidential information, taking into account takes into account the standards established by the NTC.

Finally, with this project, we hope to contribute to knowledge in the field of computer security and provide practical recommendations to improve protection against social engineering attacks in the retail sector.

INTRODUCCIÓN

La ingeniería social implica el uso de tácticas psicológicas para influir en el comportamiento humano y obtener información confidencial. Se aprovechan los sesgos mentales e instintos para recopilar datos o acceder a sistemas, y se conoce como "piratería humana" y se utiliza a nivel global. Antes se llevaba a cabo en interacciones directas, pero ahora se ha expandido a través de redes sociales y plataformas en línea.

A lo largo del tiempo, la ingeniería social ha evolucionado y se ha transformado en un instrumento valioso para ciberdelincuentes que buscan acceder a sistemas de información de organizaciones. Los piratas informáticos han mejorado sus técnicas y utilizan métodos más avanzados y sutiles para obtener información confidencial.

Para reducir estos riesgos, es esencial que las organizaciones no solo se concentren en la protección técnica de sus sistemas, sino que también capaciten a su personal en seguridad cibernética y en la identificación y prevención de ataques de ingeniería social. Los empleados tienen un papel fundamental en la protección de la información y deben estar preparados para enfrentar estas amenazas.

La capacitación en seguridad cibernética e ingeniería social debe ser un fragmento integro de la cultura de seguridad organizacional. Esto trae consigo educar a los empleados sobre diferentes tipos de ataques de ingeniería social así cómo reconocerlos y evitarlos. También es crucial que comprendan el valor de la seguridad cibernética, así como su responsabilidad en la protección de la información.

Además de la capacitación, las organizaciones deben implementar políticas sólidas de seguridad cibernética, que incluyan prácticas de autenticación seguras, control de acceso y segregación de redes. El uso de herramientas de monitoreo de amenazas puede ser útil para detectar y prevenir ataques de ingeniería social. También es esencial contar con un plan de respuesta a incidentes para reaccionar adecuadamente en caso de ataques.

En resumen, las organizaciones deben enfocarse en mantener el control de sus sistemas de información para evitar la manipulación y el robo de datos. Esto requiere capacitar y preparar adecuadamente al personal para enfrentar los

desafíos de la ingeniería social. Comprender los intentos de los piratas informáticos para manipular el comportamiento es fundamental para una gestión diaria segura. Si los empleados no se consideran parte de la solución, podrían actuar de manera arriesgada y comprometer la seguridad de la organización.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Según el Ministerio de Comercio de Colombia, a pesar de los grandes esfuerzos del país en incrementar su desarrollo, siguen presentándose marcadas diferencias con naciones desarrolladas en lo relacionado con su microambiente económico, social, ecológico y tecnológico, que para los ciudadanos representan menores condiciones de vida y para el sector empresarial un desafío mayor para su permanencia y crecimiento; pues como lo muestran los indicadores revelados por el mismo ministerio, "el Producto Interno Bruto corriente para el año 2021 fue de US$314,5 millones, un 2,7% inferior a los de prepandemia de 2019 y un PIB per cápita corriente en 2021 cercano a US$6.158, valor superior en US$790 millones al registrado el año anterior"[11]

Especialmente en lo relacionado con el avance tecnológico nacional, el panorama no es el mejor, pese a ser muy claro que para ser un país más competitivo se debe mejorar en su inversión. Al respecto la revista Forbes Colombia ha catalogado como un gran logro, pero lejos de lo requerido, el hecho de que en el año 2021 lo invertido en ciencia y tecnología estuvo por primera vez cerca del 1.0%, con participación del sector público en un 75% de lo invertido y el privado en 25%. Esta mínima inversión ha llevado al país a tener baja penetración de internet fijo y móvil, así como de computadores donde solo el 23% de los hogares lo tenían en el año 2020. [12]

En situación aún más compleja se encuentra el sector empresarial, donde prácticamente las grandes y medianas empresas son las que invierten en tecnología y muy pocas en ciberseguridad, lo que lleva a incrementar el riesgo para los equipos de cómputo, móviles y servidores; así como también para los sistemas electrónicos, de redes y de datos, ante ataques maliciosos. De esta manera, no cuentan con herramientas idóneas, así como tampoco con personal

---

[11] Inicio | MINCIT - Ministerio de Comercio, Industria y Turismo [página web]. [Consultado el 13, julio, 2023]. Disponible en Internet: <https://www.mincit.gov.co/getattachment/1c8db89b-efed-46ec-b2a1-56513399bd09/Colombia.aspx

[12] 'POR PRIMERA vez vamos a superar la barrera del 1% del PIB en inversiones en ciencia y tecnología': MinCiencias [Anónimo]. Forbes Colombia [página web]. [Consultado el 13, julio, 2023]. Disponible en Internet: https://forbes.co/2022/04/06/economia-y-finanzas/por-primera-vez-vamos-a-superar-la-barrera-del-1-del-pib-en-inversiones-en-ciencia-y-tecnologia-minciencias

capacitado que les permita disminuir sus vulnerabilidades frente a ataques informáticos.

En este orden de ideas, es muy importante reconocer que la seguridad de la información encuentra sus bases en los pilares de la integridad, como figura garantista; la confidencialidad, como aporte de reserva y la disponibilidad como capacidad de acceso de esta. Es así como, la ingeniería social representa un riesgo para las políticas de seguridad informática de las empresas colombianas, especialmente aquellas que se dedican al sector retail, máxime cuando sus trabajadores en porcentajes altos hacen trabajo remoto y free lance, convirtiéndose en el eslabón más débil por la falta de formación y cultura de la seguridad y frente a las formas de prevención de ataques informáticos.

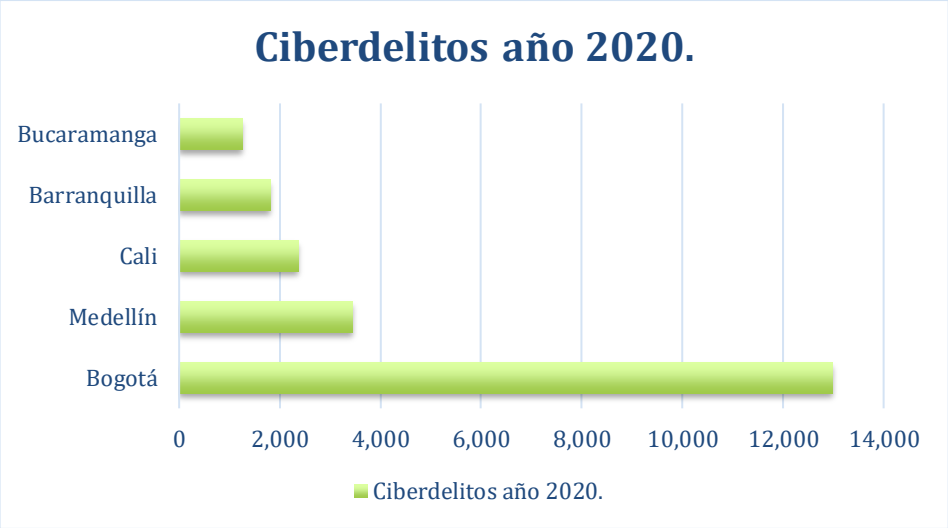
Lo anterior lo confirma el Centro Cibernético de la Policía Nacional y la Dijin citados por la Revista Semana, en donde se menciona que "cada vez los delincuentes encuentran nuevas y mejores formas de actuar. Por eso, los delitos y fraudes cibernéticos se han convertido en un dolor de cabeza para ciudadanos y autoridades, en especial con el incremento del uso de canales electrónicos para la compra y venta de bienes o servicios" [13]

El riesgo expuesto para la adquisición de bienes y servicios es lo que afecta al sector retail con sus ventas derivadas de estrategias realizadas con marketing digital, muchas de las cuales se apoyan en trabajo remoto de sus colaboradores. Situación que ha traído consigo el aumento en la cantidad de ciberdelitos que se cometen en las principales ciudades del país.

En la figura 1 se demuestra la cantidad de delitos que se cometieron en las principales ciudades de Colombia para el año 2020.

[13] ¡OJO! ESTOS son los ciberdelitos que más se cometen en Colombia [Anónimo]. Semana.com Últimas Noticias de Colombia y el Mundo [página web]. [Consultado el 14, julio, 2023]. Disponible en Internet: https://www.semana.com/tecnologia/articulo/ojo-estos-son-los-ciberdelitos-que-mas-se-cometen-en-colombia/202127/

Figura 1. Ciberdelitos en Bogotá

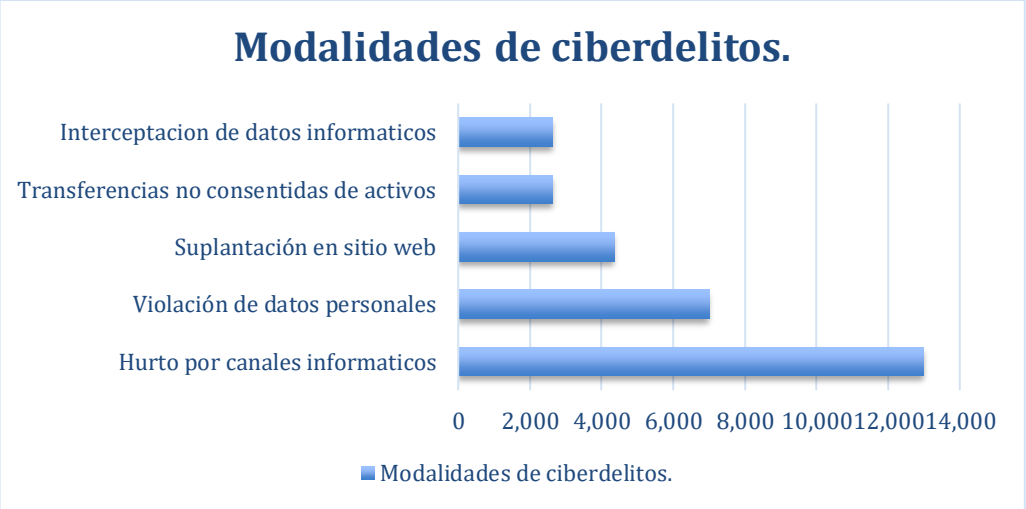


Fuente: Elaboración propia.

Como se observa en el grafico anterior, Bogotá es la ciudad en donde los ciberdelincuentes se lucran con mayor facilidad gracias a estas prácticas, seguida de Medellín, Cali Barranquilla y Bucaramanga. Es aquí, en donde se debe deben analizar las conductas delictuosas más empleadas.

En la figura 2 se muestran las modalidades de ciberdelitos más usadas por los delincuentes.

Figura 2. Modalidades de ciberdelitos más frecuentes



Fuente: Elaboración propia.

Las cifras enseñadas con anterioridad corresponden al año 2020, no obstante, la Policía Nacional, la Dijin, así como, la FISCALIA GENERAL DE LA NACIÓN asegura que la comisión de ciberdelitos se encuentra en aumento, de tal manera que, en el transcurso de los años 2021, 2022 y lo que va corrido del 2023 estas cifras ido creciendo exponencialmente.

Lo cuantificado anteriormente se complica más debido a que el mundo digital es sumamente amplio, se encuentra en un constante crecimiento y los peligros para quienes navegan en la internet no son identificables a simple vista, es por esta razón que, el espacio para que un ciberdelincuente logre su cometido puede estar a un clic. Agravando la situación se encuentra en las empresas, especialmente las dedicadas al retail con empleados que realizan trabajo remoto, que no tienen clara la importancia del conocimiento sobre riesgos informáticos, siendo por esto, que no les es fácil identificar los problemas y peligros a los que pueden exponer la información de la organización empleadora.

De continuar el incremento de ciber delitos, sin que se tomen medidas adecuadas, el miedo de los potenciales compradores va a crecer y con esto, aumentaran las dificultades de las empresas en general y desde luego las del sector retail, para cumplir sus objetivos presupuestales. Por esto, resulta importante en el presente trabajo analizar ¿Cómo influye la implementación del trabajo remoto sobre las empresas del sector retail en el aumento de ataques mediante la ingeniería

social?, esto con la finalidad de evaluar las medidas que pueden implementar las empresas del sector retail con los trabajadores que desarrollen trabajo remoto a fin de prevenir ataques informáticos.

1.2 FORMULACIÓN DEL PROBLEMA

El trabajo remoto se ha convertido en una herramienta cada vez más utilizada por las empresas, incluido el comercio retail. Si bien esta forma de trabajar ha demostrado ser efectiva en términos de flexibilidad y productividad, también crea nuevos desafíos en lo que se refiere a la seguridad de la información. En particular, las empresas del sector retail han visto un aumento en los ataques de ingeniería social desde la introducción del trabajo remoto. Por lo tanto, se propone la siguiente investigación: ¿Cómo influye la implementación del trabajo remoto sin adecuadas medidas de seguridad sobre las empresas del sector retail para el aumento de ataques mediante la ingeniería social?

Para responder a esta pregunta, se revisará la literatura existente sobre el tema y se analizarán empíricamente los datos disponibles sobre las empresas del sector retail que implementan el trabajo remoto. Se examinarán las capacidades de implementación de seguridad de estas empresas y se evaluará su eficacia para atenuar el riesgo de ataques de ingeniería social. Colombia es un país del tercer mundo, lo que significa que es diferente a otros países en términos de condiciones de vida, estatus económico, educación, etc. Esto ha llevado a que algunas empresas del país tengan dificultades para dedicar recursos a asegurar su información; por lo tanto, no cuentan con los instrumentos adecuadas ni personal capacitado para reducir su vulnerabilidad ante ataques informáticos.

La seguridad de la información se fundamenta en su integridad; confidencialidad; igualmente en su disponibilidad. Así, la ingeniería social amenaza la política en seguridad de la información de las empresas colombianas, especialmente en el sector retail, más cuando sus empleados son la parte más débil por falta de capacitación, pedagogía y ataques culturales. El mundo digital es vasto, en constante crecimiento y, dados los peligros de ser invisibles a simple vista, los ciberdelincuentes están a solo un clic de lograr sus objetivos. Sin embargo, los empleados de la empresa no tienen claro el significado de conocimiento de riesgos informáticos, por lo que no les resulta fácil identificar los problemas y peligros a los que puede estar expuesta la información del empleador; a la industria retail en forma de ataques mejorados utilizando ingeniería social, es decir, para evaluar las medidas que las empresas pueden implementar en la industria retail. Un departamento de empleados que trabajan a distancia en

empresas del sector retail para prevenir ataques informáticos. Los resultados de este estudio permiten comprender mejor el impacto de la puesta en marcha del trabajo remoto en la seguridad de la información de las empresas del sector retail.

2. JUSTIFICACIÓN

La adopción del trabajo remoto se ha convertido en una práctica más usual para muchas empresas de la industria retail, especialmente debido a la pandemia mundial originada por el COVID-19. Si bien el trabajo remoto ha demostrado ser una forma eficaz de aumentar la flexibilidad y la productividad de los empleados, también crea nuevos desafíos de seguridad de la información. Las empresas del sector retail en particular han visto un aumento en los ataques de ingeniería social desde la introducción del trabajo remoto. El entorno social, económico y político dicta que el mundo tecnológico está en un inmutable progreso y siempre esforzándose por compensar plenamente las insuficiencias de las personas; lamentablemente, las personas con malas intenciones no se han librado y han ideado diferentes formas de llevar a cabo los ciberdelitos, una de ellas es la ingeniería social; esta es una técnica de ataque cada vez más común que utiliza la manipulación psicológica para extraer información confidencial u obtener acceso no autorizado a los sistemas informáticos.

En la industria se maneja grandes cantidades de información personal, como también financiera de los compradores, la seguridad de la información es fundamental para el renombre y la confiabilidad de una empresa. Con el inicio de la situación extraordinaria en el ámbito sanitario del Covid-19, las empresas del sector retail necesitan implantar el trabajo remoto; sin embargo, esto abrió la puerta a brechas de seguridad y resultó un aumento en las técnicas de ingeniería social contra las compañías. Por lo tanto, en este trabajo se discutirá la importancia de la ingeniería social y las diversas técnicas utilizadas en ella. También es importante señalar que este estudio puede aportar otra información valiosa no solo para las empresas del sector retail, sino también para las industrias que implementan el trabajo remoto.

Luego, describirá los ataques de ingeniería social más empleadas por los ciberdelincuentes para comprometer la seguridad de las empresas retail que utilizan el trabajo remoto como una forma de trabajo y, finalmente, describirá las prácticas que deben implementarse en dicho trabajo. Las empresas están trabajando con sus usuarios para prevenir ataques de ingeniería social; es por ello por lo que se justifica realizar este estudio, ya que permitirá comprender mejor el impacto de la implementación del trabajo remoto en la seguridad de la información de las empresas del sector retail. Además, ayudará a determinar las medidas de seguridad adicionales necesarias para proteger a estas empresas de los ataques de ingeniería social; asimismo, esta investigación es importante porque el comercio retail es una industria clave en muchas economías, y la seguridad de la información en esta industria es indispensable para proteger los datos personales y financieros de los clientes. Los ataques de ingeniería social pueden traer

nefastas consecuencias para las empresas del sector retail, incluida la pérdida de confianza del cliente y posibles infracciones de las leyes y normativas de protección de datos.

3. OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar el impacto de la implementación del trabajo remoto sobre las empresas del sector retail en el aumento de ataques mediante la ingeniería social a fin de implementar prácticas que mitiguen este tipo de ataques.

3.2 OBJETIVOS ESPECÍFICOS

Evaluar Las herramientas de trabajo remoto más usadas comparando sus características de seguridad para generar recomendaciones al momento de su respectivo uso.

Identificar las técnicas más usadas de ingeniería social describiendo su modo de operación evidenciando que el mayor factor detonante es la falta de conocimiento por parte del usuario.

Proponer a las empresas del sector retail con modalidad de trabajo remoto acciones correctivas y preventivas con el fin de reducir o mitigar el riesgo de un ataque de ingeniería social mediante las técnicas de Phishing, Smishing, Vishing y pharming.

4. MARCO REFERNCIAL

4.1 MARCO TEÓRICO

La ingeniería social, conocida como (SE), por sus siglas en inglés, a través del tiempo y conforme lo han mencionado distintos autores; “ha dado lugar a diversas opiniones acerca de lo que significa y la manera cómo esta técnica funciona. No se trata sólo del hecho de simplemente mentir para estafar o cometer un fraude, también se refiere a las herramientas utilizadas por los delincuentes para cometer estos actos delictivos. Esta es una ciencia algo más compleja, cuyas teorías se pueden dividir en partes o ecuaciones para poder ser estudiadas”[14]

La ingeniería social es empleada en los aspectos de la vida diaria más de lo que se piensa; a modo de ejemplo, se puede pensar en el caso “un empleado que no se siente bien pago y que busca un aumento está utilizando la ingeniería social, la manera en que los niños hacen que sus padres cedan a sus caprichos, la manera en que los maestros interactúan con sus estudiantes, en la forma en que médicos, abogados o psicólogos obtienen información de sus pacientes o clientes”[15]. De los casos mencionados en líneas anteriores es claro que en acciones simples y del diario vivir usamos las técnicas de ingeniería social, pero es de destacar que no siempre con intenciones al margen de la ley.

Además, la ingeniería social ciertamente sucede en otros contextos, tales como como los negocios, en la administración nacional y territorial, en el desarrollo del objeto social de las empresas grandes y pequeñas y desafortunadamente, en el ámbito ilegal cuando los delincuentes, los estafadores, etc., engañan a los individuos para que revelen información que facilite la comisión de delitos. En definitiva, es evidente que la ingeniería social no resulta ni buena ni mala, solo que el propósito con el que se aprovecha la herramienta es diferente, lo que le da el enfoque delictivo o legal.

---

[14] Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 17, julio, 2023]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/18701/1075273452.pdf?isAllowed=y&sequence=1

[15] Ibíd., p. 24

En el campo informático, la ingeniería social es definida como “el método utilizado por una persona externa a una organización para robar información por ejemplo el engaño a empleados, generalmente el atacante pretende ser una persona legítima con algún tipo de autoridad para solicitar la información. El atacante de ingeniería social usualmente usa esta información de privilegios para acceder a un sistema informático o base de datos para modificar, alterar o robar información confidencial.”[16]

Los ingenieros sociales a menudo usan herramientas como el teléfono o Internet para engañar a los sujetos del común con la finalidad de que revelen información confidencial en violación de las políticas de seguridad. Los ingenieros sociales que utilizan este enfoque se aprovechan de la tendencia humana a confiar en los demás. Los pilares de la ingeniería social se basan en la explotación humana, que es el eslabón más débil del mecanismo de seguridad.

En cuanto a los ataques, el más simple y común es engañar al usuario haciéndole creer que el delincuente es un administrador del sistema y luego llamar a un técnico para solicitar la contraseña del usuario para un evento específico. En algunos casos, por ejemplo, los PIN de los productos financieros que se encuentran a nombre de la víctima.

Con todas las vulnerabilidades existentes, la mejor estrategia que pueden implementar las compañías para aminorar los riesgos que corre su información, es educar tanto a empleados como usuarios sobre todo lo que atañe la ingeniería social; es decir los diversos métodos de ataque que utilizan los delincuentes, de tal manera que puedan confiar en su privacidad y en la seguridad de sus datos, además de que se les facilitaría cumplir con las políticas de seguridad.

La contribución del estudio a la presente investigación es el enfoque a los instrumentos de las ventajas del trabajo remoto como una modalidad para el buen funcionamiento de las organizaciones; sobre el tema distintos autores han expresado sus puntos de vista, siendo quizás uno de los más relevantes Suárez Vásquez, quien en su tesis de maestría titulada Implementación del teletrabajo y calidad de servicio de la Unidad de Gestión Educativa Local San Pablo, abordó como objetivo general el de determinar la relación de Implementación del

[16] Ibíd., p. 25

Teletrabajo con Calidad de Servicio de la Unidad de Gestión Educativa Local San Pablo.[17]

Por otra parte, Acosta Prada en su artículo Calidad de servicio en comercios retail. Un estudio empírico en Colombia, ilustra como el sector retail es una de las actividades comerciales más vigorosas e importantes del comercio en Colombia y el mundo.[18] A esta clasificación pertenecen magnas compañías y establecimientos que poseen un alto prestigio y reconocimiento; por ello se indaga de manera práctica sobre la calidad de servicio de algunas tiendas de gran superficie en el país, partiendo de aspectos físicos; de confiabilidad; interacción de personal; resolución de problemas y política; aspectos que se consideran son apropiadas para la comprobación de la calidad del servicio del comercio.

El trabajo remoto de define como "un trabajo que se realiza fuera del entorno tradicional de la oficina, también llamado trabajo desde casa o trabajo a distancia. El concepto de trabajo remoto hace referencia a que los empleados puedan ejecutar con éxito los proyectos y las tareas diarias sin necesidad de ir a una oficina todos los días. Existen distintos niveles de oportunidades para el empleo remoto, pero cada uno proporciona el beneficio de la flexibilidad en la vida profesional y personal del empleado."[19]

Los beneficios económicos que trae consigo la implementación del trabajo remoto se traducen en la productividad que cada empleado traería a la empresa, es decir, aumentarían las ventas corporativas al existir mayor motivación del empleado y con los costos fijos se mantienen bajos mientras que los variables lograrían una estabilidad derivando en un crecimiento exponencial de los ingresos que se estiman en un 35% anual dependiendo de la cantidad de trabajadores remotos que tenga la compañía.

---

[17] Institutional Repository [página web]. [Consultado el 17, julio, 2023]. Disponible en Internet: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/46386/Suarez_VLM-SD.pdf?isAllowed=y&sequence=1

[18] REVISTA ESPACIOS | Vol. 38 (NÂº 34) AÃ±o 2017 [Anónimo]. Revista Espacios | HOME [página web]. [Consultado el 17, julio, 2023]. Disponible en Internet: https://www.revistaespacios.com/a17v38n34/17383406.html

[19] ENTENDER LA diferencia entre teletrabajo y trabajo remoto [Anónimo]. Noticias de Abogados, bufetes, jurisprudencia, avisos de ley, de Colombia| Asuntoslegales.com.co [página web]. [Consultado el 19, julio, 2023]. Disponible en Internet: https://www.asuntoslegales.com.co/consultorio/entender-la-diferencia-entreteletrabajo-y-trabajo-remoto-3114944

4.2 MARCO CONCEPTUAL

El trabajo remoto ha ganado significativamente en popularidad en los últimos años, y ha sido aún más acelerado por la coyuntura mundial gracias a la pandemia mundial de COVID-19. En tanto que las organizaciones han adoptado el trabajo remoto para mantener a sus empleados seguros, han surgido nuevos desafíos en cuanto a la seguridad informática. Las compañías del sector retail, en particular, pueden ser especialmente susceptibles a las técnicas de ingeniería social, ya que manejan información susceptible de los clientes. Este marco conceptual proporciona una revisión de la literatura relevante sobre la implementación del trabajo remoto y el aumento de los ataques de ingeniería social en las empresas del sector retail, así como los planes de seguridad que se pueden efectuar para reducir los peligros asociados.

4.2.1 IMPLEMENTACIÓN DEL TRABAJO REMOTO

El trabajo remoto, igualmente distinguido como trabajo a distancia, es una forma de trabajo en la que los empleados pueden realizar sus tareas desde cualquier lugar, utilizando las TIC´S a fin de conectarse con sus colegas o compañeros en la empresa para la cual se labora. El trabajo remoto en los últimos años ha venido tomando popularidad, y no resulta un secreto que la pandemia de COVID-19 ha acelerado aún más la necesidad de su adopción.

Según una encuesta realizada por Gartner a nivel mundial en marzo de 2020 a un numero de 800 ejecutivos especializados en el área de Recursos Humanos “el 88% de las organizaciones han alentado o exigido a sus empleados que trabajen desde sus casas, independientemente de que muestren o no síntomas relacionados con el coronavirus. Casi todas las organizaciones (97%) han cancelado los viajes relacionados con el trabajo, un aumento de más del 80% desde el 3 de marzo del mismo año.”[20]

El trabajo remoto puede proporcionar una serie de beneficios tanto para los

[20] GARTNER: PANDEMIA de COVID-19 impulsa al 88% de las empresas al teletrabajo | Corporate IT [Anónimo]. Corporate IT [página web]. [Consultado el 19, julio, 2023]. Disponible en Internet: https://corporateit.cl/index.php/2020/03/24/gartner-pandemia-de-covid-19-impulsa-al-88-de-las-empresas-al-teletrabajo/

empleados como para las empresas. Los empleados pueden disfrutar de una mayor flexibilidad en cuanto a horarios, lo que puede optimizar la armonía entre la vida laboral lo mismo que, personal. Las empresas pueden disfrutar de una mayor productividad y reducir los costos asociados con las instalaciones de oficina y el transporte.

Sin embargo, el trabajo remoto también puede presentar desafíos, especialmente en cuanto a la seguridad informática. Cuando los colaboradores trabajan fuera de la oficina, pueden estar utilizando dispositivos y redes que no están controlados por la empresa, lo que puede acrecentar la amenaza de ataques cibernéticos y de ingeniería social.

4.2.2 ATAQUES DE INGENIERÍA SOCIAL

La ingeniería social se presenta como una metodología empleada por ciertos individuos con habilidades técnicas para obtener información confidencial o inducir a otros a realizar acciones no deseadas. Los perpetradores utilizan técnicas basadas en aspectos psicológicos, como la persuasión, la presión emocional o la comprensión, con el propósito de obtener datos sensibles o acceder a sistemas de información.

Los ataques de ingeniería social suelen obtener particularmente un resultado positivo en el trabajo remoto, ya que los empleados pueden estar menos conscientes de los riesgos y menos capacitados respecto de lo que concierne a la seguridad de la información. Los ataques pueden incluir phishing, técnica en donde los asaltantes remiten correos electrónicos engañosos para obtener datos sensibles; Pharming; en donde se suplantan páginas web oficiales engañando a la víctima para que piense que la dirección web suministrada por el atacante es verídica o Vishing, en la que los ciberdelincuentes realizan contacto telefónico para influir a la persona atacada a que proporcione su información.

El sector retail es especialmente susceptible a las técnicas de ingeniería social, ya que en algunos casos maneja información privada de los clientes, entre ellos datos de identificación; números de tarjetas de crédito y direcciones de correo electrónico. Además, el sector retail ha sido objeto de numerosos ataques de datos en el pasado, lo que ha advertido el menester de instaurar medidas de seguridad efectivas.

4.2.3 MEDIDAS DE SEGURIDAD

A fin, de reducir los riesgos en la implementación del trabajo remoto y las técnicas de ingeniería social, las organizaciones pueden implementar una serie de medidas de seguridad. Estas medidas pueden incluir la formación de los empleados en mejores prácticas de seguridad de la información, la implementación de políticas de seguridad claras y la utilización de tecnologías de seguridad, como firewalls y software antivirus.

Además, las empresas pueden utilizar la autenticación multifactorial con la finalidad de agregar una capa extra de seguridad a sus sistemas de información. La autenticación multifactorial solicita a los usuarios proporcionar múltiples formas de autenticación para acceder a un sistema, como una contraseña y/o una huella dactilar, lo que aumenta la seguridad de los sistemas de información.

Otra medida de seguridad importante es la implementación de una política de privacidad sólida. Las empresas deben asegurarse de que los datos confidenciales de sus clientes estén protegidos y de que se cumplan todas las leyes y sean relevantes en cuanto a la privacidad de los datos.

En conclusión, la implementación del trabajo remoto ha descubierto la vulnerabilidad de las empresas del sector retail a los ataques de ingeniería social. Es importante que las empresas implementen planes de seguridad adecuados para mitigar los riesgos asociados con el trabajo remoto y los ataques de ingeniería social. Esto puede incluir la capacitación de empleados con la finalidad de entender cuáles son las mejores prácticas de seguridad informática a tener en cuenta, la utilización de tecnologías de seguridad, como la autenticación multifactorial y la implementación de políticas de privacidad sólidas. Al tomar estas medidas de seguridad, las empresas pueden ayudar a proteger los datos confidenciales de sus clientes y conservar la confianza en su marca.

Otros planes de seguridad que pueden ser establecidos por las empresas del sector retail para mitigar los riesgos de las técnicas de ingeniería social incluyen la segmentación de la red; la gestión de parches, así como las actualizaciones. La segmentación de la red implica la división de una red en segmentos pequeños, esto con el fin de controlar el acceso a los datos sensibles y reducir el riesgo de propagación de ataques. La gestión de parches y actualizaciones es importante porque los sistemas que no están actualizados pueden ser indefensos a los ataques de ingeniería social, ya que los atacantes pueden utilizar las vulnerabilidades conocidas para ingresar a sus sistemas.

La formación de los empleados referente a las mejores prácticas que se deben tener en cuenta respecto de la seguridad informática también es crucial para proteger a las empresas del sector retail de las diferentes técnicas de ingeniería social. Los empleados deben ser conscientes de los diferentes tipos de ataques de ingeniería social, como el phishing, Smishing, Vishing y Pharming, y cómo pueden ser detectados y evitados. Las empresas también pueden realizar simulaciones de ataques para evaluar la forma de reacción de los empleados en este tipo de eventos a fin de proporcionar formación adicional o retroalimentación en caso necesario.

Por último, poner en marcha un plan de respuesta ante incidentes puede ser crítico para mitigar el impacto de los ataques utilizados por los ciberdelincuentes. Un plan de respuesta a estos sucesos debe incluir la identificación y aislamiento del mismo, la notificación de las partes afectadas, la recuperación de los sistemas y la realización de un análisis para determinar las causas del incidente y las medidas necesarias para prevenir futuros incidentes.

4.3 MARCO HISTÓRICO

La aparición de la ingeniería social en los años 80’ como una táctica de ataque se vio favorecida por el crecimiento de las TIC y el uso de redes en las empresas. Durante esta década, los primeros intentos de ingeniería social se basaron en el engaño y la manipulación psicológica para obtener información confidencial de empleados y usuarios desprevenidos.

En 1990 el auge de Internet y la adopción masiva de correos electrónicos proporcionaron nuevos canales para la propagación de ataques de ingeniería social. Los ciberdelincuentes empezaron a utilizar emails fraudulentos y páginas falsas con el fin de engañar a los usuarios y así extraer información personal o credenciales de acceso a sistemas empresariales.

4.3.1 Principios del siglo XXI: Con la llegada de las redes sociales y una mayor presencia en línea, los ataques de ingeniería social se volvieron más sofisticados y dirigidos. Los ciberdelincuentes aprovecharon la abundante información personal disponible en redes sociales para personalizar los ataques y hacerlos más convincentes.

Además, la creciente adopción de tecnologías móviles y la proliferación de aplicaciones en dispositivos inteligentes abrieron nuevas oportunidades para los ataques de ingeniería social. Los empleados de las empresas empezaron a utilizar sus dispositivos personales para acceder a sistemas corporativos, lo que aumentó la superficie de ataque y la vulnerabilidad a este tipo de amenazas.

4.3.2 Mediados del Siglo XXI: Con la implementación masiva del trabajo remoto en muchas empresas, como resultado de avances en las comunicaciones y las TIC, los ataques de ingeniería social encontraron un nuevo campo de oportunidades. La falta de infraestructura de seguridad en algunos entornos de trabajo remoto y la posibilidad de empleados desprevenidos o menos conscientes de los riesgos, hicieron que los ataques de ingeniería social se intensificaran y se volvieran más persistentes.

4.3.3 Actualidad: El desarrollo tecnológico sigue influyendo en los ataques de ingeniería social. El uso generalizado de aplicaciones de mensajería y redes sociales, así como la creciente integración de la inteligencia artificial en sistemas de comunicación, han permitido a los atacantes adaptar y personalizar aún más sus tácticas de ingeniería social. Además, la aparición de técnicas más avanzadas, como el Phishing, Smishing, Pharming, Vishing, ha llevado a una mayor sofisticación en los ataques, lo que dificulta su detección y prevención por parte de las empresas.

Conforme avanza la tecnología, se espera que los ataques de ingeniería social continúen progresando y ajustándose a las nuevas tendencias tecnológicas. Los delincuentes cibernéticos aprovecharán el crecimiento a lo que se refiere al internet de las cosas (IoT), la expansión de la inteligencia artificial y la adopción de tecnologías emergentes para incrementar la efectividad igual que el alcance de sus ataques.

Por lo tanto, es crucial que las empresas se mantengan al día y tomen medidas proactivas para reforzar sus políticas de seguridad, sensibilizar a sus empleados acerca de los riesgos de la ingeniería social y adoptar soluciones avanzadas de protección para afrontar los futuros desafíos en materia de ciberseguridad.

4.4 ANTECEDENTES O ESTADO ACTUAL

El avance tecnológico es imparable y la vida de las personas ha cambiado drásticamente en el transcurso de los años. con el fin de cubrir sus necesidades profesionales, personales, laborales y sociales, incluso de supervivencia; el acceso a conexión de redes WI-FI es uno de los mayores avances; sin embargo, a pesar de los grandes beneficios que trae la tecnología, también tiene su lado oscuro, que puede ser peligroso para quien la usa, y lo más importante para quien no sabe usarla correctamente pues las consecuencias pueden llegar a ser irreversibles.

Los ataques informáticos, son ataques personales muy comunes que causan el máximo daño a la mayor cantidad de sistemas posibles, no tienen un objetivo específico, no obstante, en los últimos años el perfeccionamiento de estos ataques dirigidos a usuarios determinados se ha destacado, pues utilizan varias técnicas para evitar la detección de los sistemas de defensa actuales.

Teniendo en cuenta que día a día los ciberdelincuentes utilizan técnicas más sofisticadas "el código malicioso utilizado en los ataques actuales tiene consecuencias mucho más devastadoras que los gusanos y virus de la última década. Muchos sistemas de protección existentes no son suficientes para detener nuevos tipos de código malicioso. Reconocido por los piratas se empiezan a desarrollar debilidades en las defensas con nuevas vulnerabilidades y nuevos ataques."[21]

> "Una característica clave de los ataques modernos es que se dirigen al eslabón más débil de la cadena de seguridad: los humanos, como hablan los autores K. Mitnick y W. Simon Los ataques de Ingeniería Social pueden tener éxito cuando la gente es estúpida o, más comúnmente, simplemente ignorante acerca de las buenas prácticas de seguridad Puede ser difícil ignorar el enorme impacto que este libro y sus autores han tenido en ellos.

[21] Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 17, julio, 2023]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/18701/1075273452.pdf?isAllowed=y&sequence=1

Este tema apenas se toca en este libro, aunque hoy en día puedes encontrar miles de fuentes de información sobre ingeniería social."[22]

[22] Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 17, julio, 2023]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/18701/1075273452.pdf?isAllowed=y&sequence=1

4.5 MARCO CIENTÍFICO O TECNOLÓGICO

En esta sección, se realizará un análisis exhaustivo del marco científico y tecnológico relacionado con la implementación del trabajo remoto y las técnicas de ingeniería social en el sector retail. Se explorarán estudios, investigaciones y avances relevantes en el campo, proporcionando una base sólida para comprender la problemática y los desafíos asociados.

4.5.1 Avance tecnológico en el ámbito del trabajo remoto.

En primer lugar, se examinarán los avances tecnológicos que han impulsado el desarrollo y la adopción del trabajo remoto en las últimas décadas. Se analizarán las herramientas de comunicación y colaboración digital, como videoconferencias, plataformas de gestión de proyectos en línea y aplicaciones móviles, que han facilitado la realización de tareas a distancia. Además, se revisarán las tendencias y los desafíos emergentes en el ámbito del trabajo remoto, como la seguridad informática y la custodia de datos.

4.5.2 Investigaciones sobre ingeniería social y seguridad informática.

En esta sección, se examinarán las investigaciones más relevantes asociadas con la ingeniería social y la seguridad informática. Se abordarán estudios que han analizado las técnicas implementadas por los ciber atacantes para llevar a cabo ataques de ingeniería social, así como las consecuencias y los impactos que han tenido en las organizaciones. También se destacarán las estrategias y medidas preventivas propuestas en la literatura científica para contrarrestar este tipo de ataques.

4.5.3 Estudios sobre la situación tecnológica y de seguridad en el sector retail.

En esta subsección, se explorarán investigaciones y estudios que han analizado la situación tecnológica y de seguridad en el sector retail, particularmente en relación con la implementación del trabajo remoto. Además, se revisarán los desafíos y las brechas de seguridad identificadas en investigaciones previas.

4.5.4 Marco normativo y regulaciones relevantes.

Por último, se abordará el marco normativo y las regulaciones relevantes relacionadas con la implementación del trabajo remoto y la seguridad informática en el sector retail. Se analizarán las normas y estándares nacionales, así como las políticas igual que las regulaciones nacionales que influyen en la defensa de la información y la precaución de ataques de ingeniería social.

En resumen, en este apartado se realizará una revisión crítica del marco científico y tecnológico relacionado con el trabajo remoto y los ataques de ingeniería social en el sector retail. Se presentarán investigaciones y avances tecnológicos relevantes que respalden y contextualicen la problemática abordada en el proyecto. Además, se examinarán las investigaciones sobre ingeniería social y seguridad informática, así como la situación tecnológica y de seguridad en el sector retail. Por último, se abordará el marco normativo y las regulaciones pertinentes para comprender el contexto legal y las políticas relacionadas con la temática.

4.6 MARCO LEGAL

Ley 527 de 1999: “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.[23]

Ley 594 de 2000: “Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.[24]

Ley 1266 de 2008: “Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”.[25]

La Ley 1273 de 2009, conocida como “Ley de Protección de la Información y los Datos, es una legislación que introduce modificaciones al Código Penal y establece la creación de un nuevo bien jurídico tutelado. Su objetivo principal es preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.”[26]. Esta ley contempla disposiciones que buscan proteger la integridad, reserva y accesibilidad de la información, también busca sancionar los delitos informáticos y las violaciones a la seguridad de los sistemas. En resumen, la Ley 1273 de 2009 tiene como finalidad fortalecer el cuidado y seguridad de los datos en el entorno digital, con el propósito de asegurar un uso correcto y garante de las tecnologías de la información y las comunicaciones.

---

[23] LEY 527 de 1999 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

[24] LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [LEY_0594_2000] [Anónimo]. SECRETARÍA GENERAL DEL SENADO [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_0594_2000.html

[25] LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [LEY_1266_2008] [Anónimo]. SECRETARÍA GENERAL DEL SENADO [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

[26] LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009] [Anónimo]. SECRETARÍA GENERAL DEL SENADO [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Ley 1341 de 2009: “Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones”.[27]

Ley Estatutaria 1581 de 2012: “Por la cual se dictan disposiciones generales para la protección de datos personales”.[28]

Ley 1712 de 2014: “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.[29]

CONPES 3854: “Política Nacional de Seguridad Digital en Colombia, donde el Estado se basa en principios fundamentales como; salvaguardar derechos humanos, enfoque incluyente y colaborativo, responsabilidad compartida y enfoque de gestión de riesgo.[30]

---

[27] LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [LEY_1341_2009] [Anónimo]. SECRETARÍA GENERAL DEL SENADO [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

[28] LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [LEY_1581_2012] [Anónimo]. SECRETARÍA GENERAL DEL SENADO [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[29] LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [LEY_1712_2014] [Anónimo]. SECRETARÍA GENERAL DEL SENADO [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

[30] [Consultado el 20, julio, 2023]. Disponible en Internet: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854_Adenda1.pdf

5. DESARROLLO DE LOS OBJETIVOS

El desarrollo de los objetivos corresponde a al fragmento de mayor relevancia en cualquier investigación, ya que permite definir con claridad las finalidades específicas que se escudriñarán mediante el desarrollo de la investigación.

En el presente capítulo, se seguirá la ampliación del objeto de la investigación, que se ha llamado: Análisis del impacto en la implementación del trabajo remoto, respecto del aumento de ataques de ingeniería social en las empresas del sector retail.

En un aspecto general, esta investigación buscará responder al interrogante de ¿cómo influye la implementación del trabajo remoto sin adecuadas medidas de seguridad sobre las empresas del sector retail para el aumento de ataques mediante la ingeniería social?, esto con la finalidad de implementar prácticas que mitiguen este tipo de ataques. Para lograr responder esta pregunta y emitir las recomendaciones que permitan reducir dichos ataques se abordarán como temas principales las herramientas de trabajo remoto más usadas en las empresas del sector retail, así como las características de seguridad que cada herramienta puede poseer y sus recomendaciones. Por otro lado, se hablará de las técnicas más usadas de ingeniería social y finalmente, se hará referencia acciones correctivas y preventivas para reducir o mitigar el riesgo de un ataque de ingeniería social en entornos de trabajo remoto.

Cada tema a abordar se enfoca en una tarea distinta dentro de la investigación, pero todos están interconectados y son necesarios para dar respuesta al interrogante planteado y así alcanzar el objetivo general.

El desarrollo de estos objetivos permitirá una mayor claridad en la planificación de la investigación, asegurando que se alcancen los resultados deseados y se puedan obtener conclusiones relevantes sobre el impacto de la implementación del trabajo remoto en los ataques de ingeniería social en las empresas del sector retail.

5.1 EVALUAR LAS HERRAMIENTAS DEL TRABAJO REMOTO MÁS USADAS COMPARANDO SUS CARACTERÍSTICAS DE SEGURIDAD PARA GENERAR RECOMENDACIONES AL MOMENTO DE SU RESPECTIVO USO.

Para llevar a cabo esta tarea, es necesario identificar las herramientas de trabajo remoto más utilizadas en las empresas del sector retail y llevar a cabo una valoración completa de sus propiedades de seguridad. Es importante tener en cuenta que las herramientas de trabajo remoto deben cumplir con altos estándares de seguridad, ya que se trata de una de las primordiales preocupaciones de las compañías en cuanto a la implementación del trabajo remoto.

La evaluación de las herramientas de trabajo remoto debe considerar aspectos como la autenticación, el cifrado de datos, la gestión de contraseñas, la gestión de permisos; así entonces resulta necesario evaluar cada herramienta en función de estos aspectos y comparar sus fortalezas y debilidades.

Una vez realizada la evaluación de las herramientas de trabajo remoto, se podrán generar recomendaciones sobre su uso adecuado en el ejercicio de las obligaciones y finalidades de cada compañía del sector retail. Estas recomendaciones pueden incluir la adopción de ciertas herramientas de trabajo remoto en función de su seguridad, la puesta en funcionamiento de medidas adicionales de seguridad a fin de mejorar la protección de datos, además de la capacitación del personal en cuanto mejores prácticas de seguridad en el trabajo remoto.

Además, es importante destacar que dicha evaluación de las herramientas de trabajo remoto debe ser un proceso continuo y actualizado, ya que la seguridad es un tema que evoluciona constantemente. Es necesario estar al tanto de los novedosos riesgos y vulnerabilidades que puedan manifestarse con el propósito de ajustar las medidas de seguridad que correspondan.

Es posible que algunas herramientas de trabajo remoto puedan presentar características de seguridad más avanzadas que otras, por lo que es importante que las empresas del sector retail tengan en cuenta sus necesidades y objetivos específicos al elegir la herramienta más adecuada. Por ejemplo, una empresa que maneja grandes cantidades de datos sensibles puede requerir una herramienta con una mayor protección contra ataques de ingeniería social, mientras que una empresa que se enfoca más en la comunicación y colaboración en línea puede requerir herramientas que permiten una mayor facilidad de uso y acceso remoto.

El trabajo remoto se ha tornado en una praxis más frecuente en el mundo laboral actual. Con el aumento del trabajo remoto, también ha habido un aumento en el uso de las herramientas de trabajo remoto disponibles. Estas herramientas van desde aplicaciones de videoconferencia hasta plataformas de colaboración en equipo. Sin embargo, no todas estas herramientas ofrecen el mismo nivel de seguridad.

Es importante evaluar las herramientas de trabajo remoto más utilizadas para establecer qué herramientas son las más seguras y ofrecen las mejores características de seguridad para preservar datos sensibles de la organización y de los usuarios. Al evaluar las herramientas de trabajo remoto, resulta posible delimitar las fortalezas y debilidades de cada herramienta en términos de seguridad y se pueden tomar decisiones informadas sobre qué herramientas utilizar en una tarea específica.

5.1.1 Zoom: Es una plataforma de videoconferencia que ha tenido algunos problemas de seguridad en el pasado. Sin embargo, la plataforma se ha enfocado en mejorar significativamente su seguridad a fin de favorecer a sus usuarios.

Esta plataforma ofrece una amplia gama en opciones de seguridad, tales como contraseñas de reunión, salas de espera, y la capacidad de bloquear una reunión una vez que todos los asistentes han llegado. Estas características ayudan a asegurar que solo los individuos autorizados puedan unirse a una reunión y que la información transmitida durante la reunión esté protegida.

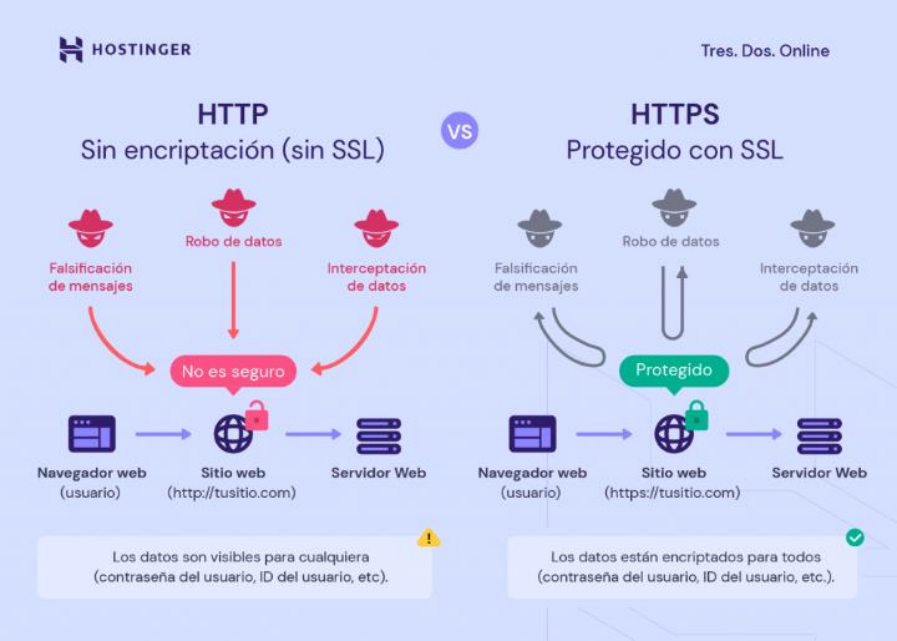
Una de las debilidades más marcadas de ZOOM se traduce a la facilidad con la cual cualquier persona puede acceder a las reuniones conociendo el ID de la reunión, siempre que el creador no cuente con las salas de espera y las contraseñas activadas; lo que permite entonces decir que quien se denomina en esta plataforma como el anfitrión, tiene a su cargo los estándares de seguridad de las reuniones; por ejemplo si el anfitrión de una reunión en la que se tratarán los temas comerciales de una compañía, no hace un buen uso de las opciones de seguridad y permite que cualquiera de los asistentes pueda compartir pantalla, podría suceder que cualquiera proyectara su pantalla haciendo ver contenido para adultos, lo que no tiene ninguna conexión lógica con el fin de la reunión que se pretendía adelantar.

Esta plataforma, maneja los siguientes protocolos de seguridad:

- **TRANSPORT LAYER SECURITY**, también llamado TLS, por sus siglas en inglés, siendo esta la versión actualizada del protocolo SSL; es el encargado de brindar la seguridad a la capa de transporte proporcionando la encriptación de datos entre emisor y receptor, permitiendo así que solo los destinatarios permitidos tengan acceso a la lectura de los mensajes.

En la figura 3, se evidencia cómo funciona el protocolo de seguridad TLS.

Figura 3. Navegación segura utilizando TLS

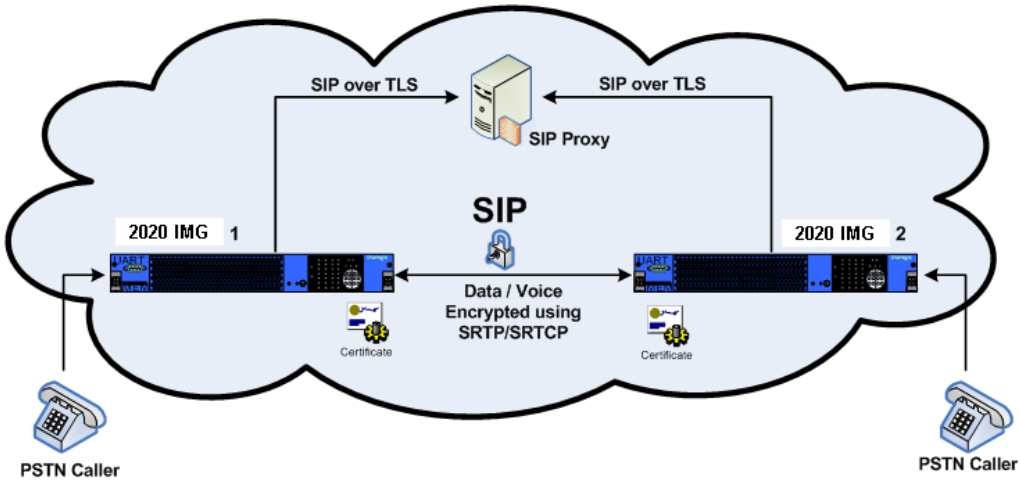


Fuente https://www.hostinger.co/tutoriales/que-es-tls#Diferencia_entre_TLS_y_SSL_y_como_saber_cual_estas_utilizando>

- **SECURE REAL-TIME TRANSPORT,** también llamado SRTP, por sus siglas en inglés; este protocolo permite la remisión de archivos multimedia de manera confiable y segura; por ejemplo, el video de una conferencia.

En la figura 4, se evidencia cómo funciona el protocolo de seguridad SRTP.

Figura 4. Protocolo SRTP

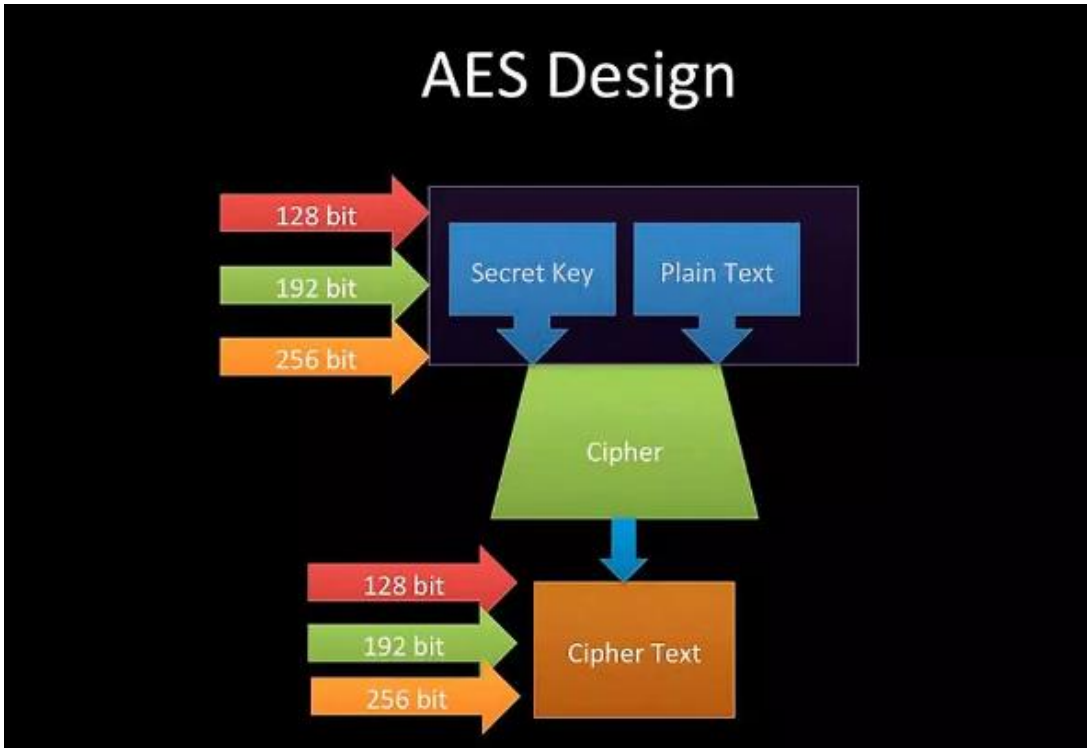


Fuente: https://wiki.freepbx.org/display/DIMG/SRTP+-+Overview>

- **AVANCED ENCRYPTION STANDARD,** también llamado AES-256 BITS por sus siglas en inglés; siendo este uno de los cifrados de extremo a extremo más seguros a nivel mundial, permitiendo que los datos antes de salir a internet se cifren con una clave criptográfica que debe ser igual tanto para el emisor como para el receptor.

En la figura 5, se evidencia cómo funciona el protocolo de diseño cifrado AES-256 Bits.

Figura 5. Diseño cifrado AES-256 Bits



Fuente: https://hardzone.es/tutoriales/rendimiento/cifrado-aes-256-bits-como-funciona/

A continuación, basándonos en las herramientas MITRE ATT&CK y NATIONAL VULNERABILITY DATABASE, se evidencian algunas vulnerabilidades de la plataforma y sus recomendaciones con el fin de ser mitigadas:

CVE-2023-39218

- **Descripción:** La aplicación del lado del cliente de la seguridad del lado del servidor en los clientes de Zoom antes de 5.14.10 puede permitir que un usuario privilegiado habilite la divulgación de información a través del acceso a la red.

- **Mitigación:** Actualización a la versión Zoom 5.14.10

CVE-2023-39216

- **Descripción:** Se identificó un fallo en la verificación de datos ingresados en la aplicación Zoom Desktop Client en su versión para Windows previa a la 5.14.7. Esta vulnerabilidad podría dar la posibilidad a un individuo que no ha iniciado sesión de activar un proceso de aumento de sus privilegios mediante el aprovechamiento de la conexión a la red.

- **Mitigación:** Actualización Zoom a la versión 5.14.7.

CVE-2023-39214

- **Descripción:** La exposición de información confidencial en Zoom Client SDK antes de 5.15.5 puede permitir que un usuario autenticado habilite una denegación de servicio a través del acceso a la red.

- **Mitigación:** Actualización a la versión 5.15.5.

CVE-2023-34119

- **Descripción:** El archivo temporal no seguro en el instalador de Zoom Rooms para Windows anterior a la versión 5.15.0 puede permitir que un usuario autenticado habilite una escalada de privilegios a través del acceso local.

- **Mitigación:** Actualización zoom a la versión 5.14.0

Basándose en la descripción proporcionada, así como en las vulnerabilidades antes referidas, paso seguido, se ofrecen algunas recomendaciones de seguridad para los usuarios al utilizar la plataforma ZOOM.

- Habilitar la sala de espera y contraseñas: El anfitrión de la reunión debe activar la opción de sala de espera y establecer una contraseña para todas

las reuniones. Esto ayudará a evitar que personas no autorizadas accedan a la reunión con solo conocer el ID de la misma.

- Compartir el enlace de la reunión de forma segura: El anfitrión debe compartir el enlace de la reunión de manera privada, preferiblemente a través de correos electrónicos individuales o plataformas de mensajería segura, en lugar de hacerlo públicamente en redes sociales u otros medios abiertos.

- Limitar los permisos de los participantes: El anfitrión debe revisar y ajustar los permisos de los participantes en la reunión. Por ejemplo, restringir la capacidad de compartir pantalla y silenciar a los asistentes cuando no estén hablando para evitar interrupciones no deseadas.

- Actualizar el software de ZOOM: Tanto el anfitrión como los participantes deben asegurarse de tener instalada la versión más reciente del software de ZOOM, ya que las actualizaciones suelen incluir mejoras en la seguridad.

- Estar atento a los participantes desconocidos: El anfitrión debe supervisar constantemente la lista de participantes y, si identifica a alguien desconocido o sospechoso, puede expulsarlos de la reunión.

- Concientizar a los participantes sobre la seguridad: Antes de iniciar la reunión, el anfitrión puede recordar a los participantes las pautas de seguridad y el interés de mantener la privacidad de la información tratada en la reunión.

5.1.2 Microsoft Teams: Es una herramienta de colaboración en equipo que ofrece chat, videollamadas y la capacidad de compartir archivos; utiliza una variedad de medidas de seguridad, como la autenticación multifactor, encriptación de datos y la capacidad de establecer permisos de usuario. Estas medidas de seguridad ayudan a garantizar que la información transmitida a través de la plataforma esté protegida y que solo las personas autorizadas puedan acceder a ella.

Esta plataforma tiene similitudes con Zoom en cuanto a la seguridad de datos se refiere, pues igual que aquella utiliza los protocolos TLS, SRTP y AES-256 BITS,

que como se mencionó líneas arriba, buscan asegurar la protección de datos mediante la encriptación de los mismos, el cifrados de extremo a extremo y el intercambio de archivos multimedia de manera confiable. Para soportar esta información la figura referenciada continuación busca evidenciar los tráficos de Microsoft Teams y el protocolo que aplica para cada uno de ellos.

En la figura 6, se evidencia el cifrado por tipo de tráfico.

Figura 6. Cifrado por tipo de tráfico

Tipo de tráfico	Cifrado por
Servidor a servidor	TLS (con MTLS o OAuth de servicio a servicio)
Del cliente al servidor, por ejemplo, mensajería instantánea y presencia	TLS
Flujos multimedia, por ejemplo, uso compartido de audio y vídeo multimedia	TLS
Uso compartido de audio y vídeo en elementos multimedia	SRTP/TLS
Señalización	TLS
Cifrado mejorado de cliente a cliente (por ejemplo, llamadas de cifrado de un extremo a otro)	SRTP/DTLS

Fuente: https://learn.microsoft.com/es-es/microsoftteams/teams-security-guide

En esta plataforma, para la función específica de videollamadas, el moderador (creador de la reunión), tiene bajo su cargo herramientas proporcionadas por Microsoft Teams que permiten aumentar la seguridad de las reuniones, de tal manera que bajo su mando están los controles que permitirán durante el transcurso de las reuniones, por ejemplo, permitir el intercambio de datos, el acceso al chat, admitir o eliminar participantes, iniciar o detener grabaciones, entre otras. Es aquí en donde cobra especial relevancia la capacitación que puedan

recibir las personas sobre el uso del aplicativo, pues si bien es cierto la responsabilidad de seguridad recae de manera principal en Microsoft, los usuarios deben conocer las políticas para el uso correcto y seguro de la aplicación.

A continuación, se evidencia algunas vulnerabilidades de Microsoft Teams y sus recomendaciones con el fin de ser mitigadas.

CVE-2020-10146

- **Descripción:** La plataforma en línea de Microsoft Teams presenta una debilidad relacionada con la manipulación de secuencias de comandos entre diferentes sitios. Almacenada en el parámetro displayName que se puede explotar en los clientes de Teams para obtener información confidencial, como tokens de autenticación, y posiblemente para ejecutar comandos arbitrarios.

- **Mitigación:** Se solucionó con una actualización realizada por el fabricante en el mes de octubre de 2020.

CVE-2023-24881

- **Descripción:** Vulnerabilidad de divulgación de información de Microsoft Teams.

- **Mitigación:** Aplicación parche de seguridad sugerido por el fabricante.

CVE-2022-21965

- **Descripción:** Vulnerabilidad de denegación de servicio de Teams.

- **Mitigación:** Aplicación parche de seguridad sugerido por el fabricante.

A consecuencia de lo anterior descrito, se presentan algunas recomendaciones de seguridad para los usuarios al utilizar Microsoft Teams.

- Asegurar una autenticación segura al habilitar el método de autenticación multifactor en las cuentas de Microsoft Teams. Esto añade una capa extra de protección al exigir una segunda forma de comprobación, como recibir un código en tu dispositivo móvil, además de ingresar el password, para poder iniciar sesión.
- Contraseñas sólidas: Utilizar password alfanuméricos de la cuenta de Microsoft Teams. Evitar reutilizar Password de otras cuentas y cambia las contraseñas periódicamente.

- Controlar permisos de usuario: Como moderador o creador de la reunión, revisa y establece cuidadosamente los permisos de usuario para los participantes de la videollamada. Limita el acceso a funciones sensibles, como compartir archivos o grabar la reunión, solo a las personas necesarias.

- Mantener el software actualizado: Asegurar la versión más actualizada de Microsoft Teams y cualquier complemento que se utilice. Las actualizaciones suelen incluir mejoras de seguridad y corrección de vulnerabilidades.

- Cuidado con archivos y enlaces sospechosos: Ser precavido al momento de ejecutar clic en una URL o ejecutar archivos enviados por desconocidos, ya que podrían contener malware o intentar engaños para revelar información confidencial.

- Conocer las políticas de seguridad de la empresa: Al momento de utilizar Microsoft Teams en un entorno empresarial, asegurarse de conocer y cumplir con las políticas instauradas por la compañía.

- Cerrar sesiones y reuniones adecuadamente: Al finalizar una videollamada o cuando ya no se necesite el uso Microsoft Teams, se debe asegurar cerrar sesión correctamente para evitar accesos no autorizados.

- Capacitación y concientización: Es importante que todos los usuarios reciban capacitación sobre las medidas de seguridad y buenas prácticas al utilizar Microsoft Teams. Esto incluye el conocimiento de cómo configurar adecuadamente las reuniones, gestionar los permisos y evitar riesgos de seguridad.

5.1.3 Microsoft Outlook: Es una aplicación desarrollada por Microsoft para gestionar información, incluida en la suite de Microsoft Office. Aunque su principal función es como cliente de correo electrónico, adicionalmente brinda diversas utilidades para organizar calendarios, contactos y tareas. Su interfaz intuitiva y facilidad de uso la hacen muy popular ya sea en el entorno laboral o en el ámbito personal, facilitando la comunicación y la organización cotidiana.

En su rol como cliente de correo electrónico, Outlook autoriza a los usuarios realizar el envío, recepción y ordenamiento de correos electrónicos de forma efectiva y ágil, con opciones para crear reglas en las bandejas de entrada y buscar mensajes y archivos adjuntos de una forma ágil.

La propiedad de calendario de Outlook brinda a los usuarios la posibilidad de planificar y organizar eventos y reuniones, configurar recordatorios y compartir sus horarios con otros, simplificando la programación y coordinación de actividades. Además, Outlook ofrece una herramienta de administración de contactos, donde los usuarios pueden almacenar y organizar información sobre personas y empresas, lo que facilita el envío de correos electrónicos y la gestión de datos de contacto importantes.

Microsoft Outlook es una solución completa para gestionar información, que incluye correo electrónico, calendario y contactos, proporcionando a los usuarios las herramientas necesarias para mantenerse organizados y productivos tanto en su vida personal como laboral. Cada persona que utiliza Outlook.com experimenta beneficios gracias al filtrado de correos no deseados y software malicioso. No obstante, aquellos que son suscriptores de Microsoft 365 reciben una ventaja adicional; en este caso, Outlook.com lleva a cabo un análisis adicional de los archivos adjuntos y enlaces de los mensajes que les llegan, buscando brindar una mayor seguridad y protección.

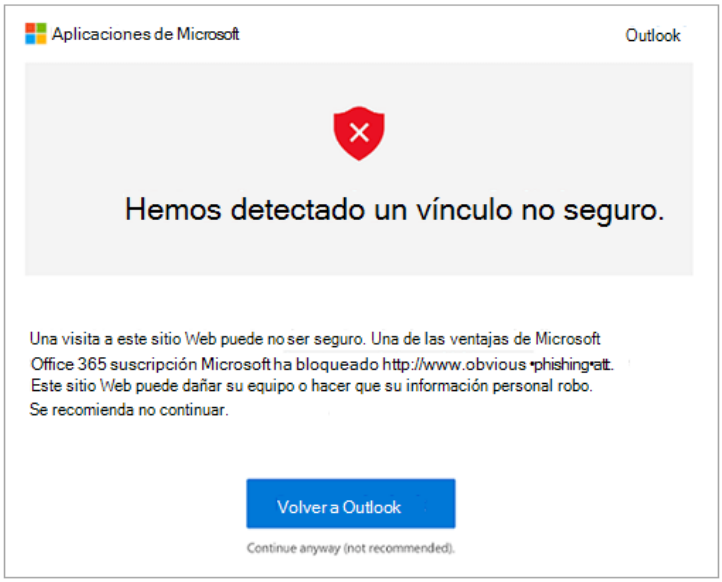
Cuando un usuario recibe mensajes con archivos adjuntos en Outlook.com, el sistema realiza un minucioso análisis de dichos archivos para detectar posibles virus y software malicioso. Este proceso se lleva a cabo utilizando métodos de identificación avanzados que ofrecen una capa de seguridad más elevada en

comparación con la versión gratuita del servicio. Si se identifica un archivo peligroso, Outlook.com lo eliminará automáticamente para evitar que el usuario lo abra por accidente. De esta manera, se asegura una experiencia más segura y libre de riesgos al utilizar el servicio de correo electrónico.

Outlook pretende garantizar vínculos confiables. Cuando el usuario recibe mensajes con enlaces a sitios en internet, Outlook.com verifica si dichos enlaces están vinculados a intentos de técnicas de suplantación de identidad (phishing) o si cabe la posibilidad de que se descargue virus o software malicioso en el dispositivo de acceso. Si se ingresa a un enlace dudoso, el cliente será redirigido a un sitio de advertencia similar a esta.

En la figura 7, se evidencia el bloqueo que realiza Microsoft cuando detecta un vínculo no seguro.

Figura 7. Ejemplo bloqueo de vinculo no confiable



Fuente: https://support.microsoft.com/es-es/office/seguridad-avanzada-de-outlook-com-para-suscriptores-de-microsoft-365-882d2243-eab9-4545-a58a-b36fee4a46e2#:~:text=Todos%20los%20usuarios%20de%20Outlook,de%20los%20mensajes%20que%20recibe.

Estas medidas de seguridad funcionan de forma independiente sin importar cómo se accede al correo electrónico en Outlook.com. Las características de seguridad se implementan en nube, lo cual garantiza la protección, ya sea que acceda a el correo a través del sitio web de Outlook.com, desde el móvil o localmente en el sistema operativo de preferencia.

Es importante destacar que esta protección se aplica exclusivamente a las cuentas de correo de Outlook.com. Las medidas de protección superior no serán aplicadas a las cuentas que no pertenezcan al dominio Outlook, que están vinculadas o sincronizadas con una cuenta de Outlook.com. En otras palabras, las características de seguridad adicionales implementadas en Outlook.com solo protegen la propia cuenta de Outlook.com y no se extienden a otras cuentas de correo electrónico externas que se utilizan en conjunto con ella, como las mencionadas (Gmail y Yahoo Mail).

Outlook utiliza el cifrado S/MIME el cual permite enviar mensajes de manera segura y con certificación digital. Al utilizar S/MIME, puede cifrar y firmar digitalmente los correos electrónicos. Esto ofrece diversas ventajas a los destinatarios del mensaje, ya que les ayuda a:

- Asegurarse de que el mensaje que reciben es exactamente el mismo que envió el remitente.

- Verificar que el mensaje proviene específicamente del remitente y no de alguien que pretenda serlo.

Para lograr esto, S/MIME utiliza técnicas de seguridad criptográfica como autenticación, integridad del mensaje y firmas digitales para evitar el repudio del origen. Además, S/MIME mejora la confidencialidad y seguridad de la información mediante el cifrado, brindando una mayor confianza y protección en la comunicación electrónica.

A continuación, se evidencia algunas vulnerabilidades y sus recomendaciones con el fin de ser mitigadas.

CVE-2023-36895

- **Descripción:** Vulnerabilidad de ejecución remota de código de Microsoft Outlook.

- **Mitigación:** Actualización Aplicación Word 2013

CVE-2023-36893

- **Descripción:** Vulnerabilidad de falsificación de Microsoft Outlook.

- **Mitigación:** Actualización de seguridad para Microsoft Outlook 2013, archivo de actualización agosto de 2023 (KB5002449).

CVE-2023-23397

- **Descripción:** Vulnerabilidad de elevación de privilegios de Microsoft Outlook.

- **Mitigación:** actualización de seguridad para Outlook 2016: 14 de marzo de 2023 (KB5002254).

Considerando la investigación realizada, se presentan algunas recomendaciones de seguridad para los usuarios al momento de utilizar Microsoft Outlook:

- Mantener contraseñas seguras: Los usuarios deben asegurarse de tener contraseñas fuertes y únicas para su cuenta de Microsoft Outlook. Es importante evitar reutilizar password de otras cuentas y cambiarlas periódicamente para garantizar una mayor protección.

- Habilitar la autenticación en dos pasos: Se sugiere activar la autenticación en dos pasos para una mayor protección de la cuenta de Microsoft Outlook. Esto requerirá una segunda forma de comprobación, como un código

enviado al dispositivo móvil del usuario, además del password, para iniciar sesión.

- Tener cuidado con archivos adjuntos y enlaces: Al recibir mensajes con archivos adjuntos o enlaces en Outlook.com, se recomienda tener precaución y evitar abrir aquellos que parezcan sospechosos o provengan de remitentes desconocidos, esto ayudará a prevenir riesgos de virus y software malicioso.

- Utilizar el cifrado S/MIME: Aquellos usuarios que valoren una mayor seguridad en la comunicación electrónica pueden considerar utilizar el cifrado S/MIME para enviar mensajes de manera segura y con certificación digital.

- Mantener actualizada la aplicación: Es importante que los usuarios se aseguren de tener la versión más reciente de Microsoft Outlook y cualquier complemento que utilicen, ya que las actualizaciones suelen incluir mejoras de seguridad y corrección de vulnerabilidades.

- Evitar compartir contraseñas y datos confidenciales: Se aconseja a los usuarios que no compartan su contraseña ni otros datos confidenciales por correo electrónico, ya que esto podría comprometer la seguridad de su cuenta y la privacidad de sus comunicaciones.

- Revisar las configuraciones de privacidad: Se sugiere revisar y ajustar las configuraciones de privacidad en la cuenta de Microsoft Outlook para garantizar que la información sensible esté protegida y solo sea accesible por las personas autorizadas.

- Es de vital importancia generar conciencia sobre el phishing y capacitar a los usuarios en las estrategias empleadas para suplantar identidades en el entorno digital. Se recomienda que los clientes aprendan a reconocer emails sospechosos que podrían ser fraudulentos. Es aconsejable abstenerse de ejecutar enlaces y archivos adjuntos de los emails no solicitados o que parezcan extraños para evitar caer en posibles trampas o estafas.

5.1.4 Google Workspace: en cuanto a las herramientas de Gmail y Google Meet: Gmail, es un servicio de correo electrónico ofrecido por Google, ampliamente conocido y utilizado a nivel mundial. Ha adquirido un destacado rol como una de las principales soluciones para la comunicación a través de internet, con una enorme base de usuarios que se cuentan por millones. La plataforma de Gmail proporciona una experiencia de correo electrónico fácil de usar y versátil, que combina una interfaz sencilla con una variedad de características avanzadas y útiles.

Una de las características más destacadas de Gmail es su amplio almacenamiento, ofreciendo el almacenamiento en grandes volúmenes de correos electrónicos y archivos adjuntos en su cuenta. La búsqueda inteligente de Gmail facilita la localización de correos electrónicos específicos mediante el uso de algoritmos de clasificación y etiquetado automático. Asimismo, la integración con otras aplicaciones de Google, como Google Drive, Google Meet y Google Calendar, optimizando la productividad y la colaboración.

La seguridad es una prioridad en Gmail, y se ofrecen diversas herramientas para proteger las cuentas de los usuarios. Entre ellas se incluyen la autenticación en dos pasos, la detección de spam y el filtrado de mensajes sospechosos. Además, Gmail utiliza una avanzada tecnología de detección de ataques mediante técnicas de ingeniería social para ayudar a los usuarios a evitar ataques de suplantación de identidad.

Gmail también destaca por su capacidad de organización, gracias a las etiquetas y las categorías que permiten clasificar los mensajes de forma eficiente. Los usuarios pueden personalizar su experiencia con temas, extensiones y la opción de crear múltiples bandejas de entrada. La capacidad de acceder a Gmail desde diversos dispositivos, como computadoras, tabletas y teléfonos inteligentes, garantiza una experiencia de correo electrónico sin problemas y altamente accesible en cualquier momento y lugar. En resumen, Google Gmail es una herramienta de comunicación esencial, que combina funcionalidad, seguridad y eficiencia con el fin de complacer las exigencias actuales.

Ahora bien, en cuanto a la protección y seguridad en línea, mediante el uso de encriptación, Google garantiza un alto nivel de seguridad y privacidad a sus clientes. Cuando se envían correos electrónicos, videos, visitas a sitios web o se almacenan fotos, los datos viajan entre dispositivos, los servicios de Google y los centros de datos; protegiendo la información mediante múltiples capas de seguridad, incluyendo las mejores prácticas de encriptación como es la aplicación de HTTPS y seguridad en la capa de transporte.

Respecto de las alertas de seguridad, Google genera notificaciones si detecta actividades sospechosas que puedan afectar al usuario, como intentos de acceso no autorizados, sitios web, aplicaciones o archivos maliciosos. Además, brinda orientación para reforzar las medidas de seguridad. Por ejemplo, Gmail advierte antes de la descarga de un archivo adjunto que pueda significar peligro para la seguridad, o si alguien intenta acceder a la cuenta desde un dispositivo desconocido. Si identifica actividad sospechosa, recibirá una notificación en el teléfono o en la bandeja de entrada para que pueda proteger la cuenta con un solo clic.

También, Google realiza bloqueo de anuncios fraudulentos; los anuncios que contienen software malicioso promocionan productos falsos o violan las políticas publicitarias, pueden afectar la experiencia en línea y poner en riesgo la seguridad. Debido a lo anterior Google Aborda este problema de manera seria y efectiva. Cada año, Se genera el bloqueo de miles de millones de anuncios fraudulentos (aproximadamente 100 por segundo) utilizando una combinación de revisión en tiempo real y software de bloqueo avanzado. También proporciona herramientas para denunciar anuncios ofensivos y controlar los tipos de publicidad. El objetivo principal se resume en hacer de Internet un sitio más confiable.

Por otro lado, la aplicación de Google Meet, se encuentra en el mercado como herramienta apropiada para que las organizaciones puedan interactuar a distancia, pues ofrece servicios de videollamadas, así como chats; igual que las demás plataformas a las que se ha hecho referencia en la presente investigación. Utiliza los protocolos de seguridad de TLS Y SRTP, igual que las aplicaciones anteriormente referidas; esta es una aplicación que puede ser usada sin necesidad de la instalación de complementos adicionales, se puede acceder a ella desde cualquier navegador de internet; sin embargo, debe tenerse en cuenta que se requiere de una cuenta Google activa para acceder a los servicios.

Las reuniones se crean a partir de una invitación en conexión con Google Calendar y cuentan con un código que se compone de 25 caracteres que es difícil de descifrar; lo que permite que solamente usuarios externos que cuentan con la invitación puedan acceder a la reunión; así mismo el organizador podrá silenciar y quitar participantes, también conceder permisos a los asistentes para que la reunión sea grabada. Las grabaciones de reuniones y archivos compartidos entre los usuarios son propiedad del cliente, en ningún momento Google tiene injerencia sobre ellos.

Además de lo anteriormente indicado Google Meet cuenta con un cifrado adicional denominado CPC; “este método de cifrado utiliza las claves de cifrado de la

empresa para cifrar los streams de vídeo y audio de Meet en el navegador del cliente antes de que se transmitan a otros participantes de la reunión o a Google"[31]; lo que permite un mayor nivel de seguridad sobre los datos de las compañías. También cuenta con una capa de seguridad agregada, la cual se refiere al factor de doble autenticación a partir de contraseñas con códigos que se usan una sola vez para el acceso, estos códigos se comparten al usuario de manera personal a su teléfono celular mediante mensaje de texto o llamada telefónica.
Finalmente, debe hacerse referencia a una falencia de la aplicación, en la cual el cifrado de los datos puede ser descifrado o desencriptado; situación que se presenta en el caso en el que la conexión a una reunión se haga desde un dispositivo móvil; pues este usara la conexión a internet proporcionada por el proveedor de telefonía celular, la cual no cuenta con los mismos protocolos de seguridad de la aplicación.

A continuación, se evidencia algunas vulnerabilidades para estas dos herramientas de Google Workspace y sus recomendaciones con el fin de ser mitigadas.

CVE-2022-20270

- **Descripción:** Dentro del apartado de Contenido, se presenta una oportunidad factible para descubrir la identificación de la cuenta de Gmail configurada en el dispositivo. Esta posibilidad emerge debido a un descuido en la gestión de permisos, lo que podría resultar en la revelación de datos almacenados localmente sin requerir permisos extra de ejecución. Lo notable es que no se precisa de la participación del usuario para llevar a cabo esta manipulación. Este hallazgo se aplica al sistema operativo Android, específicamente en las versiones anteriores a Android-13, y está registrado bajo el identificador de problema A-209005023.

[31] GOOGLE MEET security & privacy for admins - Google Workspace Admin Help [Anónimo]. Google Help [página web]. [Consultado el 27, julio, 2023]. Disponible en Internet: https://support.google.com/a/answer/7582940?sjid=9778274602957846483-NA#top&safety&privacy&encryption&counterabuse&secure&incident&&zippy=,privacidad-y-cumplimiento,cifrado,medidas-contra-el-uso-inadecuado,implementación-acceso-y-controles-seguros,gestión-de-incidentes,prácticas-recomendadas-de-seguridad

- **Mitigación:** Realizar actualización a la última versión Android 13.

CVE-2020-24904

- **Descripción:** Se descubrió un problema en el parámetro adjunto en GNOME Gmail versión 2.5.4, que permite a los atacantes remotos obtener información confidencial a través del enlace "mailto" manipulado.

- **Mitigación:** Realizar actualización a la versión Chrome estable más reciente.

CVE-2019-8932

- **Descripción:** Redbrick Shift hasta 3.4.3 permite a un atacante extraer tokens de autenticación de servicios (como Gmail, Outlook, etc.) utilizados en la aplicación.

- **Mitigación:** Realizar actualización parche Redbrick Shift 3.4.4.

Considerando la investigación, se presentan algunas recomendaciones de seguridad para los usuarios al momento de utilizar Gmail y Google Meet como herramientas principales de Workspace:

- Garantizar la seguridad de la cuenta de Google: Dado que es necesario tener cuenta de Google con el fin de ingresar a las herramientas del Google Workspace, es fundamental asegurarse de mantener la cuenta protegida mediante una contraseña sólida y activar la autenticación en dos pasos para añadir una capa adicional de seguridad.

- Utilizar Google Calendar para crear reuniones: Las reuniones se pueden crear en Google Meet a través de Google Calendar y compartir las invitaciones solo con las personas que necesitan participar en la reunión.

- Compartir el código de reunión con cuidado: El código de reunión de 25 caracteres es una medida de seguridad importante. Se debe compartir el

código solo con los invitados autorizados y evitar hacerlo público o enviarlo a personas no autorizadas.

- Gestionar los permisos de los participantes: Como organizador, es necesario revisar y controlar los permisos de los participantes en la reunión. Se debe conceder acceso solo a las personas necesarias y limitar la capacidad de silenciar o eliminar a otros participantes a personas de confianza.

- Conocer los derechos sobre grabaciones y archivos: Es importante tener en cuenta que las grabaciones de reuniones y archivos compartidos son propiedad del cliente, lo que significa que Google no tiene acceso a ellos. Sin embargo, es importante informar a los participantes sobre las grabaciones y obtener su consentimiento si es necesario.

- Estar alerta ante el cifrado en los teléfonos móviles: Es crucial tener presente que el cifrado de los datos puede ser menos seguro cuando los participantes se conectan a una reunión desde un dispositivo móvil utilizando la conexión de datos del proveedor de telefonía celular.

- Utilizar conexiones seguras: Para obtener un mayor nivel de seguridad, se recomienda usar conexiones seguras, preferiblemente a través de redes Wi-Fi privadas y seguras. Es recomendable evitar ingresar a las reuniones desde los teléfonos conectados a redes públicas o proveedores de telefonía celular que puedan no estar tan protegidos.

- Se aconseja mantener actualizado el sistema operativo y cualquier software de seguridad utilizado en el móvil para resguardarlo de posibles vulnerabilidades.

- Educar a los participantes sobre la seguridad: Se recomienda informar a los participantes sobre las mejores prácticas de seguridad al utilizar Google Workspace, especialmente en entornos empresariales donde la confidencialidad de la información es crítica.

- Salir de las reuniones cuando no sean necesarias: Al finalizar una reunión o cuando ya no se necesita estar presente, se debe asegurar cerrar la sesión en Google Meet para evitar accesos no autorizados.

- Es importante que los usuarios estén vigilantes ante mensajes que puedan resultar sospechosos, mostrando cautela al visualizar emails de fuentes desconocidas o que generen dudas. Se sugiere evitar hacer clic en enlaces o descargar archivos adjuntos de correos que parezcan extraños o que no hayan sido solicitados previamente.

- Se sugiere aprovechar las herramientas de seguridad adicionales que ofrece Google, como el bloqueo de anuncios fraudulentos, para garantizar una experiencia en línea más segura.

- En caso de manejar información altamente sensible, se sugiere considerar el uso del cifrado de extremo a extremo al enviar mensajes o archivos adjuntos para preservar la confidencialidad de la información.

5.1.4 TeamViewer: es una herramienta de acceso remoto y soporte que permite a los usuarios conectarse a un ordenador desde cualquier lugar del mundo a través de Internet. A continuación, Se detallan ciertas atribuciones o cualidades de seguridad informática implementadas en esta herramienta:

Autenticación de dos factores: TeamViewer integra una autenticación de dos factores que añade una capa extra segura al inicio de sesión. Esta autenticación envía un código de acceso único al dispositivo del usuario a través de SMS o de una aplicación de autenticación.

Cifrado de extremo a extremo: TeamViewer encripta todas las conexiones de extremo a extremo con AES-256 y RSA 2048, que son algoritmos criptográficos seguros y robustos que ofrecen protección contra la mayoría de los ataques.

Control de acceso a través de roles: Con TeamViewer, es posible definir qué usuarios tienen acceso a determinados recursos y funciones de la herramienta. Los administradores pueden establecer diferentes perfiles de roles, con diferentes permisos para las funciones de la herramienta.

Control de acceso basado en políticas: TeamViewer tiene una característica de control de acceso basado en políticas que permite a los usuarios definir qué acciones pueden realizar otros usuarios en el dispositivo de destino durante una sesión de control remoto. Los usuarios pueden limitar acciones específicas, tales como transferir archivos, o prohibir el acceso a ciertas partes del sistema.

Registro de auditoría: TeamViewer mantiene un registro completo de todas las conexiones, inicios de sesión y desconexiones de los usuarios. Esto permite una mayor transparencia y responsabilidad por cualquier acción que ocurra durante las sesiones remotas.

A continuación, se evidencia algunas vulnerabilidades para TeamViewer y sus recomendaciones con el fin de ser mitigadas.

CVE-2023-0837

- **Descripción:** Una verificación de autorización incorrecta de la configuración del dispositivo local en TeamViewer Remote entre la versión 15.41 y 15.42.7 para Windows y macOS permite que un usuario sin privilegios cambie la configuración básica del dispositivo local, aunque las opciones estén bloqueadas. Esto puede resultar en cambios no deseados en la configuración.

- **Mitigación:** Actualizar a la última versión (15.42.8 o superior)

CVE-2022-23242

- **Descripción:** Las versiones de TeamViewer Linux anteriores a la 15.28 no ejecutan correctamente un comando de eliminación para la contraseña de conexión en caso de que se bloquee el proceso. El conocimiento del evento de bloqueo y la ID de TeamViewer, así como la posesión de la contraseña de conexión previa al bloqueo o el acceso autenticado local a la máquina habrían permitido establecer una conexión remota al reutilizar la contraseña de conexión no eliminada correctamente.

- **Mitigación:** Actualizar a la última versión (15.28 o superior)

CVE-2021-35005

- **Descripción:** TeamViewer anterior a 14.7.48644 en Windows carga archivos DLL que no son de confianza en ciertas situaciones.

- **Mitigación:** Instalar parche de seguridad v9.0.259145.

A continuación, se proporciona una explicación de las recomendaciones de seguridad para tener en cuenta:

- Se propone hacer obligatoria la activación de la autenticación de doble factor para todos los usuarios, con el fin de garantizar que ningún acceso sea efectuado sin la incorporación de esta capa adicional de seguridad.

- Se aconseja fomentar el uso de aplicaciones de autenticación como Google Authenticator en lugar de depender únicamente de mensajes de texto, ya que se consideran más seguras que los SMS.

La encriptación sólida de extremo a extremo asegura la confidencialidad de las comunicaciones. Con el propósito de optimizar esta característica:

- Se sugiere mantener actualizados tanto el cliente como el servidor con las versiones más recientes, con el objetivo de parchear posibles vulnerabilidades conocidas.

- Se recomienda establecer contraseñas sólidas y únicas tanto para la cuenta en TeamViewer como para las conexiones remotas.

El control basado en roles resulta esencial para restringir el acceso a ciertos recursos y funciones:

- Se insta a asignar roles y permisos de acuerdo con las responsabilidades específicas de cada usuario, evitando otorgar excesivos privilegios para minimizar el riesgo de abuso.
- Se aconseja llevar a cabo revisiones periódicas de los roles y permisos asignados para asegurarse de que sigan siendo pertinentes, retirando el acceso a aquellos usuarios que ya no lo necesiten.

La función de control de acceso basado en políticas brinda un manejo detallado de las acciones permitidas durante sesiones de control remoto:

- Se recomienda establecer pautas coherentes y claras para el control remoto, por ejemplo, restringiendo la transferencia de archivos únicamente a situaciones específicas y limitando el acceso a áreas sensibles.

- Se sugiere que, cuando sea posible, las sesiones de control remoto se inicien con permisos limitados y se solicite autorización explícita para acciones críticas.

El registro de auditoría asegura la transparencia y responsabilidad. Es importante:

- Se aconseja llevar a cabo supervisiones periódicas de los registros de conexiones y actividades en busca de comportamientos inusuales o sospechosos.

- Ante la detección de actividades sospechosas en los registros, se sugiere investigar y tomar las medidas apropiadas, tales como revocar el acceso o cambiar las contraseñas.

5.1.5 Red privada virtual (VPN): Es una herramienta indispensable para llevar a cabo labores remotas y asegurarse en línea. Permite a los usuarios establecer conexiones seguras y cifradas a través de Internet, simulando una conexión directa a una red local. A continuación, se examinan y explican diversas características de seguridad informática implementadas en las VPN:

Encriptación de Datos: Un aspecto fundamental de las VPN es su capacidad para cifrar los datos. Cualquier intercambio de información entre el dispositivo del usuario y el servidor de la VPN se convierte en un formato seguro a través del cifrado, garantizando que todos los datos transmitidos, ya sean archivos, correos electrónicos o contraseñas, se mantengan protegidos de accesos no autorizados. Los métodos comunes de cifrado incluyen técnicas seguras como AES (Estándar de Cifrado Avanzado) y otros procedimientos criptográficos confiables.

Ocultamiento de Dirección IP: Una VPN disimula la dirección IP original del usuario y la reemplaza con la dirección IP del servidor VPN. Esto contribuye a preservar el anonimato en línea, ya que sitios web y servicios en línea solo detectarán la dirección IP del servidor VPN, complicando la tarea de identificar y rastrear al usuario.

Protección en Redes Wireless Públicas: Las VPN resultan especialmente beneficiosas al conectarse a una red Wireless publica dado que estas redes suelen ser menos seguras y propensas a ataques. La VPN codifica los datos transmitidos, minimizando el riesgo de que terceros intercepten información confidencial.

Sorteo de la Censura y Restricciones Geográficas: A través de la ocultación de la dirección IP y el direccionamiento del tráfico a través de servidores ubicados en diversas partes del mundo, las VPN permiten a los usuarios eludir restricciones geográficas y la censura impuesta por gobiernos o proveedores de servicios.

Cortafuegos de Aplicación: Algunas VPN ofrecen cortafuegos de aplicación que bloquean el tráfico no deseado o malicioso. Esto puede ayudar a proteger contra ataques de malware y virus.

Políticas de No Registro (No-logs): Algunas VPN hacen hincapié en políticas de no registro, lo que implica que no guardan registros de las actividades de navegación de sus usuarios. Esto añade una capa extra de privacidad, ya que no hay información que compartir con terceros incluso si se solicita.

Protocolos de Seguridad: Las VPN presentan diversos protocolos de seguridad para establecer conexiones, como OpenVPN, L2TP/IPsec, entre otros. Cada protocolo presenta sus propias fortalezas y limitaciones en lo que respecta a la seguridad y la velocidad.

- **Autenticación de Usuarios:** Para acceder a una VPN, los usuarios generalmente deben autenticarse mediante credenciales como nombre y contraseña. Algunas VPN también ofrecen autenticación multifactor con el fin de incrementar la seguridad.

A continuación, se evidencia algunas vulnerabilidades para una red privada virtual (VPN) y sus recomendaciones con el fin de ser mitigadas.

CVE-2023-37849

- **Descripción:** Una vulnerabilidad de secuestro de DLL en Panda Security VPN para Windows anterior a la versión v15.14.8 permite a los atacantes ejecutar código arbitrario colocando un archivo DLL manipulado en el mismo directorio que PANDAVPN.exe.

- **Mitigación:** Realizar actualización a la versión v15.14.8.

CVE-2023-20178

- **Descripción:** Una vulnerabilidad en el proceso de actualización del cliente de Cisco AnyConnect Secure Mobility Client Software para Windows y Cisco Secure Client Software para Windows, podría permitir que un atacante local autenticado y con pocos privilegios eleve los privilegios a los de SYSTEM. El proceso de actualización del cliente se ejecuta después de establecer una conexión VPN exitosa. Esta vulnerabilidad existe porque se asignan permisos inadecuados a un directorio temporal que se crea durante el proceso de actualización. Un atacante podría aprovechar esta vulnerabilidad abusando de una función específica del proceso de instalación de Windows. Una explotación exitosa podría permitir que el atacante ejecute código con privilegios de SISTEMA.

- **Mitigación:** Realizar actualización parche de seguridad sugerida por el fabricante.

CVE-2022-20933

- **Descripción:** Una debilidad en el sistema del servidor Cisco AnyConnect VPN en los dispositivos Cisco Meraki MX y Cisco Meraki Z3 Teleworker Gateway podría dar la posibilidad a un atacante externo sin autorización de causar una situación en la que el servicio quede inaccesible, conocida como denegación de servicio (DoS), en un dispositivo afectado. Esta debilidad surge debido a que no se realiza una validación suficiente de los datos ingresados por el cliente al establecer una conexión VPN SSL. Un atacante podría aprovechar esta vulnerabilidad al crear una petición maliciosa y enviarla al dispositivo en cuestión. Si la acción es exitosa, el

atacante podría provocar que el servidor Cisco AnyConnect VPN se detenga y reinicie, lo que resultaría en la interrupción de las conexiones SSL VPN activas, forzando a los usuarios remotos a restablecer y autenticar de nuevo sus conexiones VPN.

- **Mitigación:** Cisco Meraki recomienda que los administradores actualicen los dispositivos a una versión de software más reciente.

A continuación, se presentan algunas pautas de seguridad cibernética en relación con la utilización de una Red Privada Virtual (VPN):

- Se recomienda optar por una VPN de confianza y con una sólida reputación en el mercado. Se aconseja realizar una investigación exhaustiva de las alternativas disponibles y seleccionar una que tenga un historial destacado en términos de seguridad y privacidad.

- Es aconsejable verificar que la VPN implemente una sólida encriptación, como AES, para proteger los datos durante su transferencia. Se sugiere evitar las VPN que no especifiquen claramente los métodos de encriptación que emplean.

- Se resalta la importancia de seleccionar una VPN que aplique una política confiable de no registrar (no-logs). Esto significa que no se conservan registros de las actividades en línea del usuario, reduciendo así la posibilidad de compartir datos con terceros.

- Se recomienda activar la autenticación de doble factor si la VPN ofrece esta función. Se remarca que esto añade una capa extra de seguridad al requerir una solicitud extra al momento de generar autenticación, además de los password de inicio de sesión.

- Se aconseja emplear herramientas en línea para comprobar si la VPN está filtrando la dirección IP o los datos de DNS. De esta manera, se garantiza que la dirección IP real permanezca oculta y no se revele por accidente.

- Se destaca la importancia de ejercer precaución con las VPN gratuitas, ya que pueden tener limitaciones en seguridad y potencialmente monetizar los

datos del usuario. Se aconseja investigar detenidamente la política de privacidad y los términos de servicio antes de optar por una VPN gratuita.

- Se subraya la necesidad de mantener prácticas seguras en línea, como evitar hacer clic en enlaces sospechosos y utilizar contraseñas sólidas y únicas, incluso al contar con una VPN que brinde seguridad adicional.

- Siguiendo estas pautas, se recalca que los usuarios pueden aprovechar al máximo los beneficios de seguridad ofrecidos por una Red Privada Virtual (VPN) y mantener sus actividades en línea más resguardadas y privadas.

5.1.6 Protocolo de Escritorio Remoto (RDP): es una herramienta de trabajo a distancia creada por Microsoft que posibilita a los usuarios conectarse a otros dispositivos o servidores a través de Internet o una red interna. A continuación, se examinan y detallan algunas de las características de seguridad informática implementadas en el RDP:

Autenticación: El RDP incorpora autenticación de dos factores (2FA) para fortalecer la seguridad en el proceso de inicio de sesión. Esto agrega un segundo nivel de autenticación después de ingresar las credenciales iniciales, generalmente un código enviado al teléfono o a una aplicación de autenticación.

Cifrado de Datos: El RDP emplea encriptación de datos para salvaguardar la información transmitida entre el dispositivo local y el dispositivo remoto. El cifrado se basa en el estándar de seguridad TLS (Transport Layer Security) para garantizar que los datos no sean captados durante su transmisión.

Configuración de Niveles de Acceso: Los administradores pueden definir y controlar los niveles de acceso de los usuarios al sistema remoto. Esto permite restringir las capacidades de los usuarios según sus roles y responsabilidades, reduciendo el riesgo de exposición de información crítica.

Autenticación de Redirección de Dispositivos: El RDP permite la redirección de dispositivos periféricos, como impresoras y unidades flash USB. Sin embargo, estos dispositivos también deben autenticarse antes de ser redirigidos, lo que impide la posibilidad de introducir malware en la máquina remota a través de dispositivos infectados.

Protección contra Ataques de Fuerza Bruta: El RDP implementa medidas de seguridad para prevenir estos ataques, en los que se intenta adivinar contraseñas mediante una serie de combinaciones. Después de un número definido de intentos fallidos, el RDP puede bloquear temporalmente la cuenta o aumentar los intervalos entre los intentos.

Registro de Eventos: El RDP mantiene un registro exhaustivo de los eventos de conexión y desconexión, lo que asiste a los administradores en el seguimiento de quién accedió, cuándo y desde dónde. Esto resulta esencial para mantener la visibilidad y la responsabilidad respecto a las acciones ejecutadas en sesiones remotas.

Directivas de Grupo: Microsoft proporciona herramientas para administrar el RDP mediante las Directivas de Grupo. Esto permite a los administradores definir configuraciones de seguridad específicas y aplicarlas de forma centralizada a un conjunto de dispositivos.

Actualizaciones y Parches: Microsoft publica regularmente parches de seguridad y actualizaciones para abordar vulnerabilidades conocidas en el protocolo RDP y en sus componentes. Mantener el software actualizado es esencial para garantizar la seguridad y protección.

A continuación, se evidencia algunas vulnerabilidades para un Protocolo de Escritorio Remoto (RDP) y sus recomendaciones con el fin de ser mitigadas.

CVE-2022-23613

- **Descripción:** xrdp es un servidor de protocolo de escritorio remoto (RDP) de código abierto. En las versiones afectadas, un subdesbordamiento de enteros que conduce a un desbordamiento de pila en el servidor sesman permite que cualquier atacante no autenticado que pueda acceder localmente a un servidor sesman ejecute código como root. Esta vulnerabilidad ha sido parcheada en la versión 0.9.18.1 y superior. Se recomienda a los usuarios que actualicen.

- **Mitigación:** Realizar Parcheado en las versiones 0.9.18.1 o 0.9.19 y superiores

CVE-2022-23493

- **Descripción:** xrdp es un proyecto de código abierto que proporciona un inicio de sesión gráfico para máquinas remotas mediante el protocolo de escritorio remoto (RDP) de Microsoft. xrdp < v0.9.21 contiene una lectura fuera de límites en la función xrdp_mm_trans_process_drdynvc_channel_close().

- **Mitigación:** No hay soluciones alternativas conocidas para este problema. Se recomienda a los usuarios que actualicen.

CVE-2023-30576

- **Descripción:** Apache Guacamole 0.9.10 a 1.5.1 puede continuar haciendo referencia a un búfer de entrada de audio RDP liberado. Dependiendo del momento, esto puede permitir que un atacante ejecute código arbitrario con los privilegios del proceso guacd.

- **Mitigación:** Los usuarios de versiones de Apache Guacamole 1.5.1 y anteriores deben actualizar a la versión 1.5.2.

A continuación, se proporciona una explicación de las recomendaciones de seguridad para tener en cuenta:

- Refuerzo de la Autenticación: Se puede beneficiar de la característica de autenticación de doble factor (2FA) disponible en el RDP. Esta función agrega una capa extra de seguridad durante el inicio de sesión, requiriendo una verificación extra, como un código enviado al teléfono o a una aplicación de autenticación.
- Establecimiento de Niveles de Acceso: Los administradores tienen la capacidad de definir y supervisar los niveles de acceso asignados a los usuarios. Esta práctica permite ajustar las capacidades según los roles y responsabilidades, reduciendo así el riesgo de exponer información crítica.

- Autenticación de Dispositivos Redirigidos: Si se habilita la redirección de dispositivos periféricos, como impresoras o unidades USB, es crucial

asegurarse de que estos también sean autenticados antes de ser redirigidos. Esto evita la posibilidad de introducir malware en el sistema remoto a través de dispositivos infectados.

- Prevención de Ataques de Fuerza Bruta: El RDP incorpora varias medidas de seguridad. En caso de varios intentos sin éxito de inicio de sesión, el sistema puede bloquear temporalmente la cuenta o aumentar los intervalos entre intentos como medida preventiva.

- Registro Detallado de Eventos: Se resalta la utilidad del registro exhaustivo de eventos de conexión y desconexión ofrecido por el RDP. Esta característica resulta valiosa para rastrear las acciones de los usuarios, manteniendo la transparencia y responsabilidad en las sesiones remotas.

- Gestión Mediante Directivas de Grupo: Los usuarios tienen la opción de administrar la configuración de seguridad del RDP de manera centralizada a través de las Directivas de Grupo proporcionadas por Microsoft. Esto facilita la aplicación uniforme de políticas específicas en un conjunto de dispositivos.

- Mantenimiento de Actualizaciones: Es esencial mantener el software al día. Microsoft regularmente lanza parches de seguridad y actualizaciones para abordar vulnerabilidades conocidas en el protocolo RDP y sus componentes, asegurando la integridad y protección del sistema.

5.1.7 AnyDesk: una herramienta ampliamente utilizada para el trabajo a distancia brinda a los usuarios la capacidad de acceder y gestionar dispositivos de manera remota. A continuación, se describen algunas características de seguridad informática incorporadas en AnyDesk:

Cifrado de Datos: AnyDesk emplea cifrado de extremo a extremo para salvaguardar la información transmitida entre el dispositivo local y el dispositivo remoto. Durante la negociación, utiliza un cifrado RSA de 2048 bits, mientras que, durante la transmisión de datos, se apoya en el cifrado AES de 256 bits. Esto garantiza que los datos estén salvaguardados contra intentos de intercepción.
Autenticación y Autorización: AnyDesk exige que los usuarios autentiquen su acceso mediante un ID y una contraseña únicos para cada sesión. Además, los usuarios tienen la capacidad de permitir o denegar el acceso remoto a través de

un cuadro de diálogo emergente en el dispositivo remoto. Esto añade un nivel extra de autorización.

Registro de Sesiones y Control de Acceso: AnyDesk proporciona un registro detallado de las sesiones remotas, incluyendo información sobre quién se conectó y cuándo. Asimismo, los usuarios pueden asignar contraseñas específicas para las conexiones entrantes y configurar permisos de acceso.
Protección de Privacidad: Esta herramienta exhibe notificaciones visuales en el dispositivo remoto cuando se establece una sesión, permitiendo a los usuarios mantener el control sobre las conexiones remotas y prevenir sesiones no autorizadas sin su conocimiento.

Acceso en Modo Solo Visualización: AnyDesk concede a los usuarios la opción de seleccionar distintos niveles de acceso durante una sesión remota. Pueden optar por un control completo o simplemente visualización, lo que posibilita a los usuarios mantener el control sobre las acciones ejecutadas en su dispositivo durante la conexión remota.

Restricción de Acceso por Dirección IP: AnyDesk autoriza a los usuarios a establecer restricciones de acceso basadas en direcciones IP específicas. Esto implica que solamente las direcciones IP autorizadas pueden conectarse al dispositivo remoto.

Actualizaciones de Seguridad: AnyDesk lanza de forma periódica actualizaciones de seguridad para abordar vulnerabilidades y mejorar la seguridad general del software. Mantener AnyDesk actualizado es esencial para asegurar la seguridad de las sesiones remotas.

A continuación, se evidencia algunas vulnerabilidades para AnyDesk y sus recomendaciones con el fin de ser mitigadas.

CVE-2022-32450

- **Descripción:** AnyDesk 7.0.9 permite que un usuario local alcance privilegios de SISTEMA a través de un enlace simbólico porque el usuario puede escribir en su propia carpeta %APPDATA% (utilizada para ad.trace y chat), pero el producto se ejecuta como SISTEMA cuando escribe datos de la sala de chat allí.

- **Mitigación:** Se sugiere realizar actualización del producto.

CVE-2021-44426

- **Descripción:** Se descubrió un problema en AnyDesk antes de 6.2.6 y 6.3.x antes de 6.3.5. Es posible cargar un archivo arbitrario en el directorio local ~/Downloads/ de la víctima si la víctima está utilizando el cliente Windows de AnyDesk para conectarse a una máquina remota, si un atacante también está conectado de forma remota con AnyDesk a la misma máquina remota. La carga se realiza sin ninguna aprobación o acción por parte de la víctima, pero el producto se ejecuta como SISTEMA cuando escribe datos de la sala de chat allí.

- **Mitigación:** Se sugiere realizar actualización a la versión 6.2.6

CVE-2021-44425

- **Descripción:** Se descubrió un problema en AnyDesk antes de 6.2.6 y 6.3.x antes de 6.3.3. Un puerto de escucha innecesariamente abierto en una máquina en la LAN de un atacante, abierto por el cliente Windows de Anydesk cuando usa la función de tunelización, permite al atacante el acceso no autorizado a la pila de protocolos de tunelización de AnyDesk de la máquina local (y también a cualquier software de máquina de destino remoto que está escuchando el puerto tunelizado de AnyDesk).

- **Mitigación:** Se sugiere realizar actualización a la versión 6.2.6.

A continuación, se genera una seria de recomendaciones al momento de utilizar la herramienta descrita:

- En relación con la autenticación y la autorización, se sugiere emplear un proceso adecuado de autenticación al iniciar sesiones en AnyDesk. Esto involucra el uso de identificadores únicos (IDs) y contraseñas exclusivas para cada sesión, además de la capacidad de gestionar permisos mediante notificaciones emergentes en el dispositivo remoto. Esta práctica añade una capa extra de seguridad al proceso de autorización.

- AnyDesk ofrece características como el registro de sesiones y el control de acceso, que permiten un seguimiento minucioso de las conexiones remotas. Al configurar contraseñas específicas para las conexiones entrantes y establecer permisos de acceso según las necesidades, se contribuye a un mayor control sobre las sesiones.

- Con el objetivo de preservar la privacidad, AnyDesk proporciona notificaciones visuales en el dispositivo remoto al iniciar sesiones remotas. Estas notificaciones empoderan a los usuarios al mantener el control y la visibilidad de las conexiones, previniendo sesiones no autorizadas y asegurando la privacidad.

- En AnyDesk, se ofrece la posibilidad de un control de acceso selectivo, lo que permite a los usuarios optar por un control total o solo visualización durante las sesiones remotas. Esto les brinda la capacidad de mantener el control sobre las acciones realizadas en su dispositivo durante la conexión remota, adaptando el nivel de acceso según sea necesario.

- Para añadir una capa adicional de seguridad, AnyDesk facilita la restricción de acceso basada en direcciones IP. Esto significa que únicamente se permiten conexiones desde direcciones IP específicas, lo que refuerza la seguridad al limitar el acceso a dispositivos remotos autorizados.

La evaluación de las herramientas de trabajo remoto realizadas líneas arriba, resulta elemental con el propósito de hacer efectiva la seguridad de los datos en las empresas del sector retail que han implementado el trabajo remoto. El reconocimiento de los puntos sólidos y los puntos que representan flaqueza de cada herramienta igual que la generación de recomendaciones para su uso adecuado permitirá a las empresas tomar decisiones informadas y mejorar la seguridad de sus datos en el trabajo remoto.

En general, cada una de estas herramientas de trabajo remoto tiene sus propias fortalezas y debilidades en términos de seguridad. Es importante elegir la herramienta adecuada para una tarea específica, considerando los requisitos de seguridad específicos de la organización y las necesidades de los usuarios. De manera general, todas las herramientas de trabajo remoto mencionadas ofrecen medidas de seguridad que ayudan a garantizar la protección de la información confidencial de la organización y de los usuarios. Cada herramienta tiene sus

propias características de seguridad y es importante evaluarlas cuidadosamente para determinar cuál es la mejor opción para una tarea específica.

Además, es importante destacar que la seguridad no debe ser el único factor para considerar al elegir una herramienta de trabajo remoto. La usabilidad, la compatibilidad con diferentes dispositivos y sistemas operativos, y la disponibilidad de características específicas para la tarea también son importantes. Por lo tanto, se debe hacer un equilibrio entre la seguridad y la facilidad de uso al elegir la herramienta de trabajo remoto adecuada.

A continuación, en la tabla 1, se presenta un resumen comparativo sobre las características de las herramientas más usadas en el trabajo remoto.

Tabla 1. Comparativo de las herramientas de trabajo remoto.

Herramienta	Característica de seguridad	Tipo de cifrado	Recomendaciones principales de seguridad
Zoom	Encriptación de extremo a extremo	AES-256	▪ Utilizar contraseñas seguras para las reuniones • Mantener las actualizaciones de Zoom instaladas • Evitar compartir información confidencial en las reuniones
Microsoft Teams	Cifrado de datos en reposo y en tránsito	AES-256	▪ Utilizar contraseñas seguras para las cuentas de Microsoft ▪ Mantener las actualizaciones de Microsoft Teams instaladas ▪ Evitar compartir información confidencial en las conversaciones
Microsoft Outlook	Cifrado de correo electrónico	TLS 1.2 o superior	▪ Utilizar contraseñas seguras para las cuentas de correo electrónico ▪ Mantener las actualizaciones de Microsoft Outlook instaladas ▪ Evitar abrir archivos adjuntos de remitentes desconocidos

Google Workspace	Cifrado de datos en reposo y en tránsito	AES-256	▪ Utilizar contraseñas seguras para las cuentas de Google ▪ Mantener las actualizaciones de Google Workspace instaladas ▪ Evitar compartir información confidencial en las aplicaciones de Google
TeamViewer	Encriptación de extremo a extremo	AES-256	▪ Utilizar contraseñas seguras para las sesiones ▪ Mantener las actualizaciones de TeamViewer instaladas ▪ Evitar compartir información confidencial en las sesiones
VPN	Encriptación de datos en tránsito	AES-256, 3DES, RSA	▪ Utilizar una contraseña segura para la VPN ▪ Mantener la VPN actualizada ▪ Evitar utilizar la VPN en redes públicas inseguras
RDP	Encriptación de datos en tránsito	AES-256, 3DES	▪ Utilizar una contraseña segura para el escritorio remoto ▪ Mantener RDP actualizado ▪ Evitar utilizar RDP en redes públicas inseguras
AnyDesk	Encriptación de extremo a extremo	AES-256	▪ Utilizar una contraseña segura para las sesiones ▪ Mantener AnyDesk actualizado ▪ Evitar compartir información confidencial en las sesiones

Fuente: Elaboración propia.

5.2 IDENTIFICAR LAS TÉCNICAS MÁS USADAS DE INGENIERÍA SOCIAL DESCRIBIENDO SU MODO DE OPERACIÓN EVIDENCIANDO QUE EL MAYOR FACTOR DETONANTE ES LA FALTA DE CONOCIMIENTO POR PARTE DEL USUARIO.

Para iniciar, se define la ingeniería social como “un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados. Además, los hackers pueden tratar de aprovecharse de la falta de conocimiento de un usuario; debido a la velocidad a la que avanza la tecnología, numerosos consumidores y trabajadores no son conscientes del valor real de los

datos personales y no saben con certeza cuál es la mejor manera de proteger esta información."[32]

Así las cosas, los delincuentes aplican la ingeniería social en búsqueda de vulnerar la seguridad personal y empresarial a partir de la suplantación de software, sitios web e información. Esta investigación se centrará especialmente en la ingeniería social aplicada a las empresas del sector retail, es decir, la obtención de información o datos sensibles de este tipo de empresas, pues llama la atención que son ataques que se caracterizan por ser fáciles de realizar con un elevado porcentaje de efectividad lo que se traduce en un resultado bastante lucrativo.

La ingeniería social tiene dos formas de aplicación; la primera, se refiere a los casos en los cuales no se requiere comunicación directa con la víctima, es el caso de las personas que espían las credenciales en espacios abiertos; y la segunda hace referencia a los ataques que si requieres de un contacto directo con la victima; estos últimos serán a los que nos referiremos en el desarrollo de este objetivo, pues la comunicación directa con la víctima se basa en generar confusión, la inducción a error y la presión.

Kevin Mitnick, estadounidense considerado el hacker más famoso alrededor del mundo en estos últimos tiempos, quien fue acusado de diversos delitos cibernéticos y al mismo tiempo escritor del libro "The Art Of Deception"; se ha referido a la ingeniería social indicando que el hecho de generar confianza, enaltecer a la víctima, generar condiciones para que la víctima no pueda negarse a lo solicitado por el delincuente y despertar el instinto de colaboración en la victima; son cuatro líneas guías que deben seguirse para un ataque de ingeniería social exitoso; líneas que básicamente se basan en la persuasión.

La persuasión, es entendida como el talento que tiene un individuo a partir de un razonamiento para convencer a otro de hacer, no hacer algo, o pensar de determinada forma; en la ingeniería social la persuasión ha sido abordada por el psicólogo Robert Cialdini, en su obra Influence: the psychology of persuasion", a partir de principios.

---

[32] INGENIERÍA SOCIAL: definición [Anónimo]. latam.kaspersky.com [página web]. [Consultado el 29, julio, 2023]. Disponible en Internet: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

En la figura 8, podemos analizar los principios de la persuasión expuesto por Robert Cialdini.

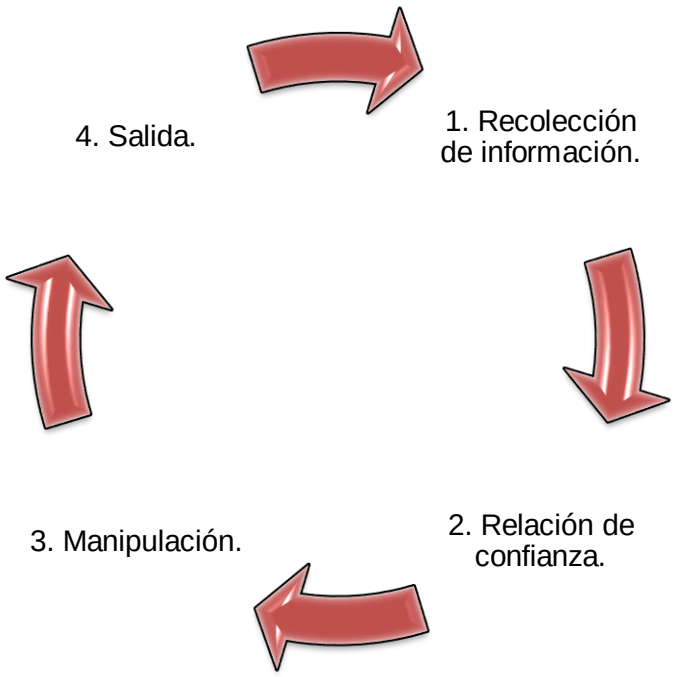
Figura 8. Persuasión

Fuente: Elaboración propia.

La mínima información sobre datos sensibles o privados de las compañías abre la puerta a un ataque de ingeniería social; en las empresas del sector retail el objetivo principal objetivo de los delincuentes será lograr obtener información de usuarios y contraseñas, pues con estas tendrían acceso libre a los sistemas.

Según se observa en la figura 9, los ataques de ingeniería social se componen de las siguientes fases:

Figura 9. Fases ataques ingeniería social



Fuente: Elaboración propia.

En la fase número uno, recolección de información, el ciber atacante sustrae información general de la víctima; sin darse cuenta, es esta misma quien entrega sus datos; una vez el delincuente tiene información de la víctima crea una situación de atracción para esta, lo que le permite desarrollar una relación de confianza, desde esta relación de confianza, el delincuente inicia su ataque buscando que la víctima haga lo que este quiere, a esta fase se le conoce como manipulación y una vez conseguido el objetivo sale de la escena sin dejar rastro, con el objetivo conseguido.

A continuación se estudiarán las vías utilizadas por los ciberdelincuentes para realizar ataques de ingeniería social; como insumo principal del cual se valen los atacantes para acceder de manera sencilla a la víctima y conseguir su objetivo; si bien es cierto parecen inofensivas es importante concientizar a los usuarios que estas vías contienen herramientas que facilitan las operaciones pero que tienen que usarse con cuidado, cautela y en observancia al detalle, pues siempre hay personas maliciosas esperando que el usuario peque en el sentido de exceso de confianza para aprovecharse con fines delictivos.

En la figura 10, se pueden evidenciar las vías más utilizadas por los delincuentes para llevar a cabo ataques de ingeniería social

Figura 10. Vías más utilizadas para ejecutar ataques de ingeniería social.

.

Fuente: Elaboración propia.

Una vez estudiadas las vías para generar ataques de ingeniería social, resulta importante llevar a cabo un estudio detallado de las técnicas de ingeniería social más utilizadas, pues estas resultan siendo las metodologías en donde los delincuentes emplean las vías de ataque. A continuación, se describirá su modo de operación, evidenciando la influencia significativa de la falta de conocimiento por parte del usuario como el factor detonante principal de su éxito.

Para lograr el objetivo general de identificar las técnicas más usadas de ingeniería social y su relación con la falta de conocimiento del usuario, se realizó una

exhaustiva investigación y análisis de diversos recursos académicos, estudios de caso y fuentes especializadas en seguridad informática.

En el marco de este análisis, se identificaron y catalogaron las técnicas más comunes y ampliamente empleadas por los ciberdelincuentes en sus ataques de ingeniería social, las siguientes:

5.2.1. PHISHING.

Esta técnica ocupa el primer lugar de las más usadas por los ciberdelincuentes para atacar empresas del sector retail; pues "se trata del envió de un mail con el fin de instar a la víctima a que por medio de un link o un formulario envíe datos personales o corporativos; (suplantación de identidad)."[33]

Esta técnica de ingeniería social se clasifica en dos tipos, el primero según el servicio objetivo del ataque y el segundo sobre el modus operandi

El phishing se basa en el vector de ataque de internet mediante correo electrónico, de tal manera que el agresor buscara la suplantación de compañías importantes valiéndose de los principios de persuasión de la escasez y la reciprocidad; de tal manera que el atacante envía un correo electrónico en donde ofrece premios, oportunidades únicas, realiza un ofrecimiento sobre bienes y servicios sobre los cuales la víctima no se negaría a adquirir o se refiere a información extremadamente llamativa y alarmante, que para ser consultada deberá de hacer clic en algún enlace que permita que el atacante efectué su objetivo, es decir acceder a la información sensible de la víctima.

A continuación se puede evidenciar un caso de phishing vía correo electrónico; allí supuestamente el Banco Davivienda, le indica al cliente que ha solicitado un cambio del número celular asociado a la cuenta Daviplata y le invita en el caso de no ser directamente el cliente quien hubiera solicitado el cambio a contactarse con un asesor a través de un link para cancelar la solicitud; allí la victima por lo

---

[33] ANÁLISIS DE las Técnicas más Usadas en la Ingeniería Social [Anónimo]. Universidad Piloto de Colombia [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: http://repository.unipiloto.edu.co/handle/20.500.12277/12497

alarmante del mensaje procederá ingresar al link por el que entregara su información sensible permitiendo que el ciberdelincuente tenga un ataque de phishing exitoso.

La figura 11, es un ejemplo de ataque de ingeniería social mediante la técnica del phishing.

Figura 11. Ejemplo ataque phishing

Fuente: Elaboración propia.

En la figura 12, se evidencia la creación de un ataque de phishing en donde el agresor suplanta una página web de una entidad o comercio reconocido, en este caso se crea una URL muy similar a la de la página web original, que será enviada por un correo electrónico a la víctima que contendrá un link que lo direccionara a una página falsa en donde se solicitara el ingreso de datos de credenciales, contraseñas y otros.

En la 12 figura, hace una exposición de los pasos que sigue un delincuente para crear un ataque de phishing.

Figura 12. Creación de un ataque phishing

Fuente: http://repository.unipiloto.edu.co/handle/20.500.12277/12497

5.2.2 SMISHING

Diversos autores que abordan las técnicas de ingeniería social relacionan el Smishing como una técnica derivada del phishing dadas sus similitudes; sin embargo, este se define como "un fraude que se ejecuta a través de mensajes de texto o apps de mensajería tales como WhatsApp. En esta técnica, los estafadores suplantan la identidad de una persona, empresa o entidad financiera para manipular a los usuarios y motivarlos a hacer clic en enlaces peligrosos"[34]

El objetivo de esta técnica de ingeniería social es instalar un malware a través de una URL o link malintencionado enviada vía mensaje de texto fraudulento, para que controle el dispositivo móvil, de tal manera que se le permita al

[34] ANÁLISIS DE las Técnicas más Usadas en la Ingeniería Social [Anónimo]. Universidad Piloto de Colombia [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: http://repository.unipiloto.edu.co/handle/20.500.12277/12497

ciberdelincuente acceder a la información almacenada en el dispositivo. A continuación, se observa la figura de un ataque de Smishing.

La figura 13, hace una exposición de los pasos que sigue un delincuente para crear un ataque de Smishing.

Figura 13. Creación ataque Smishing

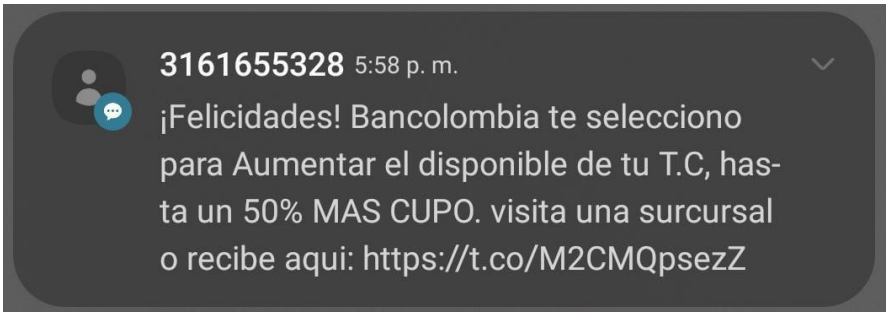
Fuente: https://dialnet.unirioja.es/descarga/articulo/6255067.pdf

La principal diferencia entre el Smishing y el phishing, radica en la vía de ataque pues el Smishing se configura mediante teléfono; de tal manera que los vectores de ataque para esta técnica son; en primer lugar, mensajes de textos engañosos y en algunos casos alarmantes, en donde por lo general se suplanta la identidad de una entidad financiera y se informa a la víctima sobre movimientos extraños en productos financieros, adicionalmente el mensaje incluye un link al que el individuo objeto del ataque deberá comunicarse, cuando este hace clic al link o se comunica vía telefónica al número suministrado el delincuente se infiltra obteniendo la información sensible objetivo del ataque.

Enseguida, se observa una figura ejemplo de un ataque de Smishing vía mensaje de texto que contiene la inclusión de una URL maliciosa con la que se busca el robo de información; pues en este caso en particular, la victima ni siquiera es titular de productos financieros en la entidad Bancolombia.

La figura 14, es un ejemplo de ataque de ingeniería social mediante la técnica del Smishing.

Figura 14. Ejemplo ataque Smishing



Fuente: Elaboración propia.

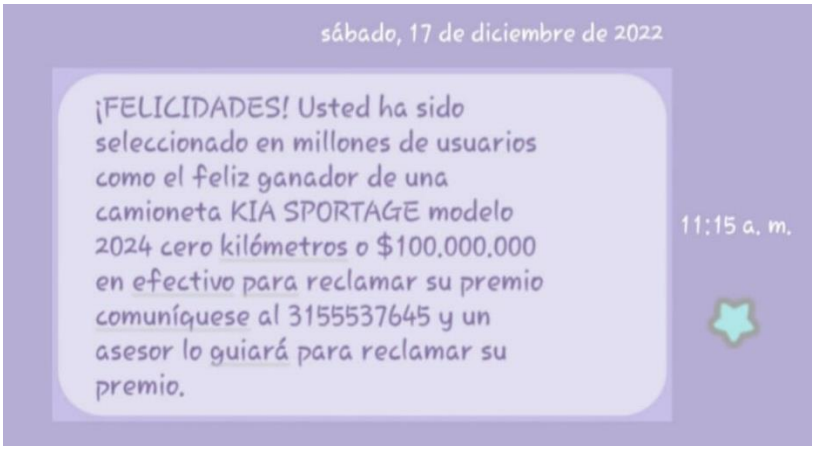
En el segundo vector de ataque, se tiene en igual sentido al anterior, la ofensiva del ciberdelincuente inicia con él envió de un mensaje de texto, pero en esta oportunidad, incluirá un número de teléfono al cual la victima deberá comunicarse.

En estos casos, el atacante se vale primordialmente del principio de persuasión de la reciprocidad, pues ofrece algo bastante llamativo a la víctima a cambio de que se comunique al teléfono indicado y durante esta comunicación pueda extraer la información objeto del ataque.

Ahora, se observa el ejemplo de un ataque de ingeniería social con la técnica Smishing incluyendo un número de teléfono para que la víctima se comunique. Se puede observar que como atractivo el delincuente ofrece un vehículo tipo camioneta, 0 kilómetros o una considerable suma de dinero en efectivo; lo que podría despertar en la victima un alto grado de fascinación, haciendo que caiga en la trampa, realice la llamada que será contestada por el delincuente quien a lo largo de la comunicación será simpático y usara sus dotes persuasivos logrando que la víctima entregue la información deseada.

La figura 14, es un ejemplo de ataque de ingeniería social mediante la técnica del Smishing, en el que se solicita comunicación a un número telefónico.

Figura 15. un ejemplo de ataque de ingeniería social mediante la técnica del Smishing.



Fuente: Elaboración propia.

Esta técnica ha adquirido una considerable relevancia para ser usada, sobre todo en las empresas del sector retail, pues con el avance tecnológico de los últimos años, sumado a la implementación de formas de trabajo como el trabajo remoto; hoy en día resulta más común que las funciones de ciertos empleados se desarrollen desde dispositivos móviles, lo que representa un riesgo considerable para que las compañías sean objeto de ataques de ingeniería social a través del Smishing.

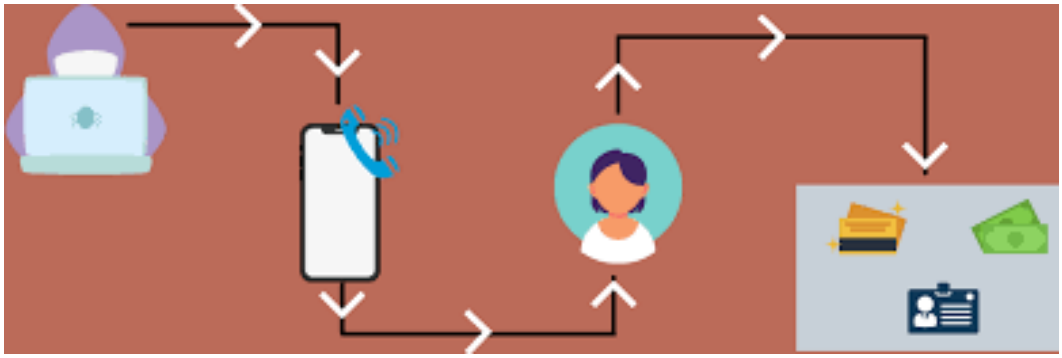
5.2.3. VISHING

Este tipo de ataque de ingeniería social es conexo al phishing; pues el Vishing según diversos autores “surge de la unión entre voice + phishing o más conocido como suplantar voz o telefonía, este se basa en el aprovechamiento de VOIP

donde se brinda un número telefónico falso, aparentando ser el verdadero y conseguir datos sensibles"[35]

En la figura 16, se puede evidenciar el ciclo de un ataque de Vishing.

Figura 16. Pasos que sigue un delincuente para crear un ataque de Vishing.



Fuente: https://geekflare.com/es/vishing-attack-prevention/

En un ataque mediante la técnica de Vishing, la victima recibe una llamada, en donde el atacante suplanta la identidad de alguna entidad o comercio reconocido generando credibilidad y confianza en la víctima, la llamada se origina con cualquier excusa o tema de conversación, en donde el atacante se muestra simpático, así como carismático, logrando persuadir a la víctima hasta lograr el objetivo de conseguir datos sensibles.

El Vishing se compone de dos vectores de ataque: (i) el ciberdelincuente realiza la llamada telefónica, una vez se establece la comunicación se reproduce una grabación que contiene información alarmante y sugiere que a fin de corroborar lo dicho en la grabación se comunique con un número telefónico, (ii) el ciberdelincuente se comunica telefónicamente vía llamada de manera directa con la víctima; por lo general en este vector el atacante se muestra afectuoso, cordial y atrayente, suplantando la identidad de un colaborador del área de servicio al

[35] Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 1, agosto, 2023]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/28152/%20jaime.sedano.pdf?sequence=1&isAllowed=y

cliente de alguna entidad o compañía de reconocimiento; a lo largo de la llamada se establece una relación de confianza por lo que al atacante inicia una serie de preguntas que conllevan a que victima entregue su información confidencial.

En los dos escenarios indicados en el párrafo anterior el atacante crea la trampa a través de la comunicación de voz, sea por la llamada que regresa la víctima o la que contesta está directamente y es mediante este contacto que se configurara el éxito del ataque con la entrega de información.

5.2.4. PHARMING

Finalmente, entre las técnicas de ingeniería social más usadas encontramos el Pharming, el cual, se relaciona también estrechamente con el phishing; sin embargo este se reviste de mayor complejidad pues consiste en “la suplantación de portales web, la diferencia radica en que es mucho más difícil detectar el portal falso ya que no necesitan que el usuario interactúe con algún correo malicioso, su complejidad radica en que el atacante modifica el sistema de resolución de nombres en dominio (DNS) y conduce al usuario a una página web falsa aunque este digite la verdadera de manera correcta en la barra de direcciones”.

Este tipo de ataque también es distinguido con el nombre de "Resolución de Nombres de Dominio; es producida en el momento que se ingresa la dirección de un sitio web por ejemplo www.jaimesedanop.com esta URL es traducida a dirección IP (Internet Protocol) ej. 200.21.200.16 este procedimiento lo realiza los famosos DNS (Servidor de Nombre de Dominio)."[36]

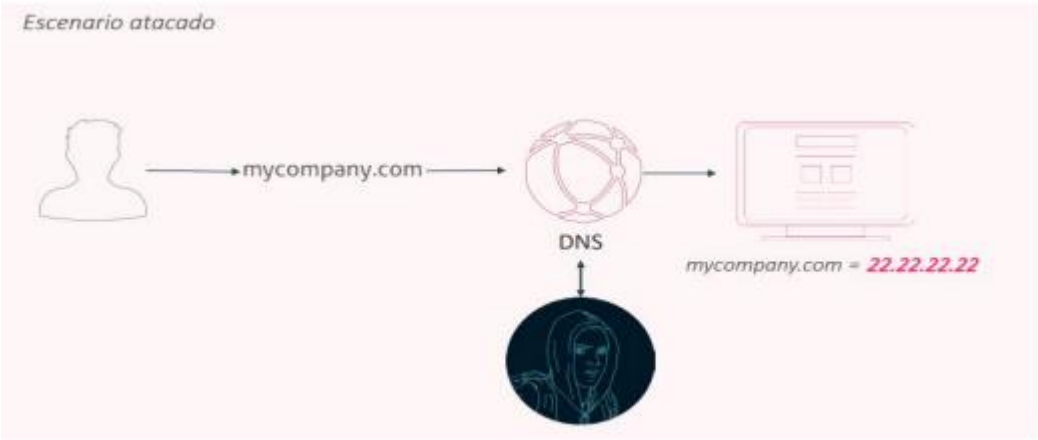
Paso seguido, se indica el proceso de desarrollo de un ataque de pharming, allí se observa como la victima intenta acceder a una página web legitima y es en ese momento cuando el atacante ayudado de un código o software malicioso realiza cambios en la DNS, direccionando a la víctima a una página web ilegitima de casi iguales características que la original.

---

[36] Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 1, agosto, 2023]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/28152/%20jaime.sedano.pdf?sequence=1&isAllowed=y

En la figura 16, se puede evidenciar el paso a paso realizado por el delincuente para implantar un ataque de pharming.

Figura 17. Pasos que sigue un delincuente para crear un ataque de pharming.



Fuente:https://repository.unad.edu.co/bitstream/handle/10596/28152/%20jaime.sedano.pdf?sequence=1&isAllowed=y

En el Pharming, se maneja un único vector de ataque, el cual será las DNS, pues el objetivo del ciberdelincuente es el manejo engañoso de estas con objetivos fraudulentos.

Como se ha visto, cada una de las técnicas de ingeniería social fue detalladamente analizada, describiendo su modus operandi y los pasos que los atacantes suelen seguir para engañar a las víctimas y obtener acceso no autorizado a sistemas y datos sensibles. Entre las técnicas destacadas en primer lugar se encuentra el phishing, seguido del Vishing; en las cuales, se resalta el uso de pretextos, la manipulación emocional.

En el análisis se evidenció claramente que uno de los factores más determinantes en el éxito de las técnicas de ingeniería social es la falta de conocimiento por parte de los usuarios. Esta carencia de conciencia y comprensión de los riesgos de seguridad informática hace que los usuarios sean más susceptibles a caer en trampas y ser manipulados por los atacantes. Los usuarios suelen ser engañados al proporcionar información confidencial, hacer clic en enlaces maliciosos o abrir archivos adjuntos infectados, todo esto como resultado de una falta de conocimiento sobre las tácticas y estrategias utilizadas por los ciberdelincuentes.

Además, se analizaron diversos casos de estudio y ejemplos reales donde se puede evidenciar que la falta de conocimiento por parte de los usuarios es objeto de explotación perpetrar ataques exitosos de ingeniería social. Estos casos ilustran claramente cómo la falta de conciencia de los usuarios puede poner en riesgo la seguridad de sistemas y datos sensibles, impactando negativamente en organizaciones del sector retail.

Como conclusión de este análisis, se resalta la importancia de la educación y la concientización en seguridad informática. Es fundamental que los usuarios adquieran un mayor conocimiento sobre las técnicas de ingeniería social, los riesgos asociados y las medidas preventivas que se pueden implementar.

Así mismo, se recomienda a las organizaciones y entidades responsables de la seguridad informática que implementen programas de capacitación y concientización para sus empleados y usuarios, con el fin de reducir la efectividad de las técnicas de ingeniería social y fortalecer la seguridad de sus sistemas y datos.

5.3 PROPONER A LAS EMPRESAS DEL SECTOR RETAIL CON MODALIDAD DE TRABAJO REMOTO ACCIONES CORRECTIVAS Y PREVENTIVAS CON EL FIN DE REDUCIR O MITIGAR EL RIESGO DE UN ATAQUE DE INGENIERÍA SOCIAL MEDIANTE LAS TECNICAS DE PHISHING, SMISHING, VISHING Y PHARMING.

El phishing es una técnica comúnmente utilizada, especialmente en entornos de trabajo remoto donde los empleados pueden ser más vulnerables a ciertos enfoques de manipulación. Para disminuir o prevenir el peligro de que ocurra un ataque basado en la manipulación psicológica en el sector retail y en situaciones de trabajo a distancia, es posible llevar a cabo una serie de medidas correctivas y preventivas que las empresas pueden adoptar:

- Concienciación y formación del personal: Realizar sesiones periódicas de concienciación y formación sobre ciberseguridad, incluyendo específicamente la identificación de técnicas de ingeniería social y phishing. Los empleados deben ser educados sobre cómo detectar correos electrónicos y mensajes sospechosos, enlaces maliciosos y otras tácticas comunes utilizadas por los atacantes.

- Políticas de seguridad claras: Implementar y comunicar políticas de seguridad sólidas para el trabajo remoto. Esto puede incluir directrices específicas sobre cómo manejar correos electrónicos no solicitados o mensajes de fuentes desconocidas, así como el uso adecuado de dispositivos personales para el trabajo.

- Verificación de identidad: Siempre que se realicen solicitudes de información confidencial o cambios en la información de la cuenta, es esencial implementar procedimientos rigurosos para verificar la identidad del solicitante. Esto puede incluir llamadas telefónicas adicionales a números de contacto previamente registrados o utilizar métodos de autenticación multifactor (MFA).

- Empleo de sistemas de filtrado avanzado: Instaurar soluciones de filtrado tanto para correos electrónicos como para el tráfico web, con el fin de bloquear mensajes de correo y enlaces maliciosos que son reconocidos como amenazas. Estas herramientas son efectivas para evitar que mensajes de phishing ingresen a los buzones de los clientes.

- Mantener al día las actualizaciones y correcciones: Es esencial mantener todos los sistemas y programas actualizados con los últimos parches de seguridad para evitar que los atacantes aprovechen vulnerabilidades conocidas.

- Supervisión de cuentas y comportamiento del usuario: Implementar un monitoreo constante de actividades sospechosas en las cuentas de los empleados. Detectar cualquier comportamiento inusual, como múltiples intenciones de inicio de sesión o intentos de acceso desde ubicaciones inusuales.

- Establecer una medida de seguridad sólida: Aplicar la autenticación de dos factores (2FA) o autenticación multifactor (MFA) en todas las plataformas y cuentas que se empleen para acceder a datos importantes o confidenciales.

- Políticas de trabajo remoto seguras: Establecer políticas claras para el trabajo remoto, que incluyan el uso de redes privadas virtuales (VPN) seguras y la protección de dispositivos personales utilizados para el trabajo con contraseñas sólidas y cifrado de datos.

- Pruebas de simulación de phishing: Realizar pruebas periódicas de simulación de phishing con el fin de simular la resistencia del personal a los ataques de ingeniería social y proporcionar retroalimentación y capacitación adicional según sea necesario.

- Canales de comunicación seguros: Establecer canales de comunicación interna seguros para que los empleados puedan reportar correos electrónicos o mensajes sospechosos sin temor a represalias.

Para reducir o mitigar el riesgo de un ataque de Vishing en el sector retail y en entornos de trabajo remoto, se pueden implementar las siguientes acciones correctivas y preventivas:

- Capacitación y concienciación: Realizar programas de formación específicos sobre Vishing para los empleados del sector retail que trabajan de forma remota. Educar a los empleados sobre las tácticas de ingeniería

social utilizadas en los ataques de Vishing y cómo reconocer y responder adecuadamente a las llamadas sospechosas.

- Políticas de seguridad claras: Establecer políticas claras para el manejo de información confidencial y solicitudes telefónicas. Hay que asegurar que los empleados comprendan que nunca deben revelar información sensible, como password, información de tarjetas o datos confidenciales a través de llamadas telefónicas no verificadas.

- Verificación de identidad: Implementar procedimientos rigurosos de verificación de identidad antes de divulgar información confidencial o realizar acciones críticas. Si un empleado recibe una llamada solicitando información sensible, debe verificar la identidad del interlocutor antes de proporcionar cualquier dato.

- Limitar la divulgación de información sensible: Minimizar la cantidad de información confidencial que se comparte por teléfono. Alentar a los empleados a evitar proporcionar detalles personales o financieros a menos que se sigan los procedimientos de verificación establecidos.

- Restricción de acceso remoto: Limitar el acceso a sistemas críticos y datos sensibles desde ubicaciones externas mediante una autenticación fuerte y soluciones de acceso seguro, como VPN y autenticación multifactor.

- Monitoreo de actividades sospechosas: Implementar un sistema de monitoreo que detecte actividades inusuales o llamadas telefónicas sospechosas. Si se detecta algún patrón o intento de ataque, se deben tomar medidas inmediatas para investigar y responder adecuadamente.

- Establecer canales de comunicación seguros: Proporcionar a los empleados una línea de comunicación segura donde puedan reportar posibles intentos de Vishing o cualquier actividad sospechosa.

- Mantenimiento de seguridad al día: Es fundamental mantener los sistemas, aplicaciones y herramientas utilizadas para el trabajo a distancia actualizados, asegurándose de instalar regularmente las últimas versiones y parches de seguridad disponibles.

- Pruebas de simulación de Vishing: Realizar pruebas de simulación de Vishing de manera periódica para evaluar la resistencia del personal frente a este tipo de ataques y proporcionar capacitación adicional si es necesario.

- Políticas de comunicación externa: Establecer reglas claras sobre la información que se puede compartir públicamente, para evitar que los atacantes utilicen datos disponibles en fuentes públicas para realizar ataques de Vishing más efectivos.

Con el objetivo de disminuir o evitar el riesgo de que ocurra un ataque de Pharming en el ámbito del comercio retail y en situaciones de trabajo a distancia, se proponen diversas medidas correctivas y preventivas que las empresas pueden aplicar:

- Seguridad en la infraestructura de DNS: Asegurarse de que la infraestructura de DNS de la empresa sea segura y esté correctamente configurada. Utilizar servidores DNS confiables y mantenerlos actualizados con las últimas correcciones de seguridad.

- Aplicar DNSSEC: Lo cual ofrece una extensión del DNS que brinda autenticación y asegurar la información en el sistema de nombres de dominio. Implementar DNSSEC puede ser de gran ayuda para evitar ataques de Pharming.

- Uso de HTTPS y certificados SSL: Asegurarse de que el sitio en internet de la empresa utilice HTTPS con certificados SSL/TLS válidos. Esto garantiza que la información se transmita de forma segura entre el usuario y el servidor, y evita ataques de intermediarios maliciosos.

- Mantenerse actualizado con las últimas actualizaciones y parches: Es esencial mantener todos los sistemas y software al día, aplicando las últimas correcciones de seguridad disponibles, con el propósito de prevenir vulnerabilidades conocidas que los atacantes podrían utilizar en su beneficio.

- Capacitación y concienciación del personal: Proporcionar a los empleados información sobre el Pharming y otros tipos de ataques de ingeniería social, de modo que puedan identificar señales de peligro y evitar caer en trampas. Hay que destacar la trascendencia de comprobar la autenticidad de los sitios web antes de compartir información confidencial.

- Políticas de seguridad claras: Establecer políticas claras sobre cómo manejar información confidencial, especialmente cuando se recopila o comparte a través de sitios web. Fomentar la verificación de la identidad del sitio y proporcionar información solo a través de canales seguros.

- VPN y conexiones seguras: Alentar el uso de VPN para todas las conexiones remotas a la red de la empresa. Esto ayuda a proteger la comunicación y los datos de los empleados mientras están fuera de la oficina.

- Supervisión y detección de actividad sospechosa: Implementar sistemas de monitoreo que puedan detectar actividades inusuales o intentos de manipulación de DNS. Esto permitirá una respuesta rápida en caso de un ataque de Pharming.

- Respaldos y recuperación de datos: Realizar copias de seguridad regulares de datos importantes para poder restaurarlos en caso de que se vean comprometidos durante un ataque de Pharming.

- Evaluación de proveedores y terceros: Verificar la seguridad de los proveedores y terceros con acceso a sistemas o información confidencial para evitar riesgos potenciales de Pharming.

Para reducir o evitar el riesgo de ser afectado por un ataque de Smishing en el sector retail y en entornos de trabajo remoto, se proponen diversas acciones correctivas y preventivas que las empresas pueden implementar para mantenerse protegidas:

- Concienciación y formación del personal: Realizar programas de concienciación y formación sobre ciberseguridad, específicamente enfocados en el Smishing. Educar a los empleados sobre cómo detectar

mensajes de texto sospechosos, identificar enlaces maliciosos y reportar actividades sospechosas.

- Políticas de seguridad claras: Establecer políticas claras para manejar mensajes de texto no solicitados y solicitudes de información confidencial. Los empleados deben estar capacitados para no compartir información sensible a través de mensajes de texto sin verificar la autenticidad de la solicitud.

- Verificación de remitentes: Alentar a los empleados a verificar el remitente de los mensajes de texto antes de responder o hacer clic en cualquier enlace. Desconfiar de mensajes de texto no solicitados o de fuentes desconocidas.

- Restricción de información sensible: Minimizar la cantidad de información sensible que se comparte a través de mensajes de texto. No proporcionar password, información bancaria u otra información personal a través de este canal.

- Uso de autenticación multifactor (MFA): Implementar la autenticación multifactor en todas las cuentas y sistemas utilizados para el trabajo remoto. Esto añadirá una capa extra de seguridad en caso de que los atacantes intenten robar credenciales mediante Smishing.

- Actualizaciones y parches: Mantener todos los dispositivos móviles y aplicaciones actualizados con los últimos parches de seguridad para prevenir vulnerabilidades conocidas.

- Filtrado de mensajes de texto: Utilizar soluciones de filtrado de mensajes de texto para bloquear mensajes de texto sospechosos o de fuentes no confiables.

- Política de comunicación segura: Establecer una política clara sobre la comunicación segura de información confidencial y alentar a los empleados a utilizar canales seguros para compartir información sensible.

- Supervisión y detección de actividad sospechosa: Implementar sistemas de monitoreo para detectar actividades inusuales o patrones de mensajes de texto sospechosos.

- Pruebas de simulación de Smishing: Realizar pruebas de simulación de Smishing de manera periódica para evaluar la resistencia del personal ante este tipo de ataques y proporcionar capacitación adicional si es necesario.

6. CONCLUSIONES

Conforme avanza la investigación, se van revelando distintos métodos de ingeniería social que históricamente se han basado en el estudio de diversas fuentes bibliográficas. Estos métodos empiezan por adquirir conocimiento sobre el tema y la terminología relacionada, seguido de un análisis detallado. Estos pasos permiten llevar a cabo un ataque y revelar la vulnerabilidad de una persona ante factores como la influencia y la ignorancia. Muchas de las tecnologías actuales tienen sus raíces en tecnologías antiguas desarrolladas en años anteriores.

La formación de los usuarios a menudo se descuida porque se cree erróneamente que el uso de software avanzado es suficiente para evitar los ciberataques. Sin embargo, debido a que los avances tecnológicos y los ciberdelincuentes están en constante evolución, es imprescindible realizar un entrenamiento continuo, sin olvidar lo ocurrido en ataques previos, ya que muchos métodos existentes derivan de otros ya conocidos y nuevas estrategias para tener éxito.

Es relevante destacar que, a lo largo del tiempo, los métodos de ingeniería social han evolucionado, volviéndose cada vez más sofisticados en su intento de engañar a los usuarios y obtener acceso a información confidencial. Teniendo en cuenta lo anterior, es importante que las empresas del sector retail estén al tanto de las últimas técnicas de ingeniería social y se preparen para enfrentarlas.

En la mayoría de los casos, los ataques de ingeniería social se basan en aprovechar la falta de conocimiento de los usuarios. Los ciberdelincuentes se valen de la ignorancia o exceso de confianza de los usuarios para extraer información o acceso no autorizado a sistemas y datos. Por eso, es fundamental capacitar a los usuarios para prevenir este tipo de ataques. Los empleados deben recibir formación para reconocer y reportar posibles ataques, así como para proteger la información confidencial y cumplir con las políticas de seguridad de la empresa.

Es relevante destacar que la seguridad cibernética no es solo un asunto tecnológico, sino que también está intrínsecamente relacionada con la cultura organizacional. En el sector retail, las empresas deben fomentar una cultura de seguridad cibernética en la que todos los usuarios entiendan el valor de salvaguardar la información y estén dispuestos a implementar medidas para asegurar la seguridad de los sistemas y datos de la empresa.

Es esencial que las empresas del sector retail implementen medidas adecuadas de seguridad cibernética para protegerse contra los ataques de ingeniería social. Estas medidas pueden incluir la adopción de soluciones avanzadas de seguridad, como el monitoreo de redes y la detección de intrusiones, así como la actualización regular de software y sistemas para protegerse contra nuevas amenazas.

De ahí que se concluye, que las compañías que operan en el sector retail deben tomar precauciones y acciones correctivas para reducir el riesgo de ser afectadas por ataques de ingeniería social en el ambiente de trabajo remoto. Para lograrlo, es esencial capacitar a los empleados sobre las amenazas de seguridad y establecer políticas sólidas para proteger la información. También se deben salvaguardar los dispositivos utilizados por los empleados, implementar sistemas seguros de autenticación y monitorear regularmente las actividades en línea de los trabajadores remotos.

La seguridad física de los dispositivos también es relevante, y es importante contar con un plan de respuesta en caso de que ocurra un ataque de ingeniería social. Para prevenir daños, es necesario realizar evaluaciones periódicas de seguridad cibernética para identificar vulnerabilidades y tomar acciones preventivas.

La seguridad cibernética no es exclusiva del departamento de TI y seguridad, sino que es responsabilidad de todos los empleados. Por ende, se debe promover una cultura de seguridad en la organización, donde todos estén informados y capacitados para detectar y prevenir ataques de ingeniería social.

Para enfrentar futuras amenazas, las empresas deben estar preparadas para adaptarse y mejorar continuamente sus medidas de seguridad cibernética. Así mismo, la implementación de políticas claras para acceder a información confidencial pueda disminuir el riesgo de que los atacantes la obtengan.

Realizar pruebas de penetración y simulaciones de ataques de ingeniería social es beneficioso para descubrir posibles debilidades y corregirlas antes de que sean aprovechadas. Contratar expertos en seguridad cibernética también puede mejorar la protección en entornos de trabajo remoto.

Un antivirus es una herramienta determinante para salvaguardar los sistemas y datos contra ataques de ingeniería social y la instalación de software malicioso, como virus, gusanos, troyanos y ransomware. Estas técnicas suelen propagarse mediante engaños en correos electrónicos o sitios web falsos. Un buen antivirus puede detectar y bloquear estas amenazas antes de que causen daño.

Los antivirus modernos ofrecen protección en tiempo real, lo que significa que monitorean constantemente el sistema en busca de comportamientos sospechosos o patrones de malware conocidos. Esto asegura una respuesta rápida ante nuevas amenazas y reduce el riesgo de infección.

Además, los antivirus incluyen funciones para bloquear el acceso a sitios web maliciosos conocidos por distribuir malware o participar en actividades de phishing. De esta manera, protegen a los usuarios de caer en trampas de ingeniería social al hacer clic en enlaces peligrosos.

Los ataques de ingeniería social suelen ocurrir a través de correos electrónicos de phishing con enlaces o archivos adjuntos maliciosos. Los antivirus pueden escanear estos correos electrónicos en busca de malware y alertar a los usuarios sobre posibles amenazas.

Los antivirus mantienen una base de datos actualizada de firmas y definiciones de malware conocidos, lo que les permite identificar y eliminar nuevas variantes de malware a medida que surgen en el panorama de amenazas.

Además, algunos antivirus utilizan técnicas avanzadas, como heurísticas y aprendizaje automático, para detectar comportamientos sospechosos en programas desconocidos. Esto ayuda a proteger contra ataques de día cero, hasta que se publiquen actualizaciones y parches de seguridad.

En resumen, la implementación de un antivirus es crítica para salvaguardar los sistemas y datos de los ataques y la instalación de malware. Ya que Detectan y previenen amenazas, protegen en tiempo real y bloquean sitios web maliciosos. Sin embargo, es importante recordar que ningún antivirus es infalible, por lo que es esencial complementar estas medidas con prácticas de seguridad y concientización del usuario.

7. RECOMENDACIONES

El aprendizaje continuo acerca de la seguridad informática, especialmente respecto a los recientes ataques de ingeniería social, puede fortalecer la protección de la información en cualquier ámbito de uso. Estas prácticas deben realizarse de manera periódica, teniendo en cuenta tanto lo ocurrido en el pasado como las posibles amenazas futuras.

Para evitar potenciales ataques de ingeniería social, como la duplicación de datos en servidores alternativos o el uso de aplicativos en la nube, es primordial ser cauteloso al acceder a sitios web seguros y evitar ignorar los certificados de seguridad, ya que esto no garantiza la protección del sitio.

Aunque ha habido numerosos ataques de ingeniería social a lo largo de la historia, la mayoría de ellos han sido resultado de la persuasión y la manipulación para lograr ejecutar con éxito el ataque. Por tanto, es importante actuar con prudencia, ser considerado e inteligente al exponer información sensible.

Además de la educación continua y la precaución al acceder a sitios seguros, existen otras medidas preventivas que las empresas pueden adoptar para reducir el riesgo de un ataque de ingeniería social. Una medida crucial es establecer políticas de seguridad sólidas que aborden los procedimientos de seguridad y las mejores prácticas para el manejo de información delicada. Estas políticas deben comunicarse de manera clara a todos los empleados y reforzarse mediante capacitaciones regulares.

También es vital implementar métodos de autenticación seguros, como la autenticación multifactorial, que requiere múltiples formas de verificar la identidad del usuario, como contraseña, token de seguridad y huella digital. Esto dificulta el acceso a información protegida por parte de atacantes malintencionados.

Además, es importante mantener una vigilancia constante sobre la red y las actividades en línea de los empleados para detectar cualquier comportamiento sospechoso. Es posible utilizar herramientas de seguimiento y análisis de seguridad para reconocer posibles riesgos y tomar medidas preventivas de forma proactiva para evitar ataques de ingeniería social.

También, las empresas del sector retail deben tomar acciones preventivas y correctivas para amortiguar el riesgo de un ataque en entornos de trabajo remoto. La educación continua, las políticas de seguridad sólidas, la autenticación segura y el monitoreo constante son algunas de las medidas recomendadas para robustecer la seguridad de la información y prevenir posibles ataques. Es fundamental tener en cuenta que los ciberdelincuentes siempre buscan nuevas formas de atacar, por lo que la prevención y el entrenamiento deben ser un esfuerzo constante y en evolución.

REFERENCIAS

ANÁLISIS DE las Técnicas más Usadas en la Ingeniería Social [Anónimo]. Universidad Piloto de Colombia [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: http://repository.unipiloto.edu.co/handle/20.500.12277/12497

BELCIC, Ivan. ¿Qué es el malware y cómo protegerse de los ataques? ¿Qué es el malware y cómo protegerse de los ataques? [página web]. (19, enero, 2023). [Consultado el 9, julio, 2023]. Disponible en Internet: https://www.avast.com/es-es/c-malware

Biblioteca Digital FCE - UBA [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1753_MussoGV.pdf

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA DEPARTAMENTO NACIONAL DE PLANEACIÓN [Anónimo]. (7, marzo, 2017). [Consultado el 20, diciembre, 2023]. Disponible en Internet: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854_Adenda1.pdf

Dialnet [página web]. [Consultado el 1, agosto, 2023]. Disponible en Internet: https://dialnet.unirioja.es/descarga/articulo/6255067.pdf

DIARIO EL DIA DE LA PLATA WWW.ELDIA.COM. Tarjetas de crédito, otro blanco para el ciberdelito. eldia.com [página web]. (3, abril, 2023). [Consultado el 9, julio, 2023]. Disponible en Internet: https://www.eldia.com/nota/2023-4-3-2-12-32-tarjetas-de-credito-otro-blanco-para-el-ciberdelito-policiales

DSpace Principal [página web]. [Consultado el 19, agosto, 2023]. Disponible en Internet: http://dspace.utb.edu.ec/bitstream/handle/49000/13062/E-UTB-FAFI-SIST-000396.pdf?sequence=1&isAllowed=y.

ENTENDER LA diferencia entre teletrabajo y trabajo remoto [Anónimo]. Noticias de Abogados, bufetes, jurisprudencia, avisos de ley, de Colombia| Asuntoslegales.com.co [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://www.asuntoslegales.com.co/consultorio/entender-la-diferencia-entreteletrabajo-y-trabajo-remoto-3114944

ESE Business School | Escuela de Negocios de la U Andes [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://www.ese.cl/ese/site/artic/20200415/asocfile/20200415123039/_3__guia_para_comunicacion_interna_en_tiempos_de_crisis.pdf

ESTAS SON las capturas de ciberataques más recientes en el país [Anónimo]. Semana.com Últimas Noticias de Colombia y el Mundo [página web]. [Consultado el 14, septiembre, 2023]. Disponible en Internet: <https://www.semana.com/nacion/articulo/estas-son-las-capturas-de-ciberataques-mas-recientes-en-el-pais/202120/>.

FORMAS de evitar los ataques de vishing [aplicaciones de bloqueo de spam] [Anónimo]. Geekflare [página web]. [Consultado el 1, agosto, 2023]. Disponible en Internet:<https://geekflare.com/es/vishing-attack-prevention/>.

GARTNER: PANDEMIA de COVID-19 impulsa al 88% de las empresas al teletrabajo | Corporate IT [Anónimo]. Corporate IT [página web]. [Consultado el 19, julio, 2023]. Disponible en Internet: https://corporateit.cl/index.php/2020/03/24/gartner-pandemia-de-covid-19-impulsa-al-88-de-las-empresas-al-teletrabajo/

GOOGLE MEET security & privacy for admins - Google Workspace Admin Help [Anónimo]. Google Help [página web]. [Consultado el 27, julio, 2023]. Disponible en Internet: https://support.google.com/a/answer/7582940?sjid=9778274602957846483-NA#top&safety&privacy&encryption&counterabuse&secure&incident&&zippy=,privacidad-y-cumplimiento,cifrado,medidas-contra-el-uso-inadecuado,implementación-acceso-y-controles-seguros,gestión-de-incidentes,prácticas-recomendadas-de-seguridad

GUIA DE seguridad para Microsoft Teams - Microsoft Teams [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. [Consultado el 26, julio, 2023]. Disponible en Internet: https://learn.microsoft.com/es-es/microsoftteams/teams-security-guide

HACKER VS Ciberdelincuente | INCIBE | INCIBE [Anónimo]. INCIBE | INCIBE [página web]. [Consultado el 9, julio, 2023]. Disponible en Internet: https://www.incibe.es/aprendeciberseguridad/hacker-vs-ciberdelincuente#:~:text=El%20ciberdelincuente%20es%20la%20persona,ingeniería%20social%20o%20el%20malware.&text=If%20playback%20doesn't%20begin%20shortly,%20try%20restarting%20your%20device.

Inicio [página web]. [Consultado el 30, julio, 2023]. Disponible en Internet: https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/abstract/215-abstract-el-uso-de-zoom-y-sus-implicaciones-para-la-seguridad-y-privacidad-recomendaciones-y-buenas-practicas/file

Inicio | MINCIT - Ministerio de Comercio, Industria y Turismo [página web]. [Consultado el 13, julio, 2023]. Disponible en Internet:

https://www.mincit.gov.co/getattachment/1c8db89b-efed-46ec-b2a1-56513399bd09/Colombia.aspx.

Institutional Repository [página web]. [Consultado el 17, julio, 2023]. Disponible en Internet: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/46386/Suarez_VLM-SD.pdf?isAllowed=y&sequence=1

International Labour Organization [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---sector/documents/publication/wcms_531116.pdf

LEY 2121 de 2021 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. [Consultado el 9, julio, 2023]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=167966

LEY 527 de 1999 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [LEY_0594_2000] [Anónimo]. SECRETARÍA GENERAL DEL SENADO [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_0594_2000.html

LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [LEY_1266_2008] [Anónimo]. SECRETARÍA GENERAL DEL SENADO [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [LEY_1336_2009] [Anónimo]. SECRETARÍA GENERAL DEL SENADO [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1336_2009.html

LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [LEY_1341_2009] [Anónimo]. SECRETARÍA GENERAL DEL SENADO [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [LEY_1581_2012] [Anónimo]. SECRETARÍA GENERAL DEL SENADO [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [LEY_1712_2014] [Anónimo]. SECRETARÍA GENERAL DEL SENADO [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009] [Anónimo]. SECRETARÍA GENERAL DEL SENADO [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

MITIGAR | Diccionario de la lengua española [Anónimo]. «Diccionario de la lengua española» - Edición del Tricentenario [página web]. [Consultado el 13, septiembre, 2023]. Disponible en Internet: https://dle.rae.es/mitigar

OJO ESTOS son los ciberdelitos que más se cometen en Colombia [Anónimo]. Semana.com Últimas Noticias de Colombia y el Mundo [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://www.semana.com/tecnologia/articulo/ojo-estos-son-los-ciberdelitos-que-mas-se-cometen-en-colombia/202127/

Pàgina inicial de UPCommons [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://upcommons.upc.edu/bitstream/handle/2117/355777/161449.pdf?sequence=1&isAllowed=y

PHISHING | INCIBE | INCIBE [Anónimo]. INCIBE | INCIBE [página web]. [Consultado el 9, julio, 2023]. Disponible en Internet: https://www.incibe.es/aprendeciberseguridad/phishing

'POR PRIMERA vez vamos a superar la barrera del 1% del PIB en inversiones en ciencia y tecnología': MinCiencias [Anónimo]. Forbes Colombia [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://forbes.co/2022/04/06/economia-y-finanzas/por-primera-vez-vamos-a-superar-la-barrera-del-1-del-pib-en-inversiones-en-ciencia-y-tecnologia-minciencias

QUÉ ES el sector retail Descubre cómo iniciarte en él con tu ecommerce [Anónimo]. Shopify [página web]. [Consultado el 9, julio, 2023]. Disponible en Internet: https://www.shopify.com/es/blog/que-es-retail#:~:text=¿Qué%20significa%20retail?,gran%20mayoría%20los%20consumidores%20finales

QUÉ ES TLS Definición, funcionamiento y diferencias con SSL y HTTPS [Anónimo]. Tutoriales Hostinger [página web]. [Consultado el 20, julio, 2023].

Disponible en Internet: <https://www.hostinger.co/tutoriales/que-es-tls#Diferencia_entre_TLS_y_SSL_y_como_saber_cual_estas_utilizando>

Repositorio de la Universidad de Fuerzas Armadas ESPE: Página de inicio [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: http://repositorio.espe.edu.ec/bitstream/21000/25916/1/T-ESPESD-003164.pdf

Repositorio Universidad Nacional [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://repositorio.unal.edu.co/bitstream/handle/unal/82270/1032430963.2021.pdf?sequence=4&isAllowed=y

REVISTA ESPACIOS | Vol. 38 (NÂº 34) AÃ±o 2017 [Anónimo]. Revista Espacios | HOME [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://www.revistaespacios.com/a17v38n34/17383406.html.

RI UMNG Principal [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://repository.unimilitar.edu.co/bitstream/handle/10654/37304/CastellanosVegaCarlosJacinto2020_Formato.pdf?sequence=1&isAllowed=y

SECURITY GUIDE for Microsoft Teams overview - Microsoft Teams [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. [Consultado el 30, julio, 2023]. Disponible en Internet: https://learn.microsoft.com/en-us/microsoftteams/teams-security-guide

SEGURIDAD AVANZADA de Outlook.com para suscriptores de Microsoft 365 - Soporte técnico de Microsoft [Anónimo]. Microsoft Support [página web]. [Consultado el 29, julio, 2023]. Disponible en Internet: https://support.microsoft.com/es-es/office/seguridad-avanzada-de-outlook-com-para-suscriptores-de-microsoft-365-882d2243-eab9-4545-a58a-b36fee4a46e2#:~:text=Todos%20los%20usuarios%20de%20Outlook,de%20los%20mensajes%20que%20recibe.

SISTEMA DE cifrado AES-256 bits, ¿es realmente tan seguro? [Anónimo]. HardZone [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: <https://hardzone.es/tutoriales/rendimiento/cifrado-aes-256-bits-como-funciona/>.

SEGURIDAD Y privacidad de Google Meet para los administradores - Ayuda de Administrador de Google Workspace [Anónimo]. Google Help [página web]. [Consultado el 30, julio, 2023]. Disponible en Internet: https://support.google.com/a/answer/7582940?hl=es#zippy=,privacidad-y-cumplimiento,cifrado

SMISHING | INCIBE | INCIBE [Anónimo]. INCIBE | INCIBE [página web]. [Consultado el 9, julio, 2023]. Disponible en Internet: https://www.incibe.es/aprendeciberseguridad/smishing

SRTP - Overview - Dialogic Integrated Media gateways - Documentation [Anónimo]. Dashboard - Documentation [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: <https://wiki.freepbx.org/display/DIMG/SRTP+-+Overview>.

TÉCNICAS DE ingeniería social [Anónimo]. Cloud Computing | Adaptix Networks | Cómputo en la Nube [página web]. [Consultado el 9, julio, 2023]. Disponible en Internet: https://www.adaptixnetworks.com/tecnicas-de-ingenieria-social/

TODO LO que se debe saber sobre el teletrabajo - Todo lo que se debe saber sobre el teletrabajo [Anónimo]. MINTIC Colombia [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://www.mintic.gov.co/portal/inicio/Sala-dePrensa/Noticias/126148:Todo-lo-que-se-debe-saber-sobre-el-teletrabajo

Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/27050/jpgiraldoma.pdf?sequence=1&isAllowed=y

Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/35224/mrgomezbu.pdf?sequence=1&isAllowed=y

Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/27420/%20myibarrai.pdf?sequence=1&isAllowed=y

Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/25187/%20eanovoag.pdf?sequence=1&isAllowed=y

Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/44501/mortizos.pdf?sequence=3&isAllowed=y

Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet:

https://repository.unad.edu.co/bitstream/handle/10596/42675/pmrinconn.pdf?sequence=3&isAllowed=y

Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/22690/91532860.pdf?sequence=1&isAllowed=y

Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/28152/%20jaime.sedano.pdf?sequence=1&isAllowed=y

Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/42674/ltsolerp.pdf?sequence=3&isAllowed=y

Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 17, julio, 2023]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/18701/1075273452.pdf?isAllowed=y&sequence=1

Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 20, julio, 2023]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/28152/%20jaime.sedano.pdf?sequence=1

Universidad Nacional Abierta y a Distancia UNAD - [página web]. [Consultado el 1, agosto, 2023]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/28152/%20jaime.sedano.pdf?sequence=1&isAllowed=y

Universidad Piloto de Colombia [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/11574/Ataques%20ciberneticos_Trabajo%20grado_Juan%20Morales_v2.pdf?sequence=1&isAllowed=y

Universidad Piloto de Colombia [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2647/00004333.pdf?sequence=1&isAllowed=y

Universidad Piloto de Colombia [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6354/El%20arte%20de%20la%20ingeniería%20social.pdf?sequence=1&isAllowed=y.

Estructura del documento para la estructura del Resumen Analítica Especializado -RAE

Fecha de Realización:	15/20/2023
Programa:	Especialización en seguridad informática
Línea de Investigación:	
Título:	ANÁLISIS DEL IMPACTO EN LA IMPLEMENTACIÓN DEL TRABAJO REMOTO, RESPECTO DEL AUMENTO DE ATAQUES DE INGENIERÍA SOCIAL EN LAS EMPRESAS DEL SECTOR RETAIL.
Autor(es):	Beltran Saavedra Diego Armando
Palabras Claves:	Ciberdelincuente, Malware, Ingeniería social, Phishing, Pharming.
Descripción:	El presente proyecto de monografía busca abordar el aumento de los ataques de ingeniería social como práctica para obtener información privada, con el impacto que ha tenido la implementación del trabajo remoto en las empresas del sector retail a partir el factor humano y los errores atribuibles al desconocimiento y falta de formación en materia de seguridad informática. Este enfoque es de vital importancia para la ingeniería, ya que la ciberseguridad ha evolucionado con el tiempo y requiere una comprensión más completa de los riesgos asociados; además de una orientación al análisis de los programas de información por parte de la empresa, se busca abordar de manera integral el tema de la ingeniería social. Además, se definen las técnicas más utilizadas por los ciberdelincuentes para acceder a la seguridad informática en las empresas del sector retail, poniendo énfasis en las vulnerabilidades que surgen de la implementación del trabajo remoto. Se examinarán detalladamente técnicas como Phishing, Smishing, Pharming y Vishing, y se

	analizará su impacto en el sector. Se expone una evaluación de las medidas preventivas que deben implementarse en las empresas del sector retail para contrarrestar los ataques de ingeniería social más comunes, de tal manera que sea posible establecer pautas claras y efectivas para proteger los sistemas informáticos y la información confidencial, teniendo en cuenta las normas establecidas por la NTC.

Fuentes bibliográficas destacadas:

PHISHING | INCIBE | INCIBE [Anónimo]. INCIBE | INCIBE [página web]. [Consultado el 9, julio, 2023]. Disponible en Internet: https://www.incibe.es/aprendeciberseguridad/phishing

Institutional Repository [página web]. [Consultado el 17, julio, 2023]. Disponible en Internet: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/46386/Suarez_VLM-SD.pdf?isAllowed=y&sequence=1

HACKER VS Ciberdelincuente | INCIBE | INCIBE [Anónimo]. INCIBE | INCIBE [página web]. [Consultado el 9, julio, 2023]. Disponible en Internet: https://www.incibe.es/aprendeciberseguridad/hacker-vs-ciberdelincuente#:~:text=El%20ciberdelincuente%20es%20la%20persona,ingeniería%20social%20o%20el%20malware.&text=If%20playback%20doesn't%20begin%20shortly,%20try%20restarting%20your%20device.

9 FORMAS de evitar los ataques de vishing [+3 aplicaciones de bloqueo de spam] [Anónimo]. Geekflare [página web]. [Consultado el 1, agosto, 2023]. Disponible en Internet:https://geekflare.com/es/vishing-attack-prevention/

¡OJO! ESTOS son los ciberdelitos que más se cometen en Colombia [Anónimo]. Semana.com Últimas Noticias de Colombia y el Mundo [página web]. [Consultado el 31, julio, 2023]. Disponible en Internet: https://www.semana.com/tecnologia/articulo/ojo-estos-son-los-ciberdelitos-que-mas-se-cometen-en-colombia/202127/

Contenido del documento:	El objetivo de la siguiente monografía es entender como la ingeniería social implica el uso de tácticas psicológicas para influir en el comportamiento humano y obtener información confidencial. Se aprovechan los sesgos mentales e instintos para recopilar datos o acceder a sistemas, y se conoce como "piratería humana" y se utiliza a nivel global. Antes se llevaba a cabo en interacciones directas, pero ahora se ha expandido a través de redes sociales y plataformas en línea. A lo largo del tiempo, la ingeniería social ha evolucionado y se ha transformado en un instrumento valioso para ciberdelincuentes que buscan acceder a sistemas de información de organizaciones. Los piratas informáticos han mejorado sus técnicas y utilizan métodos más avanzados y sutiles para obtener información confidencial. Para reducir estos riesgos, es esencial que las organizaciones no solo se concentren en la protección técnica de sus sistemas, sino que también capaciten a su personal en seguridad cibernética y en la identificación y prevención de ataques de ingeniería social. Los empleados tienen un papel fundamental en la protección de la información y deben estar preparados para enfrentar estas amenazas. La capacitación en seguridad cibernética e ingeniería social debe ser un fragmento integro de la cultura de seguridad organizacional. Esto trae consigo educar a los empleados sobre diferentes tipos de ataques de ingeniería social así cómo reconocerlos y evitarlos. También es crucial que comprendan el valor de la seguridad cibernética, así como su responsabilidad en la protección de la información.

	Además de la capacitación, las organizaciones deben implementar políticas sólidas de seguridad cibernética, que incluyan prácticas de autenticación seguras, control de acceso y segregación de redes. El uso de herramientas de monitoreo de amenazas puede ser útil para detectar y prevenir ataques de ingeniería social. También es esencial contar con un plan de respuesta a incidentes para reaccionar adecuadamente en caso de ataques. En resumen, las organizaciones deben enfocarse en mantener el control de sus sistemas de información para evitar la manipulación y el robo de datos. Esto requiere capacitar y preparar adecuadamente al personal para enfrentar los desafíos de la ingeniería social. Comprender los intentos de los piratas informáticos para manipular el comportamiento es fundamental para una gestión diaria segura. Si los empleados no se consideran parte de la solución, podrían actuar de manera arriesgada y comprometer la seguridad de la organización.
Marco Metodológico:	En el siguiente documento, se realizará un análisis exhaustivo del marco científico y tecnológico relacionado con la implementación del trabajo remoto y las técnicas de ingeniería social en el sector retail. Se explorarán estudios, investigaciones y avances relevantes en el campo, proporcionando una base sólida para comprender la problemática y los desafíos asociados. **1. Avance tecnológico en el ámbito del trabajo remoto**. En primer lugar, se examinarán los avances tecnológicos que han impulsado el desarrollo y la adopción del trabajo remoto en las últimas décadas. Se analizarán las herramientas de comunicación y colaboración digital, como

	videoconferencias, plataformas de gestión de proyectos en línea y aplicaciones móviles, que han facilitado la realización de tareas a distancia. Además, se revisarán las tendencias y los desafíos emergentes en el ámbito del trabajo remoto, como la seguridad informática y la custodia de datos. **2. Investigaciones sobre ingeniería social y seguridad informática.** En esta sección, se examinarán las investigaciones más relevantes asociadas con la ingeniería social y la seguridad informática. Se abordarán estudios que han analizado las técnicas implementadas por los ciber atacantes para llevar a cabo ataques de ingeniería social, así como las consecuencias y los impactos que han tenido en las organizaciones. También se destacarán las estrategias y medidas preventivas propuestas en la literatura científica para contrarrestar este tipo de ataques. **3. Estudios sobre la situación tecnológica y de seguridad en el sector retail.** En esta subsección, se explorarán investigaciones y estudios que han analizado la situación tecnológica y de seguridad en el sector retail, particularmente en relación con la implementación del trabajo remoto. Además, se revisarán los desafíos y las brechas de seguridad identificadas en investigaciones previas. **4. Marco normativo y regulaciones relevantes.** Por último, se abordará el marco normativo y las

	regulaciones relevantes relacionadas con la implementación del trabajo remoto y la seguridad informática en el sector retail. Se analizarán las normas y estándares nacionales, así como las políticas igual que las regulaciones nacionales que influyen en la defensa de la información y la precaución de ataques de ingeniería social.
Conceptos adquiridos :	**Efectos de la Implementación del Trabajo Remoto:** Se obtiene una comprensión detallada de cómo la implementación del trabajo remoto afecta a las empresas del sector retail, incorporando cambios en la cultura organizacional, la productividad y la eficiencia operativa. **Vulnerabilidades en la Seguridad Informática:** Se identifica y analizan las vulnerabilidades específicas en la seguridad informática asociadas con el trabajo remoto en el contexto del sector retail, con un enfoque especial en los riesgos de la ingeniería social. **Prácticas de Seguridad en el Trabajo Remoto:** Se examina las prácticas de seguridad implementadas por las empresas del sector retail durante la transición al trabajo remoto. Esto incluirá políticas de seguridad, medidas de protección de datos y protocolos de respuesta a incidentes, proporcionando una visión detallada de cómo las organizaciones gestionan la seguridad de la información en un entorno de trabajo remoto. **Conciencia y Educación en Seguridad:** Se destaca la importancia de la conciencia y la educación en seguridad para los empleados

	que trabajan de forma remota. Se podrían proponer recomendaciones específicas para mejorar la capacitación y la sensibilización en cuestiones de seguridad, buscando fortalecer la preparación y el conocimiento de los colaboradores frente a posibles amenazas. **Evaluación de Riesgos de Ingeniería Social:** Se realiza una evaluación detallada de los riesgos de ingeniería social asociados con el trabajo remoto en empresas del sector retail. Esta evaluación identifica posibles puntos de vulnerabilidad y áreas de mejora en la seguridad, permitiendo una comprensión más profunda de los desafíos específicos vinculados a la ingeniería social en el ámbito laboral remoto. **Adaptabilidad Tecnológica:** Se examina cómo las empresas del sector retail han adaptado su infraestructura tecnológica para respaldar el trabajo remoto. La investigación evaluará la efectividad de estas adaptaciones en términos de seguridad y resistencia a amenazas, proporcionando una visión detallada de las soluciones tecnológicas implementadas para garantizar la integridad de los sistemas de información. **Recomendaciones para Mitigar Riesgos:** Se investiga recomendaciones específicas y prácticas para mitigar los riesgos identificados, ofreciendo a las empresas del sector retail una guía con acciones concretas para fortalecer sus estrategias de seguridad en el entorno de trabajo remoto.
Conclusiones:	La formación de los usuarios a menudo se descuida porque se cree erróneamente que el uso de software avanzado es suficiente para evitar los ciberataques. Sin embargo, debido a que los avances tecnológicos y los

	ciberdelincuentes están en constante evolución, es imprescindible realizar un entrenamiento continuo, sin olvidar lo ocurrido en ataques previos, ya que muchos métodos existentes derivan de otros ya conocidos y nuevas estrategias para tener éxito. Es relevante destacar que, a lo largo del tiempo, los métodos de ingeniería social han evolucionado, volviéndose cada vez más sofisticados en su intento de engañar a los usuarios y obtener acceso a información confidencial. Teniendo en cuenta lo anterior, es importante que las empresas del sector retail estén al tanto de las últimas técnicas de ingeniería social y se preparen para enfrentarlas. Es esencial que las empresas del sector retail implementen medidas adecuadas de seguridad cibernética para protegerse contra los ataques de ingeniería social. Estas medidas pueden incluir la adopción de soluciones avanzadas de seguridad, como el monitoreo de redes y la detección de intrusiones, así como la actualización regular de software y sistemas para protegerse contra nuevas amenazas. Realizar pruebas de penetración y simulaciones de ataques de ingeniería social es beneficioso para descubrir posibles debilidades y corregirlas antes de que sean aprovechadas. Contratar expertos en seguridad cibernética también puede mejorar la protección en entornos de trabajo remoto.