

**Estrategia para la prevención de ataques de ingeniería social en las empresas del sector
financiero en la ciudad de Bogotá**

Diana Norela Duque Gallego

Asesor

Edgar Mauricio López Rojas

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Especialización en Seguridad Informática

2024

Dedicatoria

Con amor dedico este trabajo a mi hermana Sandra Milena Duque, quien siempre ha sido mi apoyo incondicional y fuente constante de inspiración. Tú amor, paciencia y aliento han sido muy importantes para mi logro académico. Este trabajo está dedicado a ti, con gratitud. A mi esposo Luis Macias, mi compañero de vida, una gran motivación. Tú constante apoyo y comprensión han sido fundamentales durante este arduo proceso. Este logro es nuestro, y esta dedicatoria es una muestra de mi amor inquebrantable hacia ti.

A mis padres Luz Elena Gallego y José Arturo Duque, quienes han sido mis guías, mis mayores impulsores en la vida. No tengo palabras para agradecerles la dedicación, sacrificios y el amor incondicional que han hecho posible que hoy pueda celebrar este éxito. Este trabajo está dedicado a ustedes con el amor más profundo que pueda existir.

A mis sobrinos Mariana Alejandra y José Alejandro, quienes han llenado mi vida de alegría y han sido fuente constante de inspiración. A través de este trabajo, espero ser un ejemplo para ustedes y mostrarles que los sueños se pueden hacer realidad por más difícil que veamos el camino, este lo logramos con esfuerzo y determinación. Esta dedicación es un testimonio de mi amor y deseo de verlos crecer y triunfar en la vida.

Agradecimientos

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, en especial al Ingeniero Edgar Mauricio López Rojas porque me acompañó en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

Resumen

Esta monografía centra su importancia en el estudio de las amenazas cibernéticas a las que se ven enfrentadas frecuentemente las entidades financieras en la ciudad de Bogotá, estas se dan desde la práctica de la ingeniería social. Este tipo de amenaza son muy peligrosas ya que desde allí se puede explorar la vulnerabilidad de los seres humanos.

La ingeniería social se relaciona estrictamente con las técnicas de manipulación tecnológicas, donde se busca engañar de una manera psicológica desde el robo de información personal o empresarial, donde por medio de diferentes acciones se roban mucha información no solo personal si no confidencial de las empresas, involucrando así la seguridad de las organizaciones, dichas tácticas pueden tener una serie de estrategias y técnicas que pueden ser adaptadas las características del objetivo.

En la ciudad de Bogotá, hay diferentes entidades financieras que se han visto particularmente vulneradas con las tácticas de robo de información, estas dan como resultado alto robos de información, extorsiones y manipulación de todo el sistema. Esta monografía resalta la falta de cultura organizacional que centra en el interés de la seguridad y la falta de conciencia en los directivos y empleados que dejan brechas significativas en las tecnologías de seguridad.

Palabras clave: Ataques informáticos, ingeniería social, seguridad de la información.

Abstract

This monograph focuses its importance on the study of the cyber threats that financial entities in the city of Bogotá frequently face, these occur from the practice of social engineering.

This type of threat is very dangerous since from there the vulnerability of human beings can be explored. Social engineering is strictly related to technological manipulation techniques, where it seeks to deceive in a psychological way from the theft of personal or business information, where through different actions a lot of information is stolen, not only personal but also confidential from companies, thus involving the security of organizations, these tactics can have a series of strategies and techniques that can be adapted to the characteristics of the objective.

In the city of Bogotá, there are different financial entities that have been particularly vulnerable to information theft tactics, which result in high information theft, extortion, and manipulation of the entire system. This monograph highlights the lack of organizational culture that focuses on the interest of security and the lack of awareness among managers and employees that leaves significant gaps in security technologies.

Keywords: Computer attacks, social engineering, information security.

Tabla de Contenido

Introducción	13
Planteamiento del Problema	14
Justificación	15
Objetivos	16
Objetivo General	16
Objetivos Específicos	16
Marco Referencial	17
Antecedentes	17
Ataques de Ingeniería Social Ocurren en los Últimos Tres Años en Colombia	18
Marco Conceptual	21
Conceptos	21
<i>Marco Teórico</i>	<i>24</i>
Algunas Características Comunes del Spear Phishing	26
Algunas Características Comunes del Vishing	27
Algunas Características del Smishing	28
Características Principales Mensajes Engañosos	29
Objetivos de los Atacantes	29
Vulnerabilidades Explotadas	32

Técnicas para Evitar Ataques	36
Tipos de Pentesting	37
Estadísticas Ataques.....	38
Estadísticas de Phishing.....	40
<i>Marco Legal</i>	42
Desarrollo Objetivo 1	44
Diseño Metodología	44
<i>Tabla 1</i>	45
Los Seis Tipos de Controles de Seguridad Relacionados con la Norma	48
Principales Vectores de Ataques en Colombia Phishing	49
Herramientas De Ciberseguridad	50
<i>Sistemas de Intrusión (IDS/IPS) Snort</i>	51
Herramientas de Seguridad de end Point Antivirus/Antimalware Symantec end Point <i>Protection</i>	52
<i>Endpoint Detection and Response (EDR) Crowd Strike Falcon</i>	52
Herramientas de Gestión de Identidades y Accesos (IAM) RSA SecurID	52
<i>Gestión de Identidades y Accesos Okta</i>	53
Herramientas de Gestión de Vulnerabilidades Nessus	53
Gestion de Parches	54
Herramientas de Seguridad de Datos BitLocker	54
<i>Prevención de Pérdida de Datos (DLP) Forcepoint DLP</i>	55

Herramientas de Monitoreo y Gestión de Eventos de Seguridad (SIEM) Splunk	55
Herramientas de Respuesta a Incidentes	56
Herramientas de Seguridad en la Nube AWS security hub	56
<i>Gestión de Identidades y Accesos en la Nube Okta</i>	56
Herramientas de Análisis de Red Nmap.....	57
<i>Wireshark</i>	57
Desarrollo Objetivo 2	58
Estrategia para La Capacitación y Sensibilización en Ciberseguridad	58
Desarrollo Objetivo 3	63
Recomendaciones para Mitigar Riesgos de Ingeniería Social en el Sector Financiero de Bogotá	63
Conclusiones.....	66
Referencias Bibliográficas.....	67

Lista de Tablas

Tabla 1	<i>Controles de Seguridad Adaptados de la Norma SP 800-53</i>	41
Tabla 2	<i>Resumen Analítico</i>	8

Lista de Figuras

Figura 1	<i>Principios Fundamentales de la Seguridad de la Información.....</i>	25
Figura 2	<i>Medidas de Seguridad.....</i>	26
Figura 3	<i>Ataques Smishing a Número Propio</i>	31
Figura 4	<i>Suplantación de Identidad.....</i>	31
Figura 5	<i>Tipos de Vectores de Ataque</i>	32
Figura 6	<i>Creación de Correo Suplantando Identidad</i>	32
Figura 7	<i>Colombia entre los 20 Países más Atacados</i>	39
Figura 8	<i>Colombia 30% Ataque Ransomware.....</i>	40
Figura 9	<i>Estadística Spam 2021</i>	40
Figura 10	<i>Empresas Blanco de Ataques de Phishing</i>	41
Figura 11	<i>Áreas de Enfoque.....</i>	48
Figura 12	<i>Ingreso a Gophish y Creo la Campaña.....</i>	58
Figura 13	<i>Creación de Campaña de Phishing de Facebook</i>	59
Figura 14	<i>Detalla Envío de Correo</i>	59
Figura 15	<i>Verificamos Detalles de Envío</i>	60
Figura 16	<i>Ingreso Bandeja de Entrada.....</i>	60
Figura 17	<i>Apertura del Correo</i>	61
Figura 18	<i>Ingreso a Página Web Facebook Phishing</i>	61
Figura 19	<i>Verificación Dashboard</i>	62
Figura 20	<i>Insertar Credenciales de Acceso.....</i>	62
Figura 21	<i>Creación de Curso.....</i>	72
Figura 22	<i>Conceptos</i>	73

Figura 23 Ataques	73
Figura 24 Estudio de Ataques Ingeniería Social	74
Figura 25 Que es Ingeniería Social	74
Figura 26 Preguntas Didácticas	75
Figura 27 Se Realiza un Quiz Didáctico Enfocado a Ingeniería Social	75
Figura 28 Inicio Juego	76
Figura 29 Modo Inicio de Juego	76
Figura 30 Preparando Juego	77
Figura 31 Código Acceso a Juego	77
Figura 32 Se Loguean	78
Figura 33 Pregunta 1	78
Figura 34 Pregunta 2	79
Figura 35 Pregunta 3	79
Figura 36 Pregunta 4	80
Figura 37 Pregunta 5	80
Figura 38 Pregunta 6	81
Figura 39 Pregunta 7	81
Figura 40 Pregunta 8	82
Figura 41 Finaliza.....	82

Apéndice

Apéndice A *Estrategia que se Debe Implementar para Prevenir Ataques de Ingeniería*

Social.....71

Apéndice B *Módulo 1*.....72

Apéndice C *Módulo 2*.....75

Introducción

En la era digital actual, las organizaciones se encuentran constantemente en la mira de ciberataques, especialmente aquellos impulsados por la ingeniería social. Estos ataques no solo comprometen la seguridad de la información, sino también puede poner en riesgo la privacidad de los usuarios y generar pérdidas financieras significativas. En Bogotá, las empresas enfrentan desafíos al implementar estrategias efectivas de prevención de ingeniería social entre su personal. Estos desafíos pueden variar desde la falta de conciencia y capacitación adecuada hasta las limitaciones presupuestarias que dificultan la contratación de especialistas en seguridad de la información. Es fundamental identificar y abordar los desafíos que enfrentan sus organizaciones para fortalecer la seguridad de sus sistemas y protegerse contra los ataques de ingeniería social.

El presente trabajo planteara un ejercicio de phishing para realizar ingeniería social, a partir de creación de un correo falso que pretende capturar información sensible como son credenciales de acceso, con el fin de demostrar que tan expuestos vulnerables podemos llegar a ser. Con este ejercicio se busca lograr sensibilizar a los colaboradores de entidades financieras de la ciudad de Bogotá para que de esta forma tengan más precaución y verifiquen la veracidad de la información esto con el fin de realizar mejores prácticas de seguridad de la información.

Planteamiento del Problema

En la actualidad las empresas del sector financiero en Bogotá se enfrentan exponencialmente a ataques cibernéticos, especialmente ataques de ingeniería social, la ingeniería social se ha convertido en una de las principales amenazas para la seguridad de la información en las empresas del sector financiero en la ciudad de Bogotá. Este tipo de ataques explota la psicología humana y la falta de capacitación en ciberseguridad para obtener acceso a información confidencial y causar daños significativos, esta formulación reconoce la importancia de proteger a las personas y organizaciones de ataques de ingeniería social, ya que pueden dar lugar a violaciones de la privacidad, pérdidas financieras, y otros impactos negativos. Se enfatiza en la necesidad de fortalecer la seguridad de los sistemas, lo que implica identificar y abordar las vulnerabilidades específicas que surgen debido a los ataques de ingeniería social.

¿Cuáles son los desafíos más significativos que enfrentan las organizaciones del sector financiero en Bogotá al implementar estrategias de prevención de ataques de ingeniería social, y que metodologías o normativas son más efectivas para mejorar la seguridad de la información?

Justificación

Esta investigación es crucial para entender las deficiencias actuales en la capacitación y concientización en ciberseguridad dentro de las empresas del sector financiero en Bogotá. Al identificar y evaluar las estrategias y metodologías más efectivas, se podrán desarrollar recomendaciones y prácticas que fortalezcan la seguridad de la información, reduciendo la susceptibilidad a los ataques de ingeniería social.

La seguridad es un tema crítico en un entorno cada vez más digitalizado. Los riesgos de seguridad, en cuanto a virus informáticos, phishing y ciberataques, pueden provocar pérdida en datos sensibles, la interrupción del servicio y el robo de información confidencial.

La detección de vulnerabilidades a través de ataques de ingeniería social en un trabajo planteado tiene como propósito mejorar la seguridad, concientizar y capacitar a los empleados, fortalecer las políticas y procedimientos de seguridad, proteger los datos y la privacidad de una organización. Al abordar estas vulnerabilidades, se reducen los riesgos y se fortalece la postura de seguridad de la empresa.

La ingeniería social representa amenazas significativas para la seguridad de la información en las empresas del sector financiero. Estudios previos han demostrado que estos ataques pueden llegar a tener consecuencias devastadoras, y no solo en pérdidas financieras, sino también en la pérdida de confianza por parte de los clientes y daños de reputación. según un informe de la Asociación Internacional de Seguridad de la Información (ISACA), el 60% de las empresas financieras han experimentado al menos un ataque de ingeniería social en los últimos 12 meses (ISACA, 2020)

Objetivos

Objetivo General

Proponer una estrategia de capacitación y concientización en ingeniería social, mediante revisión literaria como apoyo al personal de tecnología de la información y seguridad informática de las empresas del sector financiero en Bogotá.

Objetivos Específicos

Determinar metodología, tipos de ataques, herramientas de ciberseguridad, para el diagnóstico de la seguridad de la información en organizaciones de sector financiero en Bogotá.

Plantear una estrategia para la capacitación y sensibilización en ciberseguridad y protección de datos para el 100% del personal del sector financiero en organizaciones de Bogotá, con el fin de reducir los incidentes de seguridad de la información.

Presentar las recomendaciones para prevenir ataques de ingeniería social en personal de tecnología de la información y seguridad informática en organizaciones de Bogotá.

Marco Referencial

Antecedentes

Diversos estudios han explorado la problemática de la seguridad informática en el sector financiero, identificando múltiples vulnerabilidades y áreas de mejora. Según García (2020), las empresas han incrementado sus inversiones en tecnología de seguridad, adquiriendo herramientas como firewalls, IDS/IPS, sin embargo, García también señala que la falta de capacitación en ingeniería social sigue siendo una debilidad significativa.

Un estudio realizado por López Martínez (2019) en Bogotá reveló que el 70% de las entidades financieras han experimentado intentos de phishing en los últimos tres años, a pesar de los esfuerzos tecnológicos, los ataques de phishing siguen siendo prevalentes debido a la explotación de factores humanos, como la falta de conciencia y la formación inadecuada.

Además, un informe de la Asociación Colombiana de Bancos (Asobancaria) de (2021) señala que los ataques de ingeniería social han aumentado un 35% en el último año, con un impacto significativo en la seguridad de las transacciones financieras y la confianza del cliente.

Estudios más recientes, como el de Ramírez y Pérez (2022), subrayan la importancia de la cultura organizacional en la prevención de ataques de ingeniería social. Su investigación en varias empresas financieras de Bogotá encontró que aquellas con programas de capacitación continuos y políticas de seguridad claras tienen una tasa significativamente menor de incidentes de ingeniería social.

Asimismo, el análisis de Velásquez y Gómez (2023) sobre la efectividad de las políticas de seguridad cibernética en el sector financiero colombiano revela que las organizaciones que integran la formación en ingeniería social dentro de sus programas de seguridad integral logran reducir notablemente los intentos de fraude y ataques cibernéticos.

Ataques de Ingeniería Social Ocurren en los Últimos Tres Años en Colombia

El 2 de mayo de 2024 la plataforma del Sistema Electrónico de Contratación Pública (SECOP II) de Colombia Compra Eficiente: Fue víctima de un ataque cibernético. Este ataque resultó en una caída del sistema durante más de 34 horas, impidiendo que los contratistas subieran sus cuentas de cobro y que las entidades estatales realizaran trámites de contratación y compras públicas ([infobae](#)) ([La FM](#)).

El ataque llevó a la Agencia Nacional de Contratación Pública a convocar una reunión con organismos de seguridad del Estado para investigar el incidente y tomar medidas de contención. A pesar de la interrupción, Colombia Compra Eficiente aseguró que no se comprometieron los datos de los usuarios y que se emitió una certificación para extender los plazos de los procesos de contratación afectados ([La FM](#)) ([Semana](#)).

2023 ataque a Audifarma: “La compañía farmacéutica, Audifarma, declaró el pasado domingo 22 de enero que fue objeto de un ataque cibernético en su infraestructura tecnológica. Como consecuencia, sus servidores físicos y virtuales tuvieron que ser deshabilitados temporalmente para proteger la información de la organización y los usuarios. Su página web y aplicación están fuera de servicio también” (El Espectador, 2023), según informó la empresa en comunicado oficial.

No se publicaron más detalles sobre este evento, por lo tanto, no se confirmó si efectivamente fue o no un ataque de ransomware lo que comprometió la infraestructura de la gestora farmacéutica.

El 20 de abril de 2023, el Grupo Nutresa: Una de las principales compañías de alimentos en Colombia, fue víctima de un ciberataque de ransomware. El ataque fue identificado rápidamente, y la empresa activó sus protocolos de seguridad para mitigar el impacto. A pesar de

estos esfuerzos, el grupo de ransomware Lockbit logró robar y posteriormente publicar datos sensibles de la empresa, incluyendo información de empleados y documentos internos de operaciones y costos (infobae) (ITECH S.A.S).

Aunque inicialmente Nutresa informó que la integridad de sus datos y la información de sus clientes no se había visto comprometida, la publicación de estos datos por parte de los atacantes contradice esta afirmación. La compañía ha designado un equipo especializado para gestionar el incidente y está cooperando con las autoridades para investigar el ataque y encontrar a los responsables (ITECH S.A.S) (Yahoo Finanzas).

El 13 de junio de 2023, la Policía Nacional de Colombia: sufrió un ataque cibernético dirigido al Registro Nacional de Medidas Correctivas (RNMC), una plataforma crítica que centraliza la información sobre medidas disciplinarias y correctivas impuestas por la policía. Este ataque comprometió la integridad y disponibilidad de los datos, afectando la capacidad de la policía para gestionar y consultar estas medidas SiegedSec es un grupo hacktivista que apareció días antes de la invasión rusa a Ucrania (SOCradar, 2023).

El RNMC es esencial para la transparencia y la gestión eficiente de las medidas correctivas, facilitando el seguimiento y control de estas acciones por parte de las entidades responsables y los ciudadanos interesados. La plataforma permite un acceso centralizado y mejora la rendición de cuentas, además de apoyar en la toma de decisiones estratégicas basadas en datos confiables y actualizados (Sistema).

El ataque a la plataforma del RNMC resalta la vulnerabilidad de las infraestructuras digitales críticas y la necesidad urgente de mejorar la ciberseguridad en las entidades gubernamentales. Este incidente es parte de una serie de ataques cibernéticos que han afectado a diversas instituciones en Colombia, subrayando la importancia de estrategias robustas de defensa

cibernética para proteger datos sensibles y asegurar la continuidad de los servicios públicos (infobae) (Colombia Check).

2022 DIAN: Estafadores se hacen pasar por la DIAN para alertar sobre “anomalías en la renta” Recientemente la Dirección de Impuestos y Aduanas Nacionales (DIAN) emitió una alerta sobre una campaña de estafa dirigida a quienes declaran renta en el país.

Mediante una técnica conocida como phishing, los cibercriminales están falseando la imagen de la DIAN para enviar correos electrónicos (con el logo de la DIAN y la firma de su director) a sus víctimas, advirtiéndoles que se encontraron anomalías en su declaración de renta, y que si no realizan un pago inmediato se verían expuestos a sanciones jurídicas en sus propiedades y cuentas bancarias.

Campaña de Phishing en Bancolombia (2022): Bancolombia alerta a sus clientes sobre una campaña de phishing que utilizaba mensajes de texto (SMS) fraudulentos. Los mensajes contenían enlaces a sitios web falsos diseñados para robar credenciales de acceso a la banca en línea. La entidad financiera implemento medidas adicionales de seguridad y sensibilización para proteger a los usuarios.

Marco Conceptual

Conceptos

Ciberataque. Intento malicioso de acceder, dañar o robar información.

Confidencialidad. Es el encargado de proteger la información contra los lectores no autorizados.

Integridad. La información debe permanecer íntegra, esto quiere decir que no podrá ser manipulada sin previa autorización.

Disponibilidad. Se debe garantizar la autenticidad del usuario, es decir implementar mecanismos de autenticidad en cada dispositivo con el fin de evitar suplantación.

Ataques de Ingeniería Social. Son estrategias utilizadas por personas malintencionadas para manipular y engañar a otras con el fin de obtener información confidencial, acceso a sistemas, realizar estafas u otros actos perjudiciales.

Phishing. Es uno de los ataques de ingeniería social más conocidos. Consiste en enviar correos electrónicos o mensajes falsos que aparentan ser de una entidad legítima, como un banco o una empresa reconocida, con el objetivo de obtener información confidencial, como contraseñas, números de tarjetas de crédito o datos personales.

Suplantación de Identidad. Los ciberdelincuentes se hacen pasar por organizaciones legítimas, como bancos, redes sociales, tiendas en línea o proveedores de servicios, utilizando logotipos, nombres de dominio y diseños similares para engañar a las víctimas y hacer que crean que están interactuando con la entidad genuina.

Spear Phishing. Es una variante más sofisticada del phishing. En lugar de enviar correos electrónicos masivos, los atacantes personalizan los mensajes para que parezcan provenir de una fuente confiable y conocida por la víctima. Utilizan información específica sobre la persona, como

su nombre, cargo o empresa, para aumentar la probabilidad de éxito del ataque.

Suplantación de Identidad. Los atacantes se hacen pasar por una entidad o persona de confianza para engañar a la víctima. Pueden utilizar nombres de empresas conocidas, direcciones de correo electrónico similares o incluso nombres de personas específicas dentro de la organización.

Ingeniería Social. Es una táctica de manipulación psicológica empleada por los ciberdelincuentes para engañar a las personas y obtener información confidencial o inducir acciones perjudiciales. Se basa en explotar la confianza, la falta de conocimiento y las vulnerabilidades emocionales de las personas.

Vishing (del Inglés "voice phishing"). Es una forma de ataque de ingeniería social que se basa en llamadas telefónicas para engañar a las personas y obtener información confidencial o hacer que realicen acciones específicas.

Smishing. Es una combinación de (SMS) y phishing, se refiere a un ataque en el que usan mensajes de texto para engañar a las personas y hacer que revelen información personal, como contraseñas, números de tarjetas de crédito, u otros datos sensibles. Esta técnica aprovecha el uso generalizado de teléfonos móviles y la alta confianza que la gente suele tener hacia las comunicaciones por SMS.

Baiting. Se refiere al acto de atraer, provocar o incitar a alguien para que reaccione de una manera específica. Generalmente, se utiliza en contextos negativos o manipulativos, donde se busca engañar, irritar o desencadenar una respuesta emocional en la persona objetivo.

Seguridad de la Información. ISO 27001(2013) relata. "El Sistema de Gestión de Seguridad de la Información persigue la protección de la información y de los sistemas de información del acceso, de utilización, divulgación o destrucción no autorizada.

La seguridad de la información, según ISO 27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser, electrónicos, audios o videos etc.”

Acortadores URL. Son servicios en línea que se utilizan para reducir la longitud de una URL (Dirección web) larga.

Ramsonware. Es un ataque malicioso donde el delincuente busca cifrar los datos de una organización y exige un pago para restaurar el acceso.

Marco Teórico

La norma SP 800-53 es una guía publicada por el Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU, que proporciona un catálogo de controles de seguridad y privacidad para sistemas de información federales. Aunque está diseñada para agencias federales, también es ampliamente utilizada en el sector privado. Algunos puntos clave sobre SP 800-53:

Categorías de Seguridad. SP 800-53 organiza los controles en 18 familias, tales como gestión de riesgos, control de acceso, y respuesta a incidentes.

Controles de Seguridad y Privacidad La guía ofrece controles específicos de seguridad y privacidad, y describe cómo implementar estos controles para mitigar riesgos en sistemas de información.

Marco de Gestión de Riesgos (RMF). SP 800-53 se alinea con el NIST RMF, proporcionando un proceso estructurado para gestionar los riesgos de seguridad de la información.

Flexibilidad y Escalabilidad. Los controles son diseñados para ser adaptables a diferentes tamaños de organizaciones y niveles de riesgo, permitiendo a las organizaciones personalizar los controles según sus necesidades específicas.

Actualizaciones Periódicas. NIST actualiza regularmente SP 800-53 para abordar nuevas amenazas y tecnologías emergentes, asegurando que la guía esté alineada con las mejores prácticas actuales de ciberseguridad.

La seguridad de la información cuenta con tres pilares, partiremos de la confidencialidad de la información, no divulgamos ni ponemos a disposición a personas no autorizadas. Este pilar nos garantiza que solo las personas autorizadas tienen acceso a la

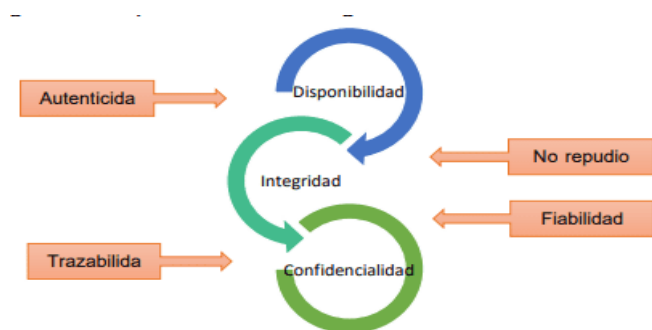
información.

Continuamos con la Disponibilidad de la información, este pilar es el encargado de garantizar que la información se encuentre a disposición de quien la necesita. Es importante resaltar que solo las personas autorizadas pueden acceder a esta. Por último, Integridad de la información, es la encargada de que la información se mantenga segura y lejos de ser alterada o manipulada por personas malintencionadas. En caso de que se requiera ser modificada se deberá contar con autorización.

La ingeniería social se define como el arte de manipular a las personas para que divulguen información confidencial. Los ataques de ingeniería social son uno de los mayores problemas en la actualidad, los ciberdelincuentes se encargan de persuadir a los usuarios para de alguna manera den información como datos confidenciales, Los ataques pueden tomar muchas formas incluyendo phishing, spear phishing, vishing, baiting y Pretexting. En entidades financieras pueden tener graves consecuencias, como pérdida de datos, daños financieros y afectación en la reputación.

Figura 1

Principios Fundamentales de la Seguridad de la Información



Nota. La imagen describe los principios que hacen formación sólida de la seguridad de la información. Tomado de *información NTC-ISO/IEC27001*

Figura 2*Medidas de Seguridad*

Nota. La imagen describe las medidas que ayudan a proteger la información contra amenazas cibernéticas y garantizan la integridad y confidencialidad de los datos críticos Tomado de *información NTC-ISO/IEC27001*

Los ataques de ingeniería social en su mayoría de veces son más difíciles de detectar, porque estos involucran nuestras actividades diarias, se aprovechan de la confianza para hacer un proceso en específico.

Algunas Características Comunes del Spear Phishing

Personalización

A diferencia del phishing general, los ataques de spear phishing se personalizan para que coincidan con los intereses, roles o actividades del objetivo. Los atacantes investigan a sus víctimas para obtener información personal o profesional y luego utilizan esta información para hacer que los correos electrónicos o mensajes sean más convincentes.

Investigación Previa

Antes de lanzar un ataque de spear phishing, los atacantes suelen investigar cuidadosamente a sus víctimas. Esto implica recopilar información de fuentes públicas, como redes sociales, sitios web de la empresa o información filtrada previamente.

Uso de Información Interna

En algunos casos, los atacantes pueden tener acceso a información interna previa de la organización o individuos específicos. Esto les permite personalizar aún más sus ataques y hacer que los mensajes parezcan más legítimos.

Uso de Técnicas Avanzadas

Los atacantes de spear phishing a menudo utilizan técnicas más avanzadas para evadir la detección, como el uso de enlaces enmascarados, archivos adjuntos maliciosos o el aprovechamiento de vulnerabilidades en el software utilizado por las víctimas.

Algunas Características Comunes del Vishing

Uso de Llamadas Telefónicas

A diferencia de otras formas de phishing que utilizan correo electrónico o mensajes de texto, el vishing se basa en llamadas telefónicas para establecer contacto directo con la víctima.

Suplantación de Identidad

Los atacantes suelen hacerse pasar por personas o entidades legítimas, utilizando técnicas de manipulación para convencer a la víctima de que están hablando con alguien confiable.

Uso de Tácticas de Ingeniería Social

Los atacantes aprovechan la psicología humana, como el miedo, la urgencia o la autoridad, para persuadir a las víctimas de que revelen información confidencial o realicen acciones no deseadas.

Obtención de Información Confidencial

El objetivo principal del vishing es obtener información personal o financiera valiosa, que luego puede ser utilizada para cometer fraude o robo de identidad.

Énfasis en la Urgencia

Los atacantes suelen crear una sensación de urgencia en la víctima, haciendo que sientan que deben actuar rápidamente para evitar consecuencias negativas.

Algunas Características Comunes del Baiting

Provocación Intencional

El "baiting" implica una acción deliberada para molestar, enojar o perturbar a alguien. Puede llevarse a cabo mediante comentarios provocativos, insinuaciones o actitudes que buscan desencadenar una reacción.

Engaño o Manipulación

En muchas ocasiones, el "baiting" involucra el uso de engañosa manipulación para atraer a la persona objetivo. Esto puede incluir hacer afirmaciones falsas o exageradas, ocultar información relevante o tergiversar los hechos con el fin de generar una respuesta emocional.

Objetivo de Generar Reacciones

El propósito principal del "baiting" es obtener una respuesta emocional o una reacción específica de la persona objetivo. Puede ser utilizado para generar conflictos, alimentar discusiones o simplemente para entretenerse a costa de la molestia de los demás.

Contexto Digital

A menudo, el "baiting" se asocia con el entorno en línea, como las redes sociales, los foros de discusión o los comentarios en línea. Las plataformas digitales proporcionan un medio fácil para lanzar provocaciones y observar las respuestas de las personas.

Algunas Características del Smishing

El smishing es una forma de phishing que utiliza mensajes de texto (SMS) para engañar a los usuarios y robarles información personal o financiera. Los ciberdelincuentes se hacen pasar

por entidades legítimas (bancos, empresas de servicios públicos, etc.) para convencer a las víctimas de que realicen acciones que beneficien a los atacantes.

Características Principales Mensajes Engañosos

Urgencia. Los mensajes suelen crear un sentido de urgencia para presionar a la víctima a actuar rápidamente.

Personalización. A veces, los atacantes incluyen información personal de la víctima para aumentar la credibilidad del mensaje.

Enlaces Maliciosos

Los mensajes contienen enlaces que redirigen a sitios web falsos diseñados para robar información.

Solicitudes de Información Confidencial

Los atacantes solicitan datos como contraseñas, números de tarjetas de crédito, información de cuentas bancarias, etc. Disfraz de entidades legítimas

Imitación de Marcas

Los mensajes suelen utilizar logotipos y nombres de empresas conocidas para generar confianza.

Temas actuales. Los atacantes aprovechan eventos actuales (pandemias, desastres naturales) para crear mensajes más convincentes.

Objetivos de los Atacantes

Robo de Identidad

Obtener información personal para hacerse pasar por la víctima.

Robo de dinero. Acceder a cuentas bancarias o realizar transacciones fraudulentas.

Infección de dispositivos. Instalar malware en los dispositivos de las víctimas.

Ejemplos de Mensajes de Smishing

"Alerta de seguridad: Se ha detectado actividad sospechosa en su cuenta. Actualice su información aquí: [enlace malicioso]"

"Felicitaciones, ha ganado un premio. Reclame su premio ahora: [enlace malicioso]"

"Su tarjeta ha sido bloqueada. Verifique sus datos aquí: [enlace malicioso]"

Cómo Protegerse del Smishing:

No hacer clic en enlaces sospechosos: Evita hacer clic en enlaces de remitentes desconocidos.

Verificar la autenticidad del remitente: Asegúrate de que el número o dirección de correo electrónico del remitente sea legítimo.

No Compartir Información Personal por SMS

Evita responder a mensajes que soliciten información confidencial.

Utilizar Aplicaciones de Seguridad

Instala una aplicación de seguridad en tu teléfono móvil para protegerte de amenazas.

Mantener el Software Actualizado

Mantén tu teléfono y aplicaciones actualizados con las últimas actualizaciones de seguridad.

Figura 3

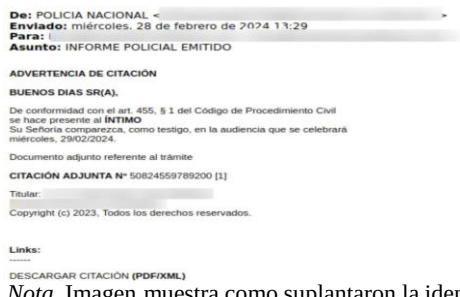
Ataques Smishing a Número Propio



Nota. La imagen refleja un ataque de smishing, el cual es fácil de detectar ya que me llegó a mi número de celular informándome, no le di clic porque no tengo cuenta en Netflix por lo tanto evite que me hicieran un fraude.

Figura 4

Suplantación de Identidad



Nota. Imagen muestra como suplantaron la identidad de la policía nacional adjuntaron un link el cual es un virus malware.

Tomado de (s/f). Incibe.es. Recuperado el 20 de mayo de 2024

Algunas características del Ramsonware

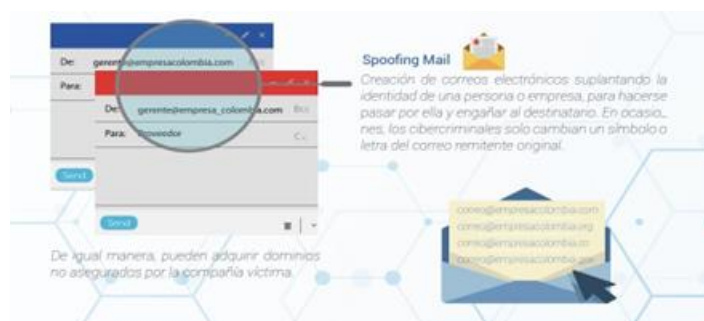
Cifrado de archivos Mensaje de rescate Plazos y amenazas

Vulnerabilidades explotadas Phishing y métodos de propagación Ataques dirigidos

Figura 5*Tipos de Vectores de Ataque*

Nota. La imagen muestra las diferentes técnicas de ataques ransomware para lograr su objetivo de alguna manera Tomado de (S/f).

Akamai.com. Recuperado el 20 de mayo de 2024, de <https://www.akamai.com/es/glossary/what-is-attack-vector>

Figura 6*Creación de Correo Suplantando Identidad*

Nota. Suplanta la identidad para tener credibilidad y engañar. Su víctima. Tomado (S/f-b).Org.co. Recuperado el 21 de mayo de

2024, de <https://www.ccit.org.co/wp-content/uploads/informe-tendencias-ciberdelincuencia-comprimido-3.pdf>

Vulnerabilidades Explotadas

La ingeniería social explota varias vulnerabilidades psicológicas y técnicas. Las vulnerabilidades psicológicas incluyen la curiosidad, la falta de conciencia de seguridad y la confianza excesiva. Las vulnerabilidades técnicas incluyen la falta de actualizaciones de software, la debilidad de las contraseñas y la falta de capacitación en conciencia de seguridad.

Algunas de las Vulnerabilidades Detectadas a Través de Ataques de Ingeniería Social

Incluyen

Falta de Conciencia

Muchas personas no están familiarizadas con las tácticas de ingeniería social y no son conscientes de los riesgos asociados. Esto las hace más propensas a caer en trampas y revelar información confidencial sin darse cuenta.

Confianza Excesiva

Los atacantes explotan la tendencia natural de las personas a confiar en otros. Utilizan técnicas de manipulación para ganarse la confianza de sus víctimas y obtener acceso a información sensible o sistemas protegidos.

Descuido en la Seguridad

Algunas personas pueden ser descuidadas en cuanto a las medidas de seguridad básicas, como mantener contraseñas seguras o proteger su información personal. Los atacantes aprovechan estas debilidades y utilizan tácticas de ingeniería social para obtener acceso no autorizado.

Curiosidad o Sensacionalismo

Los ataques de ingeniería social a menudo se basan en aprovechar la curiosidad humana o generar un sentido de urgencia o miedo. Los atacantes pueden utilizar señuelos como titulares llamativos, premios falsos o amenazas para atraer a las personas y hacer que tomen acciones impulsivas sin pensar en las consecuencias.

Falta de Entrenamiento o Educación

Muchas organizaciones y usuarios individuales no brindan suficiente capacitación o educación sobre la ingeniería social y sus riesgos asociados. Como resultado, las personas pueden no estar preparadas para reconocer las señales de un ataque de ingeniería social y actuar de manera segura.

Técnicas de Ingeniería Social Combinadas

Ataques Técnicos con Componentes Sociales

Phishing

Aunque principalmente psicológico, el phishing a menudo utiliza elementos técnicos como correos electrónicos fraudulentos con enlaces a sitios web falsificados que imitan a los auténticos, engañando a las víctimas para que ingresen sus credenciales.

Smishing

Variante del phishing que utiliza mensajes de texto para dirigir a las víctimas a sitios web maliciosos o para que descarguen aplicaciones maliciosas.

Ransomware a través de Correos Electrónicos

Correos electrónicos que contienen archivos adjuntos o enlaces a descargas que, cuando se abren, instalan ransomware en el sistema de la víctima.

Técnicas Puramente Psicológicas

Vishing

Llamadas telefónicas en las que el atacante se hace pasar por un representante de una entidad financiera para obtener información confidencial, como contraseñas o números de tarjetas.

Pretexting

Creación de una historia o pretexto falso para engañar a la víctima y lograr que revele información personal o financiera.

Baiting

Dejar dispositivos físicos (como USB) infectados con malware en lugares públicos con la esperanza de que alguien los recoja y los use, comprometiendo su sistema.

Técnicas Físicas y de Observación

Shoulder Surfing

Observación directa de la información que una persona está introduciendo en su dispositivo, como contraseñas o números de tarjetas.

Dumpster Diving

Búsqueda de información sensible en la basura de las organizaciones, como documentos desechados que contienen datos financieros o de clientes. Prevención y mitigación: Es importante capacitar y crear conciencia de seguridad, la implementación de políticas de seguridad sólidas, la actualización frecuente de software y la utilización de contraseñas seguras. También se pueden utilizar herramientas de seguridad de intrusiones para detectar y actos mal intencionados.

Técnicas para Evitar Ataques

Verificación de la Fuente

Si recibes un correo electrónico, mensaje o llamada que solicita información confidencial, verifica la fuente de la comunicación. Nunca reveles información confidencial a menos que estés seguro de que la solicitud es legítima.

No Hacer Clic en Enlaces Sospechosos

Si recibimos un enlace o link por cualquier vía, no hagas clic en él a menos que estés seguro de que es seguro. En su lugar, escribe la URL manualmente en tu navegador.

Capacitación En Conciencia de Seguridad

Todos debemos estar capacitados en conciencia de seguridad y comprendan los riesgos “ingeniería social”. Esto puede ayudar a prevenir que alguien revele información confidencial o realice acciones no autorizadas.

Mantén Tus Sistemas Actualizados

Asegurarnos de que los sistemas y software estén actualizados y parcheados. Los delincuentes informáticos pueden explotar vulnerabilidades conocidas en el software para obtener acceso no autorizado.

Usa Contraseñas Seguras

Utilizar contraseñas seguras y únicas para todas tus cuentas. No generar claves simples, ejemplo "123456".

Verifica las Solicitudes de Ayuda

Si alguien te pide ayuda o acceso a tus sistemas, verifica su identidad antes de darles acceso.

Métodos para Prevenir Amenazas

Mecanismos de Inspección

Debemos realizar revisiones periódicas a nuestros sistemas especialmente a nuestro servidor, lo hacemos con trazabilidad en log, la cual nos muestra toda la información de accesos que ha tenido nuestro servidor evidenciando los accesos autorizados y los no autorizados, de esta manera da una alerta al administrador del sistema.

Prueba de Penetración

Es un proceso autorizado y controlado en el cual se evalúa la seguridad de un sistema informático o una red. El objetivo principal de un intento de penetración es identificar vulnerabilidades y brechas en la seguridad para que puedan ser corregidas antes de que sean explotadas por personas malintencionadas.

Tipos de Pentesting

Pentesting de Red

Se enfoca en evaluar la seguridad de la infraestructura de red, incluyendo Routers,

switches, firewalls y otros dispositivos de red, para identificar vulnerabilidades que puedan ser explotadas.

Pentesting de Redes Inalámbricas

Se enfoca en evaluar la seguridad de redes inalámbricas, como Wi-Fi, para identificar vulnerabilidades que puedan permitir el acceso no autorizado a la red o la interceptación de datos.

Pentesting de Ingeniería Social

Se concentra en evaluar la resistencia de una organización a ataques de ingeniería social, que implican la manipulación psicológica de personas para obtener información confidencial o acceso no autorizado a sistemas.

Pentesting de Sistemas Operativos

Se centra en evaluar la seguridad de sistemas operativos como Windows, Linux o Mac OS, identificando vulnerabilidades en la configuración, permisos y configuración de servicios.

Hardening

Se refiere al proceso de fortalecimiento o endurecimiento de algo para hacerlo más resistente, seguro o protegido frente a posibles amenazas.

Estadísticas Ataques

Figura 7

Colombia Entre los 20 Países más Atacados



Nota. Colombia se encuentra en los 20 países más atacados por diferentes vectores. Tomado de MAPA. (s/f). MAPA | Mapa en tiempo real de amenazas cibernéticas Kaspersky. Recuperado el 21 de mayo de 2024, de <https://cybermap.kaspersky.com/es>

Hablando puntualmente de Colombia, según la Policía Nacional, los delitos cibernéticos más denunciados por la ciudadanía son:

Hurto por medios informáticos: 9.573.

Violación de datos personales: 4.705.

Acceso abusivo a sistemas informáticos: 4.610.

Suplantación de sitios web: 1.994.

Uso de software malicioso 178.

Igualmente, se estima que el 85% de las empresas que cuentan con Protocolo de Escritorio Remoto, son más vulnerables a sufrir ataques de ransomware, por lo que se sugiere que las mismas estén en constante revisión de sus políticas de protección.

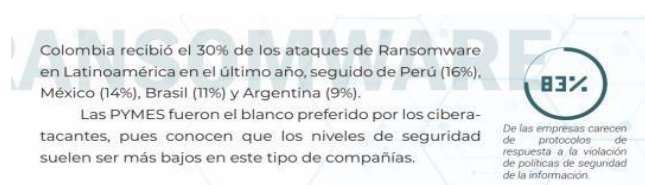
Según el Banco Interamericano de Desarrollo (BID) de continuar con la curva de crecimiento de los ciberataques en la región, el costo anual podría superar los USD \$90millones para 2025, es decir un promedio de más de 18.5 millones de ataques anuales.

Ransomware

Colombia recibió el 30% de los ataques de Ransomware en Latinoamérica en el último año, seguido de Perú (16%), México (14%), Brasil (11%) y Argentina (9%). Las PYMES fueron el blanco preferido por los ciber atacantes, pues conocen que los niveles de seguridad suelen ser más bajos en este tipo de compañías.

Figura 8

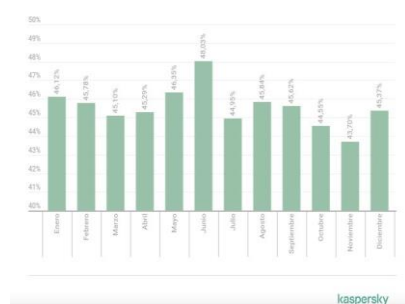
Colombia 30% Ataque Ransomware



Nota. Observamos que en Latinoamérica el 83% de las empresas no cuentan con protocolos de respuesta de información Tomado de (S/f-b). Org.co. Recuperado el 21 de mayo de 2024, de https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Figura 9

Estadística Spam 2021



Nota. El porcentaje promedio de spam es 45,56%. Tomado de Kulikova, T. (2022, febrero 9). El spam y el phishing en 2021. Kaspersky. <https://securelist.lat/spam-and-phishing-in-2021/96171/>

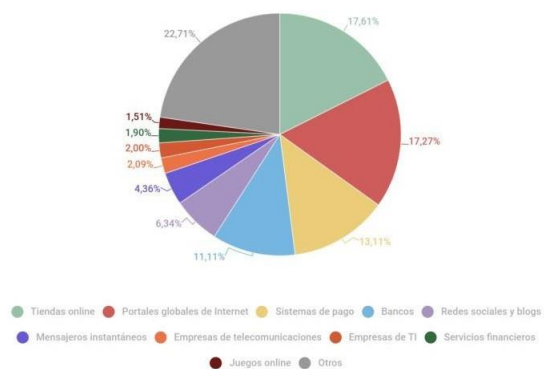
Estadísticas de Phishing

En 2021, nuestro sistema anti phishing evitó que se hicieran 253 365 212 clics en enlaces de phishing. El 8,20% de los usuarios de Kaspersky de todo el mundo han sufrido ataques de

phishing al menos una vez.

Figura 10

Empresas Blanco de Ataques de Phishing



Nota. Los ataques de phishing a bancos ocupan un 11.11% tomado de Kulikova, T. (2022, febrero 9). *El spam y el phishing en 2021*. Kaspersky. <https://securelist.lat/spam-and-phishing-in-2021/96171/>

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”² Decreto 1747 de 2000, por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales

Ley 1266 de 2008, Por la cual se dictan 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.

La Ley 1273 de 2009 establece sanciones penales para aquellos que cometan delitos informáticos, incluyendo los relacionados con ingeniería social. Algunos de los delitos informáticos contemplados en la ley que pueden estar asociados a la ingeniería social incluyen el acceso abusivo a un sistema informático, la interceptación de datos informáticos, la utilización de programas maliciosos y la suplantación de sitios web o perfiles en redes sociales.

Ley 1581 de 2012, Por medio de la cual se dictan disposiciones generales para la protección de Datos Personales.

Es importante destacar que la legislación y las medidas de seguridad pueden evolucionar con el tiempo, por lo que es recomendable consultar fuentes actualizadas y expertos en el campo de la ciberseguridad para obtener información precisa sobre el marco legal vigente en Colombia en relación con las vulnerabilidades detectadas por ataques de ingeniería social.

Decreto 1377 de 2013, reglamenta la ley 1581 de 2012 especificando aspectos relacionados con la autorización para el tratamiento de datos personales, la responsabilidad demostrada y la transferencia internacional de datos.

Ley 1928 de 2018, Refuerza las medidas contra los delitos informáticos y el cibercrimen, actualizando el marco legal para enfrentar nuevas amenazas y vulnerabilidades en el entorno digital.

Ley 2017 de 2020, Ley de la protección de infraestructura crítica, establece disposiciones para la protección de infraestructuras críticas y servicios esenciales, incluyendo sistemas de información y redes.

Ley 2052 de 2020, Regula la implementación de la política de ciberseguridad y ciberdefensa en Colombia, creando un marco para la cooperación entre sector público y privado en la protección del ciberespacio.

Ley 2108 de 2021, promueve la implementación de medias de seguridad cibernética en las entidades públicas, estableciendo requisitos para la protección de la información y la adopción de tecnologías seguras.

Decreto 338 de 2022, Reglamenta aspectos de la ciberseguridad en el sector financiero, incluyendo la obligación de reportar incidentes de ciberseguridad y establecer planes de contingencia y recuperación.

Desarrollo Objetivo 1

Diseño Metodología

Para el desarrollo de este trabajo, se ha seleccionado la norma NIST SP 800-53 organiza los controles de seguridad y privacidad que se pueden implementar en las organizaciones financieras para proteger sus sistemas de información. Estos controles están organizados en familias (Como control de acceso, auditorias, responsabilidad).

Tabla 1*Controles de Seguridad Adaptados de la Norma SP 800-53*

ID del Control	Categoría	Control de Seguridad	Descripción
AT-2	Formación y Concienciación	Programa de Concienciación y Capacitación en Seguridad	Implementar programas de formación continua para empleados sobre la identificación y respuesta a amenazas de seguridad.
AC-2	Control de Acceso	Gestión de Cuentas	Establecer procesos para la creación, modificación, eliminación y supervisión de cuentas de usuario.
AC-3	Control de Acceso	Control de Acceso Basado en Roles (RBAC)	Asignar permisos de acceso en función de los roles y responsabilidades de los empleados.
IA-2	Autenticación e Identificación	Autenticación Multifactor (MFA)	Requerir múltiples factores de autenticación para acceder a sistemas y datos sensibles.
IA-5	Autenticación e Identificación	Gestión de Autenticadores	Gestionar el ciclo de vida de autenticadores (como contraseñas, tokens) de manera segura.
SI-3	Seguridad de la Información	Actualización de Software	Asegurar que todos los sistemas y aplicaciones se mantengan actualizados con los últimos parches de seguridad.
SI-4	Seguridad de la Información	Monitoreo de Sistemas	Implementar sistemas para monitorear continuamente la actividad en la red y

ID del Control	Categoría	Control de Seguridad	Descripción
			detectar incidentes de seguridad.
SC-8	Protección de Comunicaciones	Protección de la Confidencialidad e Integridad de la Información	Implementar cifrado para proteger la información sensible en tránsito.
SC-13	Protección de Comunicaciones	Protección de la Confidencialidad	Utilizar cifrado para proteger la información sensible en reposo.
CM-2	Gestión de la Configuración	Línea Base de Configuración	Establecer y mantener una configuración base segura para sistemas y dispositivos.
CA-7	Evaluación y Autorización	Monitoreo Continuo	Realizar monitoreo continuo de los sistemas para identificar y mitigar amenazas en tiempo real.
CP-4	Planificación de Contingencias	Pruebas y Ejercicios de Planes de Contingencia	Realizar pruebas regulares y ejercicios de los planes de contingencia para asegurar la preparación ante incidentes.
IR-4	Respuesta a Incidentes	Respuesta a Incidentes	Desarrollar y mantener capacidades de respuesta a incidentes, incluyendo procedimientos para la notificación y manejo de incidentes.
MP-6	Protección de Medios	Eliminación de Información	Implementar procedimientos para la eliminación segura de datos y medios físicos que contengan información sensible.

ID del Control	Categoría	Control de Seguridad	Descripción
RA-5	Evaluación de Riesgos	Análisis de Vulnerabilidades	Realizar análisis de vulnerabilidades periódicos para identificar y mitigar riesgos en los sistemas de información.
PE-3	Seguridad Física	Control de Acceso Físico	Implementar controles de acceso físico a las instalaciones donde se almacenan o procesan datos sensibles.
PS-3	Seguridad del Personal	Investigación de Antecedentes	Realizar verificaciones de antecedentes para empleados y contratistas que tengan acceso a información crítica.

Nota. Esta tabla muestra los controles que pueden ser adaptados a entidades financieras de Bogotá

Figura 11*Áreas de enfoque*

Nota. Funciones de una organización. Tomado de *Marco para la mejora de la seguridad cibernética en infraestructuras críticas.*

(s/f). Nist.gov. Recuperado el 24 de mayo de 2024, de

https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmiellrev_20181102mn_clean.pdf

Los Seis Tipos de Controles de Seguridad Relacionados con la Norma

Controles Preventivos

Diseñados para detener incidentes antes de que sucedan. Controles Detectivos: Permiten la identificación de incidentes en tiempo real.

Controles Correctivos

Ayudan a mitigar el daño luego de un incidente de seguridad.

Controles Recuperativos

Establecen cómo se restauran los servicios y funciones tras un incidente.

Controles Compensativos

Proporcionan alternativas a los controles estándar cuando estos no son viables.

Controles Físicos

Involucran estrategias para proteger el entorno físico de los sistemas de información.

Al implementar la norma NIST SP 800-53 en entidades financieras de Bogotá proporcionara una base sólida para mejorar la seguridad de la información, cumplir con regulaciones, ganar la confianza del cliente, y mantener la eficiencia y continuidad del negocio. Estos beneficios son cruciales para enfrentar el panorama de amenazas cibernéticas cada vez más complejo y garantizar el éxito a largo plazo de las entidades financieras.

Principales Vectores de Ataques en Colombia Phishing

Los ciberdelincuentes envían correos electrónicos fraudulentos para persuadir y engañar, de esta manera logran que se revele información confidencial como claves o detalles bancarios.

Ataques de Fuerza Bruta

Los ciberdelincuentes intentan adivinar la contraseña utilizando diferentes métodos como ataques hasta lograr encontrar la correcta.

Ataques de Inyección SQL

Los hackers insertan un código SQL malicioso en las entradas del usuario para manipular la base de datos.

Malware

Los hackers utilizan software dañino para robar datos, dañar sistemas o controlarlos dispositivos por medio remoto.

Ataques de Denegación de Servicio (DDoS)

Los atacantes sobrecargan un sitio web o servicio con tráfico falso para hacerlo inaccesible.

Ataques de Intermediarios Man-in-the-Middle

Los atacantes se interponen en la comunicación para interceptar datos

Ataques Zero-Day

Los atacantes exploran vulnerabilidades antes de que se publique una solución.

Ataques de Ingeniería Social

Los hackers manipulan a las personas para obtener información confidencial

Ataques de Ransomware

Los hackers cifran archivos o sistemas y exigen un rescate para otorgar nuevamente acceso.

Ataque a Dispositivos de Internet de las Cosas (IoT)

Los atacantes comprometen dispositivos IoT para acceder a la red y robar datos

Herramientas De Ciberseguridad

Para las empresas del sector financiero en Bogotá, es fundamental elegir herramientas que no solo sean robustas y eficaces, sino que también cumplan con las regulaciones locales e internacionales de protección de datos.

Las herramientas mencionadas aquí están alineadas con los estándares de seguridad globales y pueden ser implementadas para proteger tanto infraestructuras locales como sistemas en la nube.

Además, al seleccionar estas herramientas, las empresas deben considerar la capacitación continua del personal y la implementación de políticas de seguridad estrictas para asegurar que las soluciones tecnológicas sean utilizadas de manera efectiva y segura.

Algunas de las herramientas que recomendaría y que abarquen diferentes aspectos de la ciberseguridad para empresas del sector financiero en Bogotá, son las siguientes:

Herramientas de Seguridad de Red Firewall Cisco ASA

Descripción. Soluciones de firewall que incluyen VPN, protección contra intrusiones y filtrado de contenido.

Código Abierto. No, es una solución comercial.

PfSense

Un firewall de código abierto que ofrece características avanzadas de enrutamiento y VPN

Ejemplo que se podría aplicar.

En los bancos al utilizar Cisco ASA para proteger sus redes internas y externas, asegurando que el tráfico entre sus oficinas y los servicios de banca en línea esté siempre cifrado y seguro. Además, la capacidad de VPN permite a los empleados trabajar de manera segura desde ubicaciones remotas.

Sistemas de Intrusión (IDS/IPS) Snort

Descripción. Un sistema IDS/IPS de código abierto que ofrece detección entiempos real y análisis de tráfico.

Código Abierto: Sí.

Suricata

Otra herramienta IDS/IPS de código abierto que proporciona capacidades de análisis y detección en tiempo real.

Ejemplo que se podría aplicar:

Implementar Snort como parte de su sistema de detección de intrusiones para monitorear y analizar el tráfico de red en tiempo real, identificando y respondiendo a comportamientos sospechosos que podrían indicar un ataque.

Herramientas de Seguridad de end Point Antivirus/Antimalware Symantec end Point

Protection

Descripción. Ofrece protección avanzada contra malware y capacidades de gestión centralizada.

Código Abierto: No, es una solución comercial.

ClamAV

Un antivirus de código abierto que proporciona protección contra malware en diversas plataformas. Ejemplo que se podría aplicar:

Utilizar Symantec Endpoint Protection para asegurar todos los dispositivos de los empleados contra malware y otras amenazas, proporcionando capacidades de gestión centralizada para mantener todos los sistemas actualizados y protegidos.

Endpoint Detection and Response (EDR) Crowd Strike Falcon

Descripción. Proporciona protección basada en la nube con capacidades de detección y respuesta rápida.

Código Abierto: No, es una solución comercial.

Ossec

Una solución de código abierto que combina capacidades de IDS/IPS con monitoreo y respuesta en end points. Ejemplo que se podría aplicar:

Adoptar CrowdStrike Falcon para obtener visibilidad en tiempo real de todos los end points, permitiendo una rápida detección y respuesta ante cualquier actividad maliciosa detectada, reduciendo significativamente el tiempo de reacción ante incidentes de seguridad.

Herramientas de Gestión de Identidades y Accesos (IAM) RSA SecurID

Descripción. Proporciona autenticación MFA robusta para proteger el acceso a sistemas

críticos.

Código Abierto: No, es una solución comercial.

Google Authenticator

Una aplicación de código abierto que proporciona MFA mediante códigos de un solo uso.

Ejemplo que se podría aplicar:

Implementar RSA SecurID para proporcionar autenticación multifactor a sus empleados, asegurando que solo personal autorizado pueda acceder a sistemas críticos, incluso si las credenciales de un empleado son comprometidas.

Gestión de Identidades y Accesos Okta

Descripción. Plataforma de IAM basada en la nube que simplifica la gestión de identidades y accesos.

Código Abierto: No, es una solución comercial.

Keycloak. Una solución de código abierto para la gestión de identidades y accesos.

Ejemplo que se podría aplicar:

Utiliza Okta para gestionar el acceso a sus aplicaciones en la nube, simplificando el proceso de autenticación y proporcionando un único punto de acceso seguro para todas las aplicaciones empresariales.

Herramientas de Gestión de Vulnerabilidades Nessus

Descripción: Una de las herramientas de escaneo de vulnerabilidades más populares, ofrece detección y evaluación de vulnerabilidades.

Código Abierto: No, es una solución comercial.

OpenVAS

Una herramienta de código abierto que ofrece escaneo y evaluación de vulnerabilidades.

Ejemplo que se podría aplicar:

Utilizar Nessus para realizar escaneos regulares de vulnerabilidades en su infraestructura de TI, identificando y remediando posibles puntos débiles antes de que puedan ser explotados por atacantes.

Gestion de Parches

Manage engine patch manager plus

Descripción: Herramienta de gestión de parches que soporta múltiples sistemas operativos y aplicaciones.

Código Abierto: No, es una solución comercial.

WSUS (Windows Server Update Services)

Una herramienta de Microsoft para la gestión de parches, aunque no es de código abierto, es ampliamente utilizada y gratuita. Ejemplo que se podría aplicar:

Implementar ManageEngine Patch Manager Plus para asegurar que todos sus sistemas operativos y aplicaciones estén siempre actualizados con los últimos parches de seguridad, reduciendo el riesgo de vulnerabilidades explotables.

Herramientas de Seguridad de Datos BitLocker

Descripción: Solución de encriptación de Microsoft para proteger datos en discos duros y portátiles.

Código Abierto: No, es una solución comercial integrada en Windows. VeraCrypt: Una herramienta de código abierto para el cifrado de discos duros. Ejemplo que se podría aplicar:

Utilizar BitLocker para cifrar los discos duros de los laptops y desktops de los empleados, asegurando que los datos sensibles estén protegidos en caso de pérdida o robo de los dispositivos.

Prevención de Pérdida de Datos (DLP) Forcepoint DLP

Descripción: Proporciona capacidades de monitoreo y protección de datos en todas las plataformas.

Código Abierto: No, es una solución comercial.

No existen soluciones completas de DLP de código abierto comparables en alcance y características a Forcepoint, pero herramientas como **OpenDLP** pueden ofrecer funcionalidades básicas. Ejemplo que se podría aplicar:

Implementar Forcepoint DLP para monitorear y proteger la transferencia de datos sensibles a través de correos electrónicos y otras formas de comunicación, asegurando que no se filtren datos críticos fuera de la organización.

Herramientas de Monitoreo y Gestión de Eventos de Seguridad (SIEM) Splunk

Descripción: Plataforma SIEM que proporciona capacidades de análisis de grandes volúmenes de datos y monitoreo en tiempo real.

Código Abierto: No, es una solución comercial.

ELK Stack (Elasticsearch, Logstash, Kibana)

Una solución de código abierto para análisis y visualización de datos, ampliamente utilizada como SIEM. Ejemplo que se podría aplicar:

Utilizar Splunk como su plataforma SIEM para analizar grandes volúmenes de datos en tiempo real, permitiendo a los equipos de seguridad identificar y responder rápidamente a amenazas de seguridad.

Herramientas de Respuesta a Incidentes

Automatización y Orquestación de Respuesta a Incidentes (SOAR) IBM Resilient

Descripción. Proporciona herramientas para la automatización y gestión de la respuesta a incidentes.

Código Abierto. No, es una solución comercial.

TheHive. Una plataforma de código abierto para la gestión de incidentes y la respuesta a incidentes. Ejemplo que se podría aplicar:

Implementar IBM Resilient para automatizar y orquestar su respuesta a incidentes, mejorando la eficiencia y la rapidez con la que pueden gestionar y mitigar los efectos de incidentes de seguridad.

Herramientas de Seguridad en la Nube AWS security hub

Descripción. Servicio de AWS que centraliza y automatiza la evaluación de seguridad y el cumplimiento de normas.

Código Abierto. No, es un servicio comercial de AWS.

Cloud Custodian. Una herramienta de código abierto que puede gestionar y asegurar recursos en la nube. Ejemplo que se podría aplicar:

Utiliza AWS Security Hub para centralizar la evaluación de seguridad y el cumplimiento de normas en sus entornos de AWS, permitiendo una gestión más efectiva de la seguridad en la nube.

Gestión de Identidades y Accesos en la Nube Okta

Descripción. Proporciona soluciones de gestión de identidades para aplicaciones en la nube.

Código Abierto. No, es una solución comercial Ejemplo que se podría aplicar:

Al usar Okta podemos gestionar de manera segura el acceso a sus aplicaciones basadas en la nube, facilitando la integración con múltiples servicios y mejorando la experiencia de usuario.

Herramientas de Análisis de Red Nmap

Descripción. Es una herramienta de escaneo de red que permite descubrir hosts en una red y determinar los servicios y puertos que están abiertos en esos hosts.

Código Abierto. Sí. Ejemplo que se podría aplicar:

Utilizar Nmap para realizar escaneos regulares de su red, identificando hosts y servicios activos, así como puertos abiertos, lo que ayuda a mapear y proteger su infraestructura de red.

Wireshark

Descripción. Es un analizador de protocolos de red que captura y analiza el tráfico de red en tiempo real.

Código Abierto. Sí.

Ejemplo que se podría aplicar:

Emplear Wireshark para capturar y analizar tráfico de red en tiempo real, ayudando a los equipos de seguridad a identificar y solucionar problemas de red y posibles incidentes de seguridad.

Desarrollo Objetivo 2

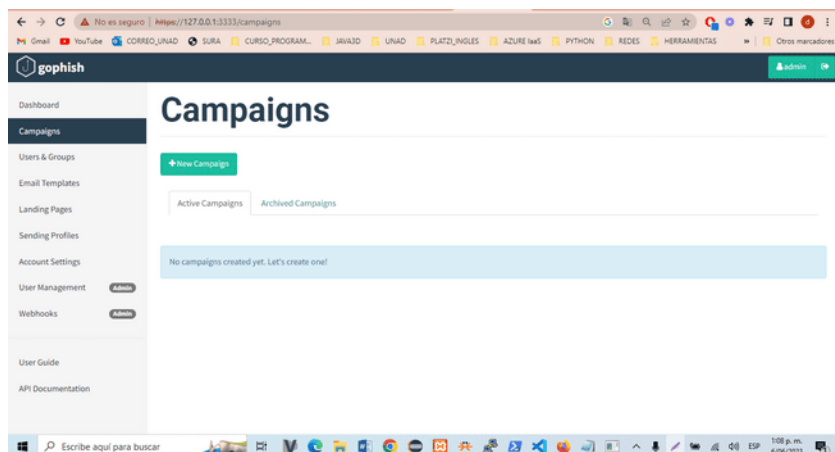
Estrategia para La Capacitación y Sensibilización en Ciberseguridad

Simulaciones de phishing Correo – Campaña de sensibilización.

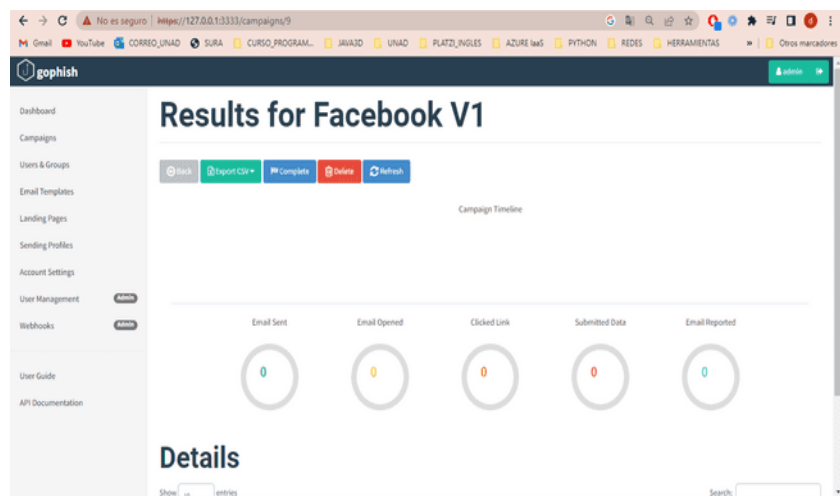
Vamos a crear un correo (phishing) simulando un ataque, utilizaremos la herramienta Gophish de código abierto, nos permitirá realizar simulación de phishing a los colaboradores de tecnologías de la información y seguridad probaremos la exposición de la organización. Los cuales son sometidos a los respectivos ajustes buscando la mejor opción que asegure que el ataque es lo suficientemente verídico para que los empleados den información.

Figura 12

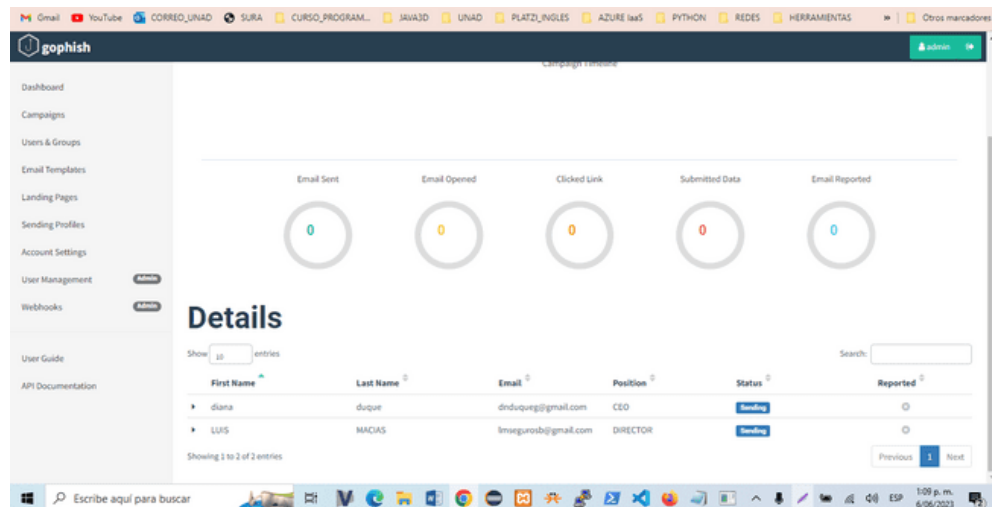
Ingreso a Gophish y Creo la Campaña



Nota. Ingreso al dashboard

Figura 13*Creación de Campaña de Phishing de Facebook*

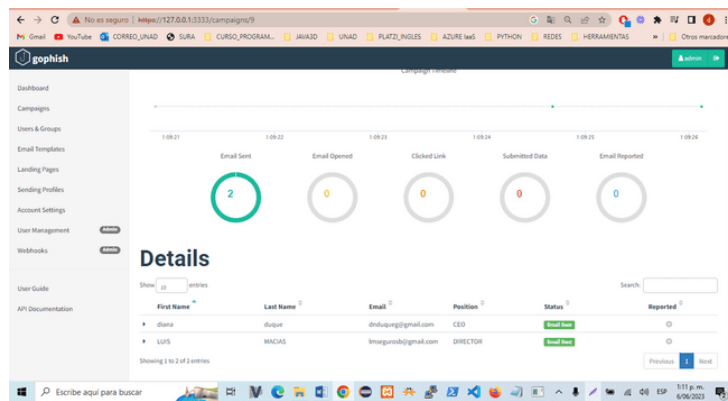
Nota. Se crea la campaña de Facebook

Figura 14*Detalla Envío de Correo*

Nota. El dashboard detalla el correo el cual voy atacar, en este caso es el mío.

Figura 15

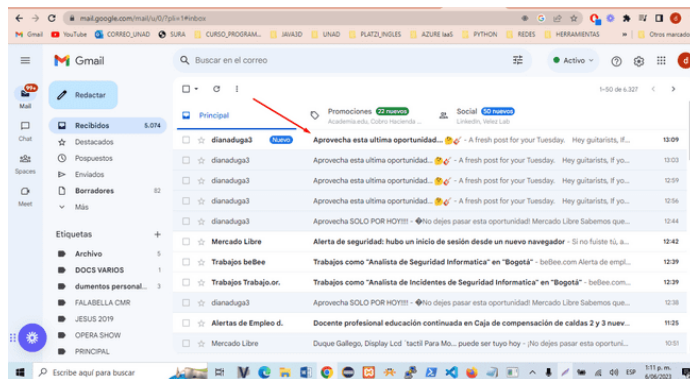
Verificamos Detalles de Envío



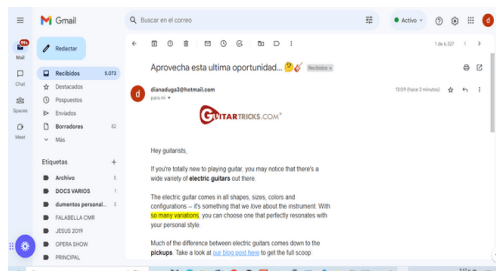
Nota. Al hacer el envío se detalla el seguimiento del correo y observamos que ha sido enviado a los dos correos ejemplos.

Figura 16

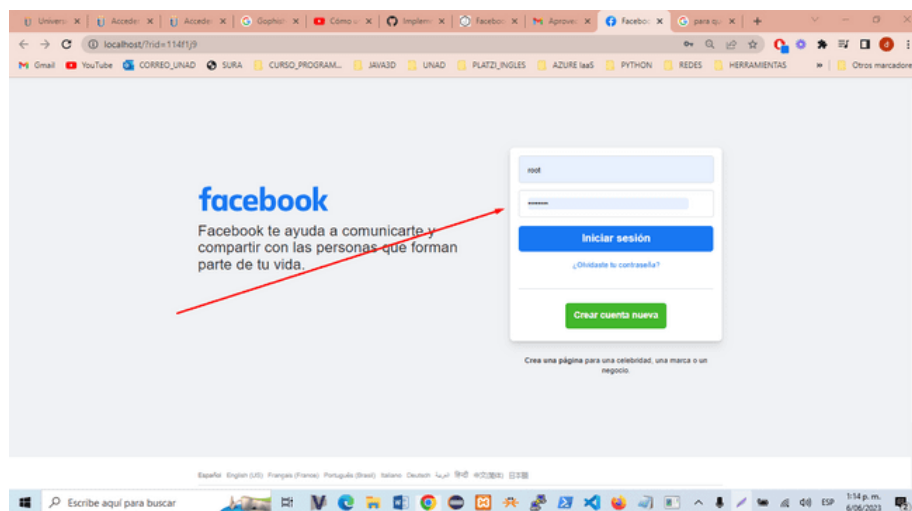
Ingreso Bandeja de Entrada



Nota. El correo se encuentra en mi bandeja de entrada con un asunto llamativo

Figura 17*Apertura del Correo*

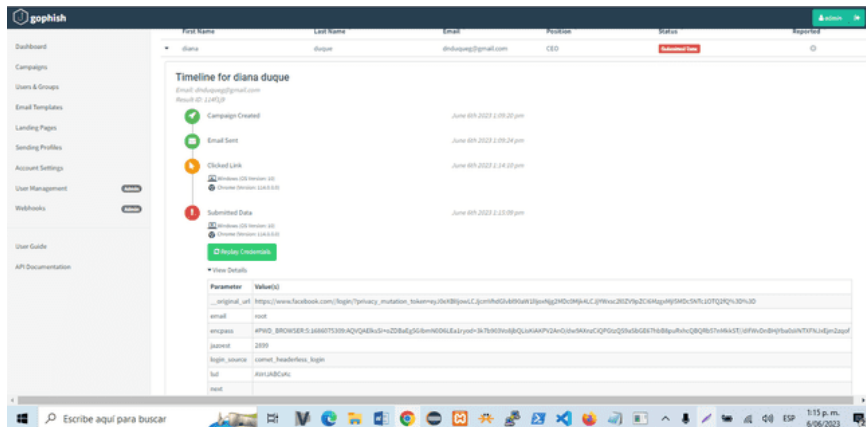
Nota. El correo tiene una información que me interesa sobre la música por tal motivo me es interesante y doy clic

Figura 18*Ingreso a Página web Facebook Phishing*

Nota. Nos direcciona a la supuesta página de Facebook real, pero en realidad lo que vamos hacer es robar las credenciales de acceso al loguear la víctima.

Figura 19

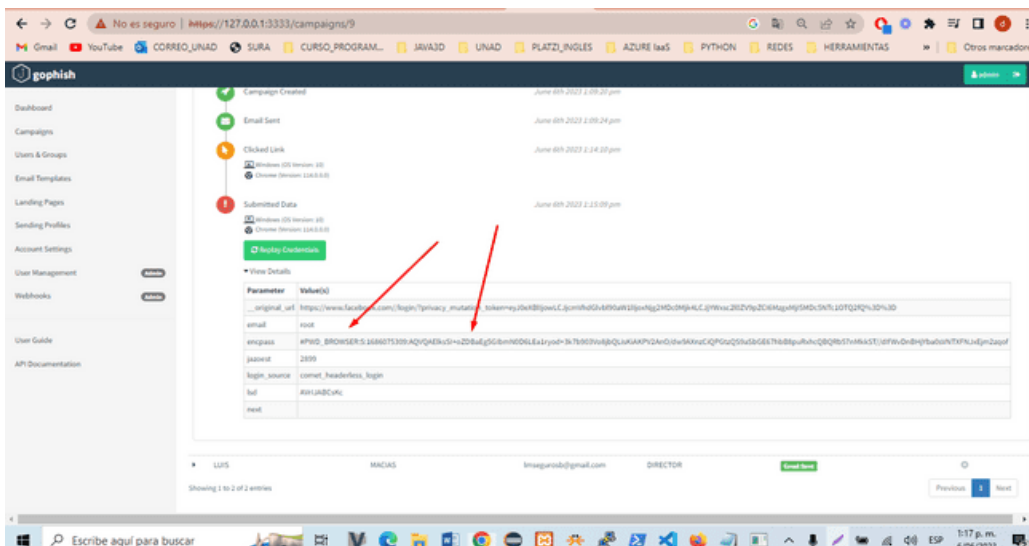
Verificación Dashboard



Nota. Verificamos en el dashboard y vemos que la víctima abrió el mensaje, le dio clic y se logueo, de esta forma esta victima nos dio las credenciales a su cuenta de Facebook

Figura 20

Insertar Credenciales de Acceso



Nota. Nos muestra el usuario y la contraseña, como en este caso es para fines educativos se muestra encriptada la contraseña

Desarrollo Objetivo 3

Recomendaciones para Mitigar Riesgos de Ingeniería Social en el Sector Financiero de Bogotá

Estar alertas ante los estafadores cuando solicitan a las víctimas que proporcionen información confidencial, como contraseñas, números de seguridad social, números de tarjetas de crédito o información bancaria. Esto se hace generalmente bajo la premisa de verificar la cuenta, solucionar un problema o recibir una recompensa falsa.

Desconfiar de los mensajes de correo a menudo contienen enlaces a sitios web falsos o archivos adjuntos que, una vez abiertos, pueden instalar malware en el dispositivo de la víctima. El malware puede robar información personal, controlar el dispositivo o permitir un acceso no autorizado.

Muchos correos electrónicos o mensajes de phishing contienen errores gramaticales, ortográficos o estructurales. Esto puede ser una señal de advertencia de que el mensaje no es legítimo, ya que las organizaciones profesionales suelen tener un nivel más alto de precisión en su comunicación.

Los ciberdelincuentes a menudo utilizan direcciones de correo electrónico o URL que se asemejan a las de organizaciones reales, pero contienen pequeñas diferencias o errores. Por ejemplo, pueden utilizar un dominio ligeramente modificado, como "g00gle.com" en lugar de "google.com".

Los correos electrónicos o mensajes de phishing a menudo contienen declaraciones urgentes o amenazas falsas para inducir a las personas a actuar rápidamente sin pensar. Pueden afirmar que hay un problema con la cuenta de la persona, que su información ha sido

comprometida o que deben tomar medidas inmediatas para evitar consecuencias negativas.

Implementar programas regulares de formación sobre concienciación en seguridad para que los empleados aprendan a identificar y responder a los ataques de ingeniería social. Estos programas deben incluir ejemplos prácticos y simulaciones de ataques.

Educar a los empleados sobre la importancia de proteger información personal, como números de teléfono y fechas de nacimiento, ya que incluso datos aparentemente inofensivos pueden ser utilizados por ciberdelincuentes para vulnerar cuentas.

Desarrollar y comunicar políticas claras sobre la gestión y protección de datos sensibles. Asegurarse de que todos los empleados comprendan y sigan estas políticas.

Implementar autenticación multifactor para todas las cuentas, añadiendo una capa extra de seguridad que dificulte el acceso no autorizado, incluso si las credenciales de inicio de sesión son comprometidas.

Utilizar autenticación adaptativa que ajuste el nivel de seguridad en función del comportamiento del usuario y el contexto del acceso, detectando y respondiendo a actividades sospechosas.

Adoptar un enfoque de seguridad de confianza cero, que asume que ninguna entidad, ya sea dentro o fuera de la red, es confiable por defecto. Esto implica verificar continuamente la identidad y el contexto de todos los intentos de acceso a los recursos de la red.

Implementar filtros antispam y pasarelas seguras de correo electrónico para bloquear correos electrónicos maliciosos antes de que lleguen a los empleados, reduciendo el riesgo de ataques de phishing

Utilizar firewalls y software antivirus actualizados para mitigar los daños causados por

atacantes que logren acceder a la red.

Mantener todos los sistemas operativos y aplicaciones actualizados con los últimos parches de seguridad para cerrar vulnerabilidades que puedan ser explotadas mediante ingeniería social.

Implementar soluciones avanzadas de detección y respuesta, como detección y respuesta de end point (EDR), que permitan a los equipos de seguridad detectar y neutralizar rápidamente amenazas que hayan logrado infiltrarse en la red.

Realizar auditorías de seguridad periódicas para evaluar la eficacia de las políticas y tecnologías implementadas.

Realizar simulaciones de ataques de ingeniería social para evaluar la preparación y la respuesta de los empleados.

Revisar y actualizar regularmente las políticas de seguridad y control de acceso para adaptarse a nuevas amenazas y tecnologías emergentes.

Como estrategia se realiza una capacitación didáctica utilizando la herramienta kahoot y se exponen diferentes conceptos, ataques, herramientas y un quiz de diferentes preguntas con el fin de llegar al objetivo que es capacitar y sensibilizar.

El objetivo de aprendizaje es reconocer y prevenir ataques de phishing Entender la importancia de las buenas prácticas de seguridad

Saber cómo enfrentar en caso de sospechar un ataque de ingeniería social.

Conclusiones

En la actualidad existe una gran variedad de herramientas de protección, que pueden ser utilizadas en base a las necesidades, la mayoría de los ataques exitosos ocurren por las malas prácticas ocasionadas internamente en la organización por los mismos colaboradores, al realizar análisis sobre los diferentes ataques, observamos que cada segundo somos atacados, la mayoría de las organizaciones en Bogotá carecen de capacitación y sensibilización sobre los diferentes ataques informáticos a los que están expuestos.

La investigación que se realizó nos muestra el impacto de la ingeniería social y como minimizarlo en las organizaciones de Bogotá con el fin de evitar pérdida de activos a causa de errores humanos, se ha identificado que las empresas con una cultura organizacional que prioriza la seguridad de la información y la formación constante de sus empleados en temas de ingeniería social presentan menos incidentes de seguridad. Esto resalta la necesidad de integrar la ciberseguridad en la cultura organizacional. Las estrategias educativas bien diseñadas y ejecutadas para la prevención de ataques de ingeniería social son efectivas para sensibilizar a los empleados sobre los riesgos y mejorar sus prácticas de seguridad. Ejercicios prácticos, como simulaciones de phishing, demostraron ser especialmente útiles.

Las recomendaciones específicas para cada empresa, basadas en un diagnóstico detallado de sus vulnerabilidades y necesidades, son esenciales para fortalecer la seguridad de la información. Una estrategia única no es suficiente dada la diversidad de estructuras y políticas internas en las organizaciones y el uso adecuado y constante de herramientas de ciberseguridad, como firewalls y sistemas de detección de intrusiones, complementado con la capacitación en ingeniería social, proporciona una defensa más robusta contra los ataques. La combinación de tecnología y educación es fundamental para una protección integral.

Referencias Bibliográficas

- Alonso, R. (2020, diciembre 10). Timo del CEO: el ciberataque con el que se roban millones haciendo una sola llamada. *ABC Redes*. Recuperado de https://www.abc.es/tecnologia/redes/abci-timo-ciberataque-roban-millones-haciendo-sola-llamada-202012090135_noticia.html
- Arias, A. (2024, abril 9). Escaneo de red: una labor del hacking ético. *Tokio School*. Recuperado de <https://www.tokioschool.com/noticias/guia-escaneo-red/>
- Axess. (2020). Ciberseguridad & Big Data: la conectividad satelital y la fábrica inteligente 4.0. Recuperado de <https://axessnet.com/ciberseguridad-big-data-la-conectividad-satelital-y-la-fabrica-inteligente-4-0/>
- Bodnar, D. (2020, octubre 29). Ingeniería social y cómo protegerse. *Avast*. Recuperado de <https://www.avast.com/es-es/c-social-engineering>
- Cancillería de Colombia. (2020). Colombia se adhiere al Convenio de Budapest contra la ciberdelincuencia. Recuperado de <https://www.cancilleria.gov.co/newsroom/news/colombia-adhiere-convenio-budapest-ciberdelincuencia>
- Cannoles, B., & Ghafarian, A. (2017). Hacking experiment by using USB Rubber Ducky scripting. *Journal of Systemics*, 15(2), 66-71. Recuperado de <http://www.iiisci.org/journal/sci/FullText.asp?var=&id=ZA340MX17>
- Casas, P. (2015, noviembre 19). El triángulo de la seguridad. *Universidad Nacional Autónoma de México*. Recuperado de <http://blogs.acatlan.unam.mx/lasc/2015/11/19/el-triangulo-de-la-seguridad/>

Cordero, W. (2018). Implementación de técnicas de ingeniería social en la Institución Técnica de Panqueba. [Tesis de especialización, Universidad Nacional Abierta y a Distancia].

Recuperado de <https://repository.unad.edu.co/handle/10596/22690>

E-systems. (2021, julio 9). Ingeniería social. *E-systems*. Recuperado de

<https://esystems.com.co/ingenieria-social-que-es/>

Educación 3.0. (2023, febrero 7). Día de la Internet segura: ¿Cómo podemos disfrutar de

Internet? *Educación 3.0*. Recuperado de

<https://www.educaciontrespuntocero.com/tecnologia/dia-de-internet-segura/>

Gil, V., & Gil, J. (2017). Seguridad informática organizacional: Un modelo de simulación

basado en dinámica de sistemas. *Scientia et Technica*, 22(2), 141-149. Recuperado de

<https://www.redalyc.org/pdf/849/84953103011.pdf>

Gómez, V. Á. (2014). *Seguridad en equipos informáticos*. RA-MA Editorial. Recuperado de

<https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/62466?page=1>

INCIBE. (2019, septiembre 5). Ingeniería social: técnicas utilizadas por los ciberdelincuentes y

cómo protegerse. *Instituto Nacional de Ciberseguridad*. Recuperado de

<https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse>

Ingeniería social: definición. (2023, abril 19). *Kaspersky*. Recuperado de

<https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering>

Jiménez, M. M. (s.f.). Vulnerabilidades que afectan la seguridad de la información. *PiraniRisk*.

Recuperado de <https://www.piranirisk.com/es/blog/vulnerabilidades-en-seguridad-de-la-informacion>

- Jones, K. S., Armstrong, M. E., Tornblad, M. K., & Namin, A. S. (2020). How social engineers use persuasion principles during phishing attacks. *Information & Computer Security*. Recuperado de <https://www.emerald.com/insight/content/doi/10.1108/ICS-07-2020-0113/full/html>
- Lisa Institute. (2020, mayo 8). Guía práctica contra la ingeniería social. Recuperado de <https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social>
- Navarrete, J. (2020, septiembre 14). Ecuador en riesgo: ciberataques. *BDO Ecuador*. Recuperado de <https://www.bdo.ec/es-ec/noticias/2020/ecuador-en-riesgo-ciberataques>
- Nelson, B. (2021, enero 20). ¿Qué es la ingeniería social? ¿Está usted en riesgo? *AVG*. Recuperado de <https://www.avg.com/es/signal/what-is-social-engineering>
- Paredes, A. R. Z., Quevedo, I. M. S., & Chalacán, L. J. M. (2020). Seguridad informática en las PyMES de la ciudad de Quevedo. *Journal of Business and Entrepreneurial Studies*, 4(2), 97-109. <https://doi.org/10.37956/jbes.v4i2.97>
- Petrosyan, K. (2022, febrero 28). Guía completa sobre la ingeniería social. *Platzi*. Recuperado de <https://platzi.com/clases/223-ingenieria-social/37094-taxonomia-de-los-ataques/>
- Portafolio. (2021). Bancos aumentaron en un 64% gastos de ciberseguridad. Recuperado de <https://www.portafolio.co/economia/finanzas/bancos-aumentaron-64-gastos-en-ciberseguridad-553594>
- Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, 12(12), 6042. <https://doi.org/10.3390/app12126042>

Szczepaniuk, E., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. *Computers and Security*, 90, 101709.

<https://doi.org/10.1016/j.cose.2019.101709>

TechTarget. (2021). Autenticación multifactor o MFA. Recuperado de

<https://searchdatacenter.techtarget.com/es/definicion/Autenticacion-multifactor-MFA>

Tyutyunnik, A., & Lazarev, A. (2021, septiembre). Intelligent system for preventing Rubber Ducky attacks using deep learning neural networks. *In 2021 International Russian Automation Conference (RusAutoCon)* (pp. 497-502). IEEE.

Apéndice

Apéndice A

Estrategia que se debe Implementar para Prevenir Ataques de Ingeniería Social.

Kahoot

Link de Acceso a Capacitación Didáctica

https://kahoot.it/challenge/04295146?challenge-id=db725fb1-b7cd-455a-83ad-12646fbf8b25_1688681154781

Apéndice B

Módulo 1

Figura 21

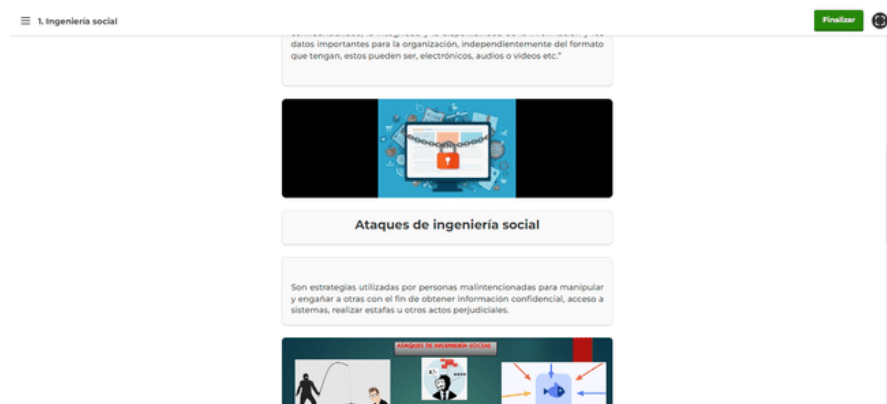
Creación de Curso



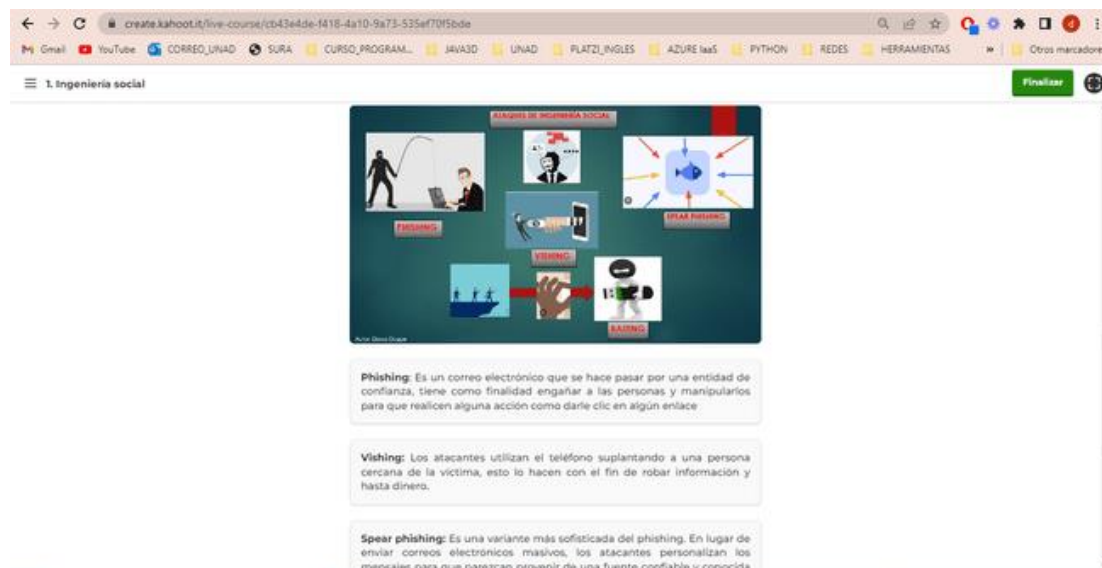
Nota. Se crea plantilla

Figura 22*Conceptos*

Nota. Conceptos norma iso 27001

Figura 23*Ataques*

Nota. Se despliegan los ataques más comunes

Figura 24*Estudio de Ataques ingeniería Social*

Nota. Definición conceptos phishing, vishing, spear phishing

Figura 25*Que es Ingeniería Social*

Fuente video. ComputerHoy.com [@Computerhoycom]. (2022, diciembre 9). ¿Sabes qué es INGENIERÍA SOCIAL?

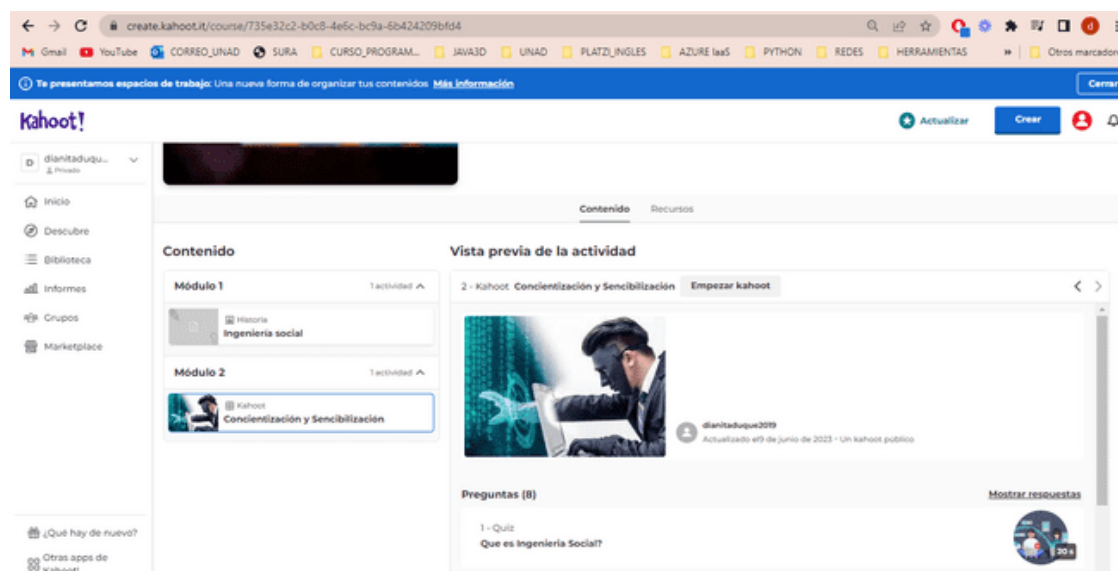
Youtube. <https://www.youtube.com/watch?v=PN0j35dbG-8>

Apéndice C

Modulo 2

Figura 26

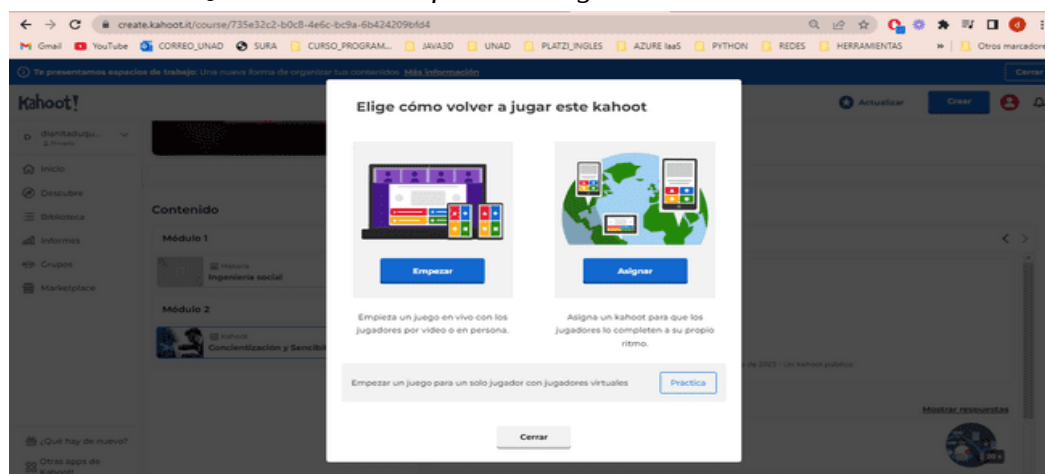
Preguntas Didácticas



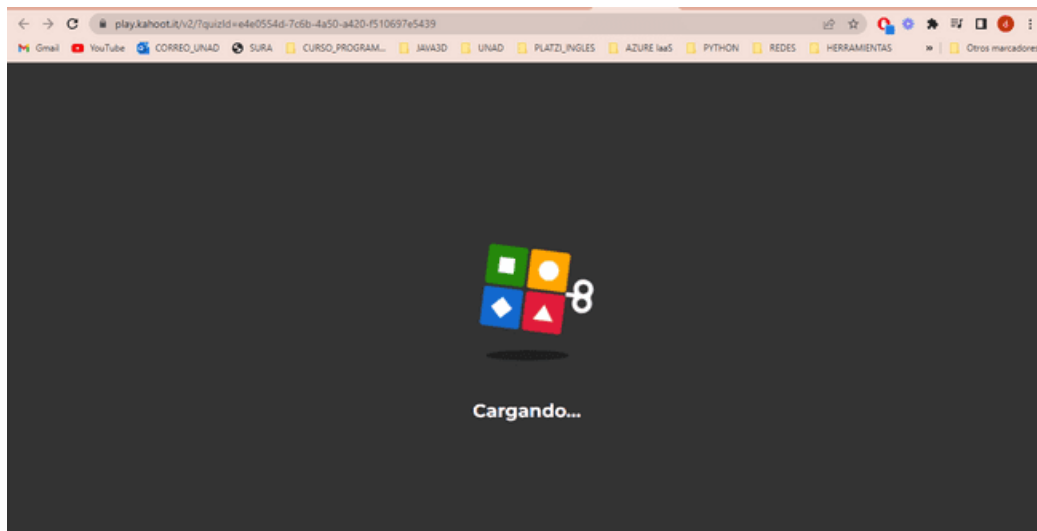
Nota. Vista previa de la actividad

Figura 27

Se Realiza un Quiz Didáctico Enfocado a Ingeniería Social



Nota: Con la herramienta kahoot iniciamos el quiz didáctico

Figura 28*Inicio Juego*

Nota. Al dar clic en empezar carga el inicio

Figura 29*Modo Inicio de Juego*

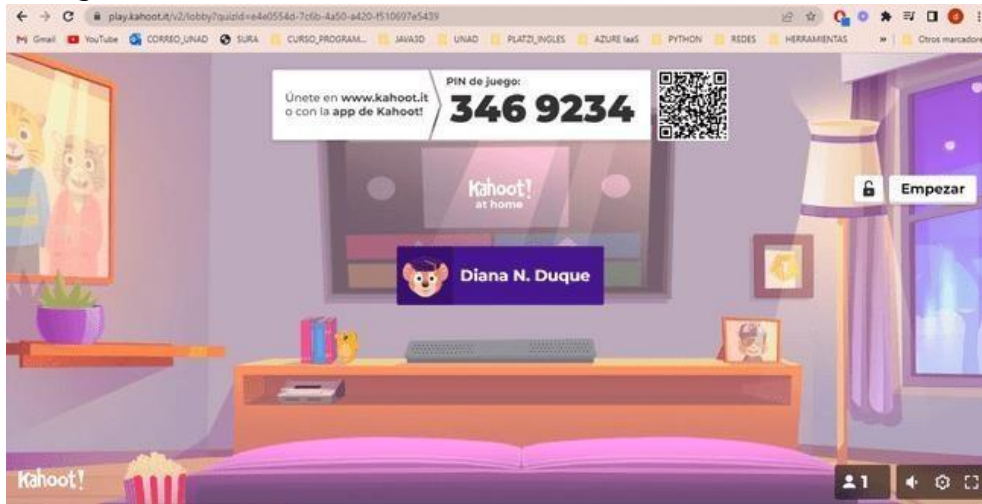
Nota. Seleccionamos alguno de los modos

Figura 30*Preparando Juego*

Nota. Nos preparamos para unirnos

Figura 31*Código Acceso a Juego*

Nota. Ingresamos el pin o escaneamos el Qr en nuestro dispositivo móvil.

Figura 32*Se Loguean*

Nota. Al scanner el Qr, nos logueamos con el nombre para iniciar

Figura 33*Pregunta 1*

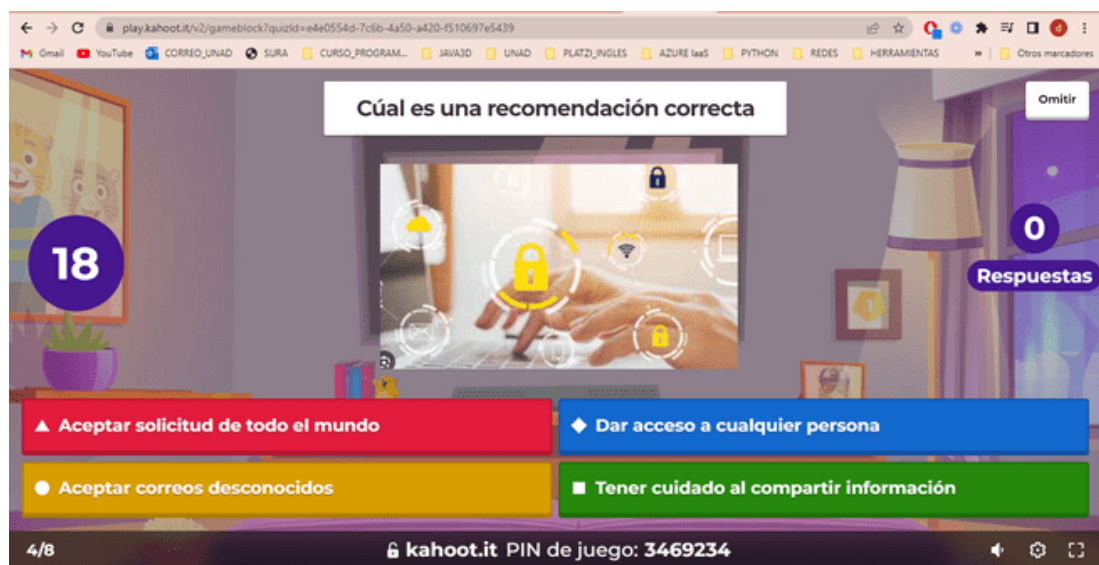
Nota. Quiz

Figura 34*Pregunta 2*

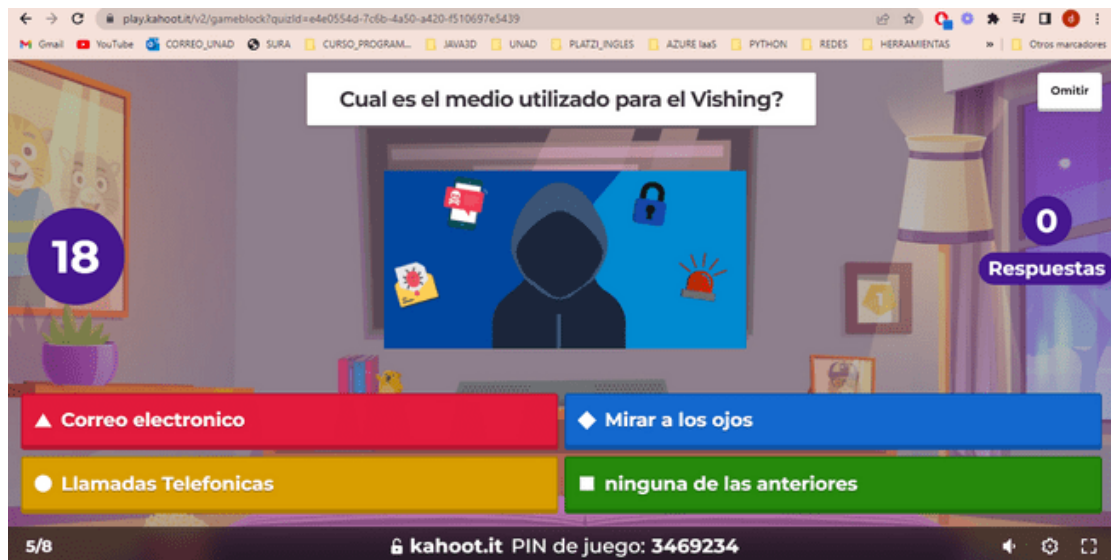
Nota. Pregunta 2

Figura 35*Pregunta 3*

Nota. Pregunta 3

Figura 36**Pregunta 4**

Nota. Pregunta 4

Figura 37**Pregunta 5**

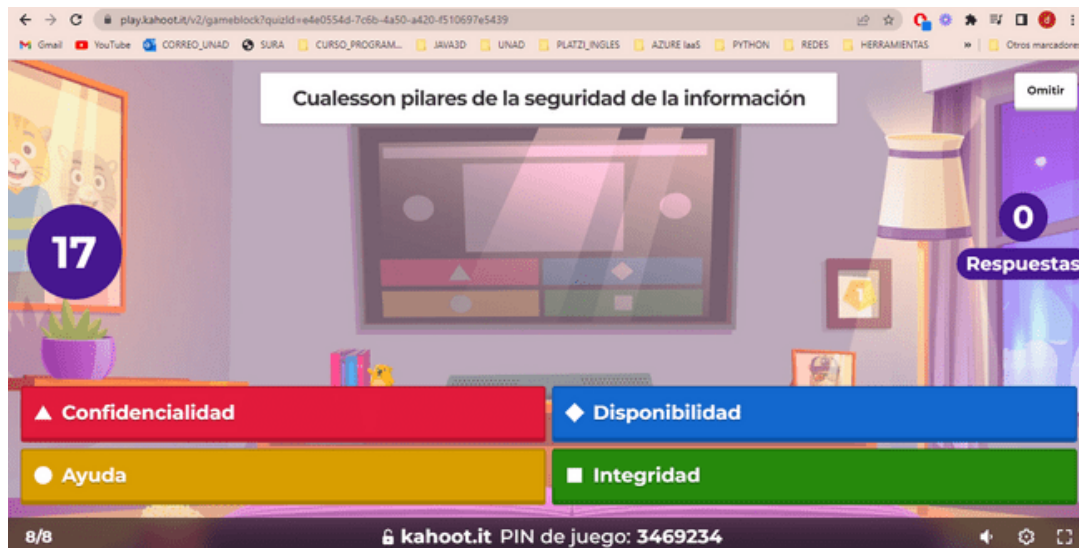
Nota. Pregunta 5

Figura 38*Pregunta 6*

Nota. Pregunta 6

Figura 39*Pregunta 7*

Nota. Pregunta 7

Figura 40*Pregunta 8*

Nota. Pregunta 8

Figura 41*Finaliza*

Nota. Concientización y Sencibilización

Resumen Analítica Especializado -RAE

Fecha de Realización	26/09/2024
Programa	Especialización Seguridad Informática
Línea de Investigación	Infraestructura Tecnológica y Seguridad en Redes
Título	Estrategia para la prevención de ataques de ingeniería social en las empresas del sector financiero en la ciudad de Bogotá
Autor(es)	Duque Gallego Diana Norela
Palabras Claves	Ataques informáticos, ingeniería social, seguridad de la información, ciberseguridad.
Descripción	Esta monografía centra su importancia en el estudio de las amenazas cibernéticas a las que se ven enfrentadas frecuentemente las entidades financieras en la ciudad de Bogotá, estas se dan desde la práctica de la ingeniería social. Este tipo de amenaza son muy peligrosas ya que desde allí se puede explorar la vulnerabilidad de los seres humanos. La ingeniería social se relaciona estrictamente con las técnicas de manipulación tecnológicas, donde se busca engañar de una manera psicológica desde el robo de información personal o empresarial, donde por medio de diferentes acciones se roban mucha información no solo personal si no confidencial de las empresas, involucrando así la seguridad de las organizaciones, dichas tácticas pueden tener una serie de estrategias y técnicas que pueden ser adaptadas las características del objetivo. En la ciudad de Bogotá, hay diferentes entidades financieras que se han visto particularmente vulneradas con las tácticas de robo de información,

estas dan como resultado alto robos de información, extorsiones y manipulación de todo el sistema. Esta monografía resalta la falta de cultura organizacional que centra en el interés de la seguridad y la falta de conciencia en los directivos y empleados que dejan brechas significativas en las tecnologías de seguridad.

Contenido del documento:

Planteamiento del Problema Justificación
Objetivos: General y Específicos
Marco referencial Marco conceptual Marco Teórico
Marco Legal
Desarrollo Objetivo 1 Metodología Desarrollo
Objetivo 2 Estrategia Desarrollo Objetivo 3
Recomendaciones
Conclusiones

Marco Metodológico:

Para el desarrollo de este trabajo, se ha seleccionado la norma NIST SP 800-53 organiza los controles de seguridad y privacidad que se pueden implementar en las organizaciones financieras para proteger sus sistemas de información. Estos controles están organizados en familias (Como control de acceso, auditorias, responsabilidad).

Conceptos adquiridos	En base al desarrollo del trabajo he comprendido varios ⁸⁵ conceptos entre los que se encuentran, segmentación de redes, gestionar políticas de seguridad, autenticación
	multifactorial, utilizar software para detección de amenazas como IDS/IPS, culturizar y realizar simulacros.
Conclusiones	En la actualidad existe una gran variedad de herramientas de protección, que pueden ser utilizadas en base a las necesidades, la mayoría de los ataques exitosos ocurren por las malas prácticas ocasionadas internamente en la organización por los mismos colaboradores, al realizar análisis sobre los diferentes ataques, observamos que cada segundo somos atacados, la mayoría de las organizaciones en Bogotá carecen de capacitación y sensibilización sobre los diferentes ataques informáticos a los que están expuestos. La investigación que se realizó nos muestra el impacto de la ingeniería social y como minimizarlo en las organizaciones de Bogotá con el fin de evitar perdida de activos a causa de errores humanos, se ha identificado que las empresas con una cultura organizacional que prioriza la seguridad de la información y la formación constante de sus empleados en temas de ingeniería social presentan menos incidentes de seguridad. Esto resalta la necesidad de integrar la ciberseguridad en la cultura organizacional. Las estrategias educativas bien diseñadas y ejecutadas para la prevención de ataques de ingeniería social son efectivas para sensibilizar a los empleados sobre los riesgos y mejorar sus prácticas de seguridad. Ejercicios prácticos, como simulaciones de phishing, demostraron ser especialmente útiles.

Nota: Cuadro realizado por autoría propia