Análisis de metodologías para la gestión de la ciberseguridad y la gestión de riesgos relacionados con ingeniería social en empresas del sector privado

Andrea Alejandra Cortes Angarita

Asesor

Ing. Edgar M. López Rojas

Universidad Nacional Abierta y a Distancia UNAD

Escuela Ciencias de la Educación ECBTI

Especialización en Seguridad Informática

2024

Resumen

La creciente pérdida de datos y los ciberataques en la actualidad nos llevan a enfocarnos en la desinformación de las personas para poder proteger los datos y adoptar buenas prácticas en su día a día en la era digital. Esto nos lleva a uno de los ataques cibernéticos más significativos: la ingeniería social, este proyecto se realiza con el propósito de presentar un estudio monográfico como proyecto de grado, en el cual se analizará la ingeniería social y los riesgos de la seguridad informática. Se validará información valiosa a través de fuentes documentales para justificar y proponer una solución al problema en cuestión. En este documento se mostrará cómo Para identificar vulnerabilidades y riesgos relacionados con la ingeniería social, es esencial implementar buenas prácticas que permitan detectar y contener brechas de seguridad en las empresas del sector privado. Se recomienda establecer controles de seguridad y estrategias basadas en políticas y buenas prácticas, entre otras medidas. Se intentará proporcionar un documento que sea fácil de describir y entender para aquellos con poco conocimiento en el área informática. Por ello, también se incluirá el análisis de conceptos importantes para un mejor manejo del tema, para este desarrollo nos basaremos en identificar los controles aplicados por las organizaciones de sector privado, que permitirían mitigar el riesgo y en la capacitación que se le puede dar a las personas para que tengan más conocimiento de ciberseguridad, como resultado de los diferentes análisis realizados frente a controles y vulnerabilidades, se darán recomendaciones que aplican para las entidades de sector privado.

Palabras clave: Ciberataques, Seguridad informática, Controles, ingeniería social.

Abstract

The growing data loss and cyberattacks today lead us to focus on people's misinformation in order to protect data and adopt good practices in their daily lives in the digital age. This brings us to one of the most significant cyber attacks: social engineering. This project is carried out with the purpose of presenting a monographic study as a degree project, in which social engineering and computer security risks will be analyzed. Valuable information will be validated through documentary sources to justify and propose a solution to the problem in question. This document will show how to identify vulnerabilities and risks related to social engineering, it is essential to implement good practices that allow detecting and containing security gaps in private sector companies. It is recommended to establish security controls and strategies based on policies and good practices, among other measures. An attempt will be made to provide a document that is easy to describe and understand for those with little knowledge in the computer area. For this reason, the analysis of important concepts will also be included for better management of the issue. For this development we will base ourselves on identifying the controls applied by private sector organizations, which would allow the risk to be mitigated, and on the training that can be given to people so that they have more knowledge of cybersecurity, as a result of the different analyzes carried out against controls and vulnerabilities, recommendations will be given that apply to private sector entities.

Keywords: Cyberattacks, Information security, Controls, Social engineering.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Introducción

Se identifican que muchas personas y empresas son víctimas de ataques cibernéticos, en su mayoría ingeniería social, en cuanto pasa el tiempo la tecnología y los sistemas informáticos se hacen más necesarios para poder tener una vida cibernética segura, sin embargo; existen muchos problemas gracias al desconocimiento y los pocos controles de seguridad que se pueden manejar, los ataques cibernéticos se han convertido en un riesgo significativo para la privacidad de personas y empresas. Como sabemos, el internet es un medio vasto y esencial para la vida virtual, el trabajo, la educación, las redes sociales y cualquier tipo de interacción virtual, por esto toda lo que se realiza en internet debería ser privado para cada uno de nosotros, los ciberdelincuentes pudieran obtener nuestra información, como dirección, números de teléfono, documento, números de tarjetas de crédito débito, aún pueden ver todo el tráfico de nuestra red. Esto significa que pueden ver a qué páginas entramos, lo que digitamos, nuestras claves de usuario o los mensajes que enviamos a otras personas. Todo esto ocurre si no se tiene el conocimiento mínimo de los riesgos y cuidados que se deben tener al usar internet.

Esta monografía se desarrollará a partir del estudio del conocimiento actual sobre los ataques de ingeniería social en las empresas del sector privado en Colombia, en el primer objetivo se identificaran las debilidades que causan los riesgos principales al realizar alguna actividad en el ciberespacio, en el segundo objetivo veremos cuales son los principales ataques de ingeniería social y cómo podemos contrarrestar los riesgos dando algunos consejos o pautas de buenas prácticas de seguridad tanto en empresas como para personas, en el tercer objetivo, presentamos un análisis de la evaluación de los déficits en la capacitación y enseñanza sobre ciberseguridad y el conocimiento de la ingeniería social.

A partir de lo anterior, se llega a generar el siguiente interrogante: ¿Cómo evitar ser víctima de ingeniería social?

Finalmente se dará el desarrollo de cada uno de los objetivos y problemáticas con conclusiones precisas para poder aplicarlas

Justificación

El desarrollo de la presente investigación permite evidenciar lo poderoso que es, o puede llegar a ser, el ataque de ingeniería social y lo vulnerables que están la ciudadanía y empresas frente a el ciberespacio, para que esto no siga sucediendo se requiere de buenas prácticas y de un conocimiento básico de cómo manejar ataques cibernéticos. Se está evidenciando lo desatendida que puede llegar a estar la ciberseguridad en las empresas, universidades o a nivel general que ha generado diferentes riesgos asociados a la seguridad de los datos sensibles.

Con esta investigación podemos tener varios beneficios del estudio para contextos específicos en cuanto a la seguridad de datos, no solo personales si no empresariales, se entenderán nuevas prácticas que nos sirven a todos, no solo en la vida personal sino también en la laboral, evitando los ataques más frecuentes en ingeniería social. La utilidad para la comunidad permitirá tener aportes a futuro en nuevos estudios e investigaciones, ya sea con propuestas de análisis o con la resolución definitiva de un problema de investigación.

Gracias a esta investigación podemos tener la justificación desde un punto de vista donde se aplica a las investigaciones que desarrollan nuevos mecanismos o procedimientos metodológicos útiles a otras investigaciones de la universidad y, de nosotros como estudiantes madurando en conocimientos, promoviendo la concientización adaptando nuevos conocimientos y prácticas de ciberseguridad.

Objetivos

Objetivo General

Análisis de las metodologías para la gestión de la ciberseguridad y la gestión de riesgos relacionados con la ingeniería social, a partir de una revisión bibliográfica y técnica, para mejorar los niveles de seguridad en las empresas del sector privado de Colombia.

Objetivos Específicos

Identificar las vulnerabilidades, amenazas y riesgos asociados con la ingeniería social mediante el análisis de diferentes tipos de ataques, respaldados por estadísticas, con el fin de determinar los riesgos más comunes a las empresas del sector privado.

Observar las buenas prácticas de seguridad identificando posibles brechas relacionadas con la ingeniería social, con el objetivo de formular recomendaciones adecuadas para las empresas del sector privado.

Seleccionar controles de seguridad recomendados según las mejores prácticas, orientados a la reducción de los riesgos relacionados con la ingeniería social.

Proponer estrategias para contrarrestar la ingeniería social que fortalezcan las capacidades del talento humano en las empresas del sector privado.

Marco Referencial

Marco Teórico

Se ha evidenciado que muchas empresas y personas no son ajenas al mundo digital, pero tampoco tienen la experiencia o el conocimiento de los múltiples ataques que son comunes en la actualidad, por lo cual caen en estafas o trampas de los ciberdelincuentes, para poder proteger nuestro activos se requiere de los tres principios más importantes de la ciberseguridad los cuales son: confidencialidad, disponibilidad, integridad y una de las ultimas que se llama no repudio, estos se deben de entender y usar para poder tener un nivel de seguridad mínimo , para esto también se tocaran diferentes significados de interés para poder proceder.

Marco Conceptual

Cibercrimen

¿Qué es el ciberdelito? Argentina.gob.ar. Published April 27, 2020. Señala que "las conductas abusivas o no aptas de los cibernéticos, en ello se identifican personas que filtran o roban información, se hacen pasar por personas que no son robando identidades, hacen fraudes, estafas, secuestro de información entre otros afectando aun la reputación de la persona, el principal interés de los ciberdelincuentes es económico, o sus ganancias".

Ciberespacio

StackPath. 2015. Señala que "Es un espacio a el cual todos tenemos derecho donde se pueden interconectar varias redes para poder interactuar en línea, aunque o es físico nos permite conectar medios físicos de forma virtual y poder generar conexiones"

Identidad 2.0

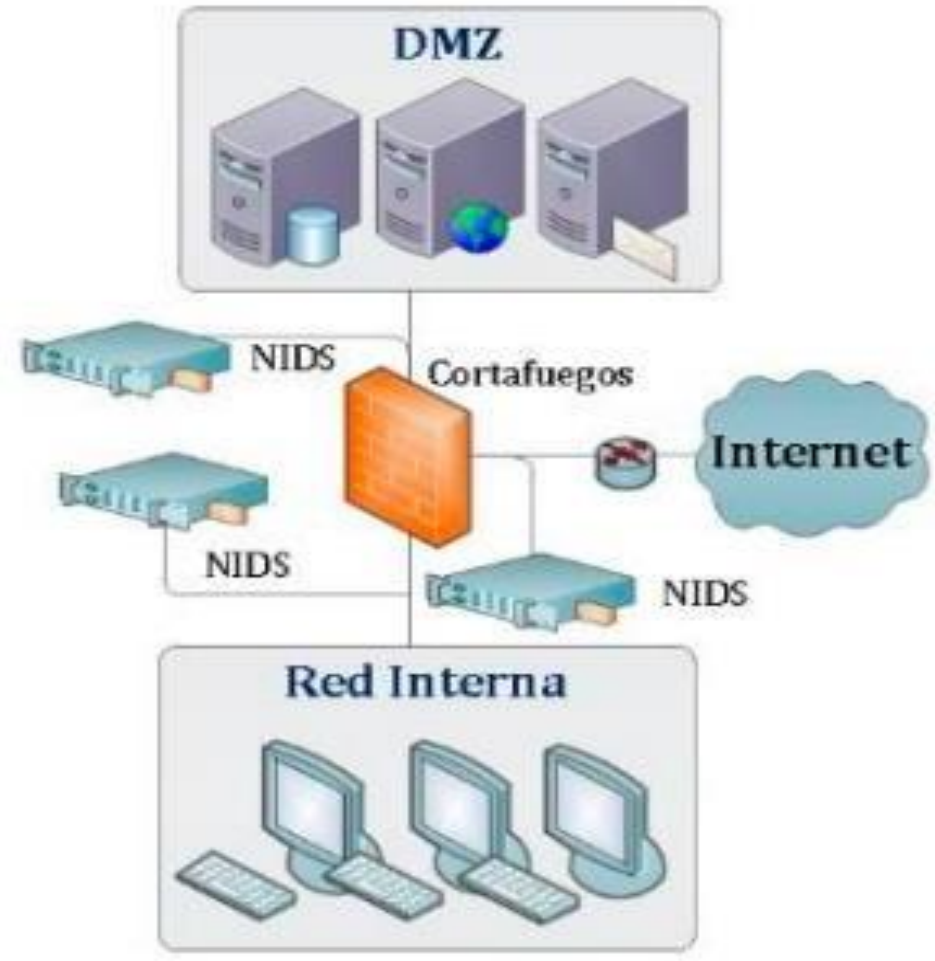
¿Qué es la Identidad digital? las TIC 2016. Señala que: "Es la identidad digital, es como nuestra cedula o nuestros antecedentes que nos identifican como usuarios de internet, todo lo que

hacemos en internet deja una huella o un rastro, proteger esta identidad es clave para nuestra seguridad y privacidad de datos”

Hay una herramienta llamada DNI electrónico el cual nos permite acreditar nuestra identidad 2.0 en el momento de realizar trámites administrativos en internet, se firman documentos, el costo de este es de $30 dólares al cambio de peso colombiano,

Figura 1

Seguridad en la Red



Nota. Esta imagen muestra una infraestructura con una zona desmilitarizada donde se tiene el servidor web, correo electrónico y hotpot. Tomado de. (2024). Upm.Es. Retrieved April 8, 2024, from http://www.criptored.upm.es/intypedia/docs/es/video5/DiapositivasIntypedia005.pdf

SaaS

SaaS, o "Software como Servicio", es un modelo de entrega de software en el que las aplicaciones se encuentran en la nube y se acceden a través de Internet, evitando la necesidad de instalarlas en dispositivos locales. Los usuarios utilizan un navegador web para acceder a estas aplicaciones.

Seguridad en la Red

Los Riesgos en Redes Sociales, Parte II. Unad.edu.co. 2019. Señala que: “Sabemos que las redes son el camino o la ruta que toman los datos para poder llegar a su destino, por lo tanto, es importante tener algún control de que lo que se envié llegue a donde es, ya que muchos intrusos pueden sacar información desviarla o dañarla desde allí Existen muchos controles de los cuales también se combinan con el hardware antivirus, firewall, un IDS o sistema de detección de intruso y el uso de redes VPN, GIDT - Seguridad Información”.

Seguridad de Hardware

Los equipos físicos son cruciales para la ciberseguridad, ya que controlan el acceso a información sensible. Si estos dispositivos carecen de seguridad adecuada, es esencial verificar problemas eléctricos, la presencia de detectores de temperatura, ventiladores y sistemas de acceso como autenticación de dos factores o biometría. Esto ayuda a identificar vulnerabilidades y prevenir accesos no autorizados a nuestros datos.

Seguridad de Software

Seguridad g m 2016. Señala que: “El software abarca todas las aplicaciones que tenemos en nuestro equipo físico. Dado que no tenemos una visión completa del espectro de internet, es posible que, a través de una descarga incorrecta o de publicidad engañosa, pongamos en riesgo

nuestras aplicaciones o nuestros datos. Existen varias formas de aumentar la seguridad, como el uso de antivirus, autenticación, claves encriptadas, doble factor de autenticación y firewall.”

Seguridad Adicional

Adicional a las importantes nombradas anteriormente también podemos estar un paso adelante para que no perder nuestra valiosa información:

- Realizar back up
- Contraseñas difíciles
- Bloqueo automático del computador después de un tiempo determinado
- Programar que después de un tiempo determinado se elimine el historial del navegador.
- No descargar nada de páginas no autorizadas
- No confiar en nadie, no ceder accesos físicos ni lógicos a nadie
- Validar los proxys autorizados de navegación.

Como Protegerse de los Ataques Cibernéticos

Para comenzar, es fundamental profundizar en cómo protegerse y evitar caer en un ataque cibernético. De acuerdo con El Mundo Cambio (2024) Señala que: “En Colombia se registraron miles de ataques de ingeniería social, posicionando al país como el tercero con más ataques de este tipo”. Esto evidencia nuestra vulnerabilidad a ser manipulados psicológicamente, permitiendo que se obtenga información confidencial de manera sencilla. Los sectores más afectados son las telecomunicaciones y las finanzas, donde tanto empresas como ciudadanos enfrentan crecientes riesgos de suplantación de identidad, robo de datos y fraudes. Además, la acelerada transformación digital del país se ha convertido en un blanco atractivo para estos

ciberataques, ya que se basan en explotar vulnerabilidades humanas, no técnicas. Esto subraya la necesidad de mejorar nuestra educación en ciberseguridad.

Home Office

De acuerdo a Jaimovich, D. (2021), “Se ha identificado que la mayoría de las empresas no cuentan con esquemas de ciberseguridad robustos para poder manejar de lleno el trabajo home office”. El cibercrimen es cada vez más inteligente y especializado. El primer riesgo empresarial global, De acuerdo con Semana (2024), incluye: “Los ataques de ransomware, el riesgo de la interrupción de negocios, las catástrofes naturales (que pasaron del sexto al tercer lugar), e incendios y explosiones (que escalaron del décimo al octavo puesto)”. Los ciberdelincuentes hoy más que nunca esperan maniobrar cualquier ataque, usando nuevas tecnologías, como las inteligencias artificiales generativas (IA), para automatizar y acelerar estos, creando amenazas de programas malignos, métodos de ingeniería social, bases de datos y phishing más eficaces.

Ataques más Comunes

Cerca del 90% de los ciberataques son por ingeniería social, esto es cuando los ciber atacantes quieren suplantar identidades, falsificar correos, y más formas donde logran engañar a las personas.

Algunos de los más comunes son los siguientes:

- Correos Fraudulentos Personalizados, (Spear Phishing).
- Suplantación de identidad.
- Enmascaramiento de correos Spoofing.
- Infección de sitios frecuentemente visitados por empleados (Watering Hole).

Caso 1, Vishing.

Nueva Estafa que Aprovecha el Teletrabajo. El objetivo de esta forma de ataque se centraliza en los empleados fuera de sus oficinas. Esta es una mezcla de voz y phishing lo que hace es buscar que el empleado dé información sensible de sí mismo y de la empresa a través de una conversación telefónica. Lo que hacen los atacantes es hacerse pasar por un superior del empleado ejemplo departamentos de finanzas, recursos humanos o cualquier otro que sea de mayor cargo, aprovechándose con técnicas de ingeniería social para engañar a las personas y tener acceso a datos personales como teléfonos contraseñas, servicios etc., esto lo hacen para tener beneficios económicos, data sensible para manipular, o aun instalar malware en sus equipos.

Caso 2, Phishing

Promoción Panini por WhatsApp una Estafa. A través de las redes se ha evidenciado que usuarios han reportado una estafa que anda circulando por WhatsApp donde ofrece el álbum panini con 400 láminas, lideres de seguridad informática en el mundo han confirmado que es una estafa real, cuando las personas reciben este mensaje, se les pide ingresar a un enlace que las redirecciona a páginas de sorteos o de apuestas deportivas. Aunque este enlace no descarga ningún malware, la estafa ya se ha consumado, ya que la persona ha entregado información y datos sensibles al atacante. Cabe recordar que las páginas de apuestas también ganan dinero por cada persona que se registre, lo cual constituye otro tipo de fraude, ya que la persona se registra en la página esperando obtener su premio.

Caso 3, Tailgaiting

Solidaridad y Buena Voluntad. Este ataque se ejecuta cuando un empleado está ingresando a su empresa, portando un carnet, tarjetas o algún otro acceso, el atacante con una

bonita actitud llega corriendo, saludando y “colándose” como si se le hubiera quedado su tarjeta de acceso o no la quisiera sacar de su bolsillo o como si fuera un empleado más, así adquiriendo el acceso que para él no era permitido para poder robar información y filtrarse en las empresas.

Sistema de Control de Accesos

Un sistema de control de acceso es un sistema eléctrico que permite o impide el ingreso a un lugar, lo que esto hace es validar la identificación por medio de tipos de lectura y sus dos clases los cuales son:

- Clave por teclado
- Tags de proximidad
- Biometría

Autónomos. Permite tener el control de una o más puerta sin tener necesidad de estar en el PC, por ello no guarda tampoco registros de accesos, dependiendo de la marca hay unos que son más sencillos y solo usan una “llave electrónica”, las cuales pueden ser clave, proximidad o biometría.

Acceso en Red. En 2020, Arias a concluido que: “El Acceso de red si se manejan de manera remota o desde el pc, donde se hace uso de un software de control de acceso, por lo cual su lleva registro de todas las operaciones realizadas sobre el sistema, con datos como fecha, hora etc”.

Clasificación de Hackers

Black Hackers. Son personas muy hábiles que introducen en las redes, pero para robar información dañar programas o páginas, la motivación de estos es dinero, venganza o simplemente dañar la reputación de una persona empresa o nombre.

Normalmente ellos indican como “script kiddies” que son las personas novatas aficionadas que quieren encontrar vulnerabilidades con herramientas que han comprado a otros, algunos han sido capacitados de alguien para el que trabajan, estos hackers tienen un conocimiento muy amplio son personas expertas.

Muchos de ellos tienen también una especialidad ejemplo phishing o puede ser herramientas de acceso remoto, algunos trabajan a través de contratos temporales, y unos otros si por sí mismos aun con ventas por la web oscura de kits los cuales les permiten ganar bastante dinero.

White Hackers. Son también llamados hackers éticos son lo opuesto del sombrero negro, son personas con buenos conocimientos que buscan vulnerabilidades de una empresa para que el sombrero negro no pueda afectarla, ellos detectan problemas de seguridad y ayudan a las organizaciones a encontrar la solución, existe un pequeño grupo de hackers de sombrero blanco que realizan “pruebas de penetración”. Estas pruebas buscan identificar puntos débiles para determinar qué tan vulnerable es el sistema.

Cracker. Igualmente son personas hábiles con conocimientos amplios que como su nombre lo dice rompen, esto quiere decir que rompen o vulneran un sistema de seguridad sin tener permiso para ello, a diferencia del sombrero negro estas personas hacen esto por varias razones, por dinero, por protesta, por aprender más, por desafiarse, adicional normalmente su ataque se guía más a ejecutables binarios, sobre los sistemas operativos desactualizados.

Prehacker. Se trata de personas que se dedican a aprender sobre el funcionamiento de teléfonos de diferentes marcas, tecnologías de telecomunicaciones y redes telefónicas. Algunas de estas personas también realizan actividades no autorizadas, como la construcción de dispositivos que interceptan llamadas, y comparten planos y componentes en internet. Su

principal desafío suele ser resolver problemas complejos relacionados con incidentes de seguridad o fallas en los sistemas.

Lammers. Son personas que dicen saber cosas, dicen tener respectivos conocimientos en informática y realmente no saben nada, son ignorantes al tema o tiene falta de capacidades, adicional a esto estas personas tampoco tiene intención de aprender, Estas personas son llamadas Lammers por otras personas que en realidad si saben del tema y se dan cuenta que en realidad ellos no tienen la experticia o conocimiento.

Hacker. Es una persona que descubre vulnerabilidades de un sistema, equipo o información. La motivación de ellos puede ser con fines de lucro, protesta o también para desafiarse. Estos se dividen en varios tipos y son personas con conocimientos en informática; a veces también saben desarrollar.

Impacto de Cibercrimen

Los resultados de Maurer, T., & Nelson, A. (2021) indican que “Estas amenazas afectan la economía mundial ya que el robo de datos, el costo de las nuevas implementaciones y la recuperación de una caída de estatus con el que queda una empresa la cual fue víctima de ciberataques. El uso y la implementación de nuevas tecnologías con accesos lógicos modernos nos da a pensar que en el futuro no se usarán contraseñas, se tendrán accesos más sofisticados para poder reforzar la seguridad en las redes”.

Riesgos del Cibercrimen

Los riesgos normalmente son por la falta de conocimiento sobre los riesgos que se encuentran en la red es la principal causa de los problemas informáticos, las personas tienen desconocimiento o a veces hacen caso omiso a las recomendaciones o advertencias, cuando se

siguen algunas series de conductas que los convierte en víctimas de los ataques, es posible ser víctima ya que se pierde la privacidad que debe tener la información, estos son algunos riesgos:

- No tener copias de seguridad
- No tener equipos actualizados o con antivirus
- Colocar claves de seguridad muy fáciles
- Ingresar a páginas que no son seguras o recomendadas
- Compartir información con desconocidos por llamadas telefónicas o mensajes de texto
- Ingresar a enlace sospechosos o desde correos sospechosos o desconocidos.
- Creer en promociones o regalos muy buenos solo dando un clic.

Marco Histórico

Inicios

Lo primero será, aclarar nuevamente cual es la diferencia entre un hacker de un ciberdelincuente (o cracker) para evitar confusiones. Un hacker es una persona que investiga los sistemas para detectar fallos y mejorarlos, por lo contrario, un cracker busca esos mismos fallos para dañar robar u obtener algún beneficio.

El primer hacker de la historia fue el mago Nevil Maskelyne, que en 1903 logró interceptar la primera transmisión del telégrafo inalámbrico.

El primer ciberdelincuente (o cracker) de la historia fue John Draper, también conocido como «Captain Crunch», quien recibió ese nombre porque descubrió que modificando un silbato que se regalaba en las cajas de cereales «Cap’n Crunch» emitía un tono a 2600 Hz con el que se podía engañar a la central telefónica y realizar llamadas gratis.

En los mismos inicios de la informática aparecieron los primeros ciberdelincuentes y el malware. A principios de los años 70 apareció Creeper, el primer malware, este llegaba a las computadoras por medio del internet que se manejaba en ese momento llamado ARPANET era un autoejecutable que al ejecutarse mostraba un mensaje que decía «I'm the Creeper, catch me if you can!», por causa de los daños de este malware, se creó el primer antivirus llamado Reaper, el cual se manejaba siendo otro virus que se propagaba a través de la red en busca de computadoras infectadas con Creeper para eliminarlo, gracias a la actualización y evolución de las tecnologías , la existencia de más aplicaciones de más uso del IoT se generaban también más riesgos de seguridad.

Ahora seguimos en la historia de los años 80 se produjo una revolución de programa maligno ya que ha evolucionado a medida que también evolucionan los antivirus, por lo cual no es muy seguro aun solamente el uso del antivirus.

Entidades

Así como avanza la tecnología también se crean ayudas de expertos competentes para poder manejar estos problemas o temas:

La MINTIC ayuda capacita y promueve el acceso, uso efectivo de las TIC, a través de políticas y programas, para mejorar la calidad de vida de cada colombiano y el crecimiento del desarrollo del país, por esto podemos acceder a programas y capacitaciones virtuales o presenciales, muchas de ellas gratuitas.

EL ColCERT buscan mejorar los procesos de seguridad de la infraestructura tecnológica, así ayuda a prevenir incidentes de seguridad digital, reduciendo el impacto cuando estos lleguen a ocurrir.

Estado Actual

En el año 2022 se pudo identificar diversos ataques en su mayoría de ingeniería social, aunque la ciberseguridad ha sido más rigurosa en parte debido al COVID-19 los trabajos remotos y la explosión de uso de herramientas virtuales.

Se evidencia la necesidad de implementar soluciones de seguridad para abordar riesgos y vulnerabilidades en activos de información. Aunque ha habido un aumento en la conciencia sobre este tema, persiste la escasez de personal capacitado en ciberseguridad, lo que subraya la importancia de contar con profesionales formados en el área. Con el crecimiento del comercio electrónico, especialmente durante eventos como el día sin IVA, las ventas han aumentado significativamente, alcanzando $12.2 billones en 2022, un 130% más que en 2020. Este auge en las compras online ha llevado a un uso intensivo de pagos digitales, lo que resalta la creciente demanda de seguridad digital. Actualmente, se registran alrededor de 160 incidentes de ciberseguridad, siendo el phishing el más común.

La ingeniería social es uno de los principales tipos de ataques. Muchos de estos se combinan con phishing, vishing, entre otros, y afectan tanto a los ciudadanos como a las empresas.

Figura 2

Incidentes Tiempo Real

Nota. Esta imagen muestra aplicación web en la cual se identifican los ataques reportados de phishing. Tomado d*e.* CIBERINCIDENTES | Centro Cibernético Policial [Anónimo]. Centro Cibernético Policial [página web]. [Consultado el 11, octubre, 2022]. From <https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico>.

En el ciberespacio se usan la mayoría de las redes sociales para poder comprar y vender productos, por ello también están propensos a ser víctimas de suplantaciones de identidad paginas fraudulentas que puedan hacer ciberestafas.

Podemos identificar el posicionamiento del puntaje de ciberseguridad en el que esta nuestro país, el cual es evidente que se requiere más capacitación y atención al tema aún a nivel global.

Figura 3

Score Ciberseguridad

Americas region

Member State	Score	Regional Rank	Global Rank
United States of America*	0.926	1	2
Canada*	0.892	2	9
Uruguay	0.681	3	51
Mexico	0.629	4	63
Paraguay	0.603	5	66
Brazil	0.577	6	70
Colombia	0.565	7	73
Cuba	0.481	8	81
Chile	0.470	9	83
Dominican Republic	0.430	10	92
Jamaica	0.407	11	94
Argentina	0.407	11	94

Nota. En esta imagen podemos identificar el score de ataques que se presentan en Colombia Tomado de. Barros, A. (2021, May 9). La Ciberseguridad según la ITU. El Escritorio de Alejandro Barros; Alejandro Barros. https://www.alejandrobarros.com/la-ciberseguridad-segun-la-itu/

Uno de los fraudes más conocidos es manejado por la Red. Se trata la suplantación de una empresa, persona o entidad, como puede ser una empresa reconocida, un banco, una red social, o un amigo o familiar. El objetivo es tener información confidencial o sensible para manipular

robar o amenazar, como sabemos esto lo pueden hacer por medio de una llamada de un mensaje de texto, un correo electrónico o aun hasta por medio de una comunicación de red social haciéndose pasar por un banco o tal vez por su jefe.

Marco Científico o Tecnológico

De acuerdo con el desarrollo del presente trabajo nos enfocaremos en algunos ataques de ingeniería social por lo cual se contextualizará en algunos más comunes, no sin antes enfatizar en la clasificación de ataques:

Clasificación de Ataques

Ataques Pasivos. Este ataque consiste en sólo observar comportamientos, ver la información y como la manejan, esto sin intervenir ni alterar el estado del sistema ni la información. Esto quiere decir que este ataque en la triada afecta únicamente la confidencialidad de la información.

Ataques Activos. Este ataque al contrario del anterior observa y modifica y afectar la información así dañando no solo la información si no también puede afectar el estado del sistema o ambos. Esto nos muestra que en la triada afecta la confidencialidad, la integridad y la autenticidad de la información.

Riesgos. Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad.

Ransomware. Tipo de programa maligno el cual quiere inhabilitar el uso de un sistema así restringiendo el acceso a el equipo o data de un usuario, por lo cual el ciberdelincuente tiene el control de su equipo o data, lo que hace el ciber atacante es extorsionar a la persona pidiéndoles dinero por soltar su información, es un secuestro de datos.

Spyware. Un tipo de programa maligno que actúa silenciosamente mientras envía a los ciberdelincuentes información sensible sin que el usuario se dé cuenta. Entre los spyware es posible reconocer sistemas de cámara espía o KEYLOGGERS (software que almacena como texto todas las pulsaciones que el usuario hace en el teclado)

Phishing. Engaño mediante interfaces falsas, medios de comunicación directos y suplantación de identidad, los ciber atacantes manipulan a las víctimas para que suministre información confidencial o haga algo que el ciberdelincuente quiere para su beneficio.

Ciberterrorismo. Manipulación de medios de comunicación donde amenazan con publicar contenido privado generando temor o pánico en una población especifica.

Denegación de Servicio (DoS). Este por medio de bots, o pequeños robots digitales intentan saturar un servidor para que este se desactive o deshabilite, buscando entorpecer el correcto funcionamiento de un sistema, así explotando otra vulnerabilidad o afectar a las personas.

Suplantación de Identidad (Spoofing). Fraude donde el ciber atacante roba alguna identidad con el fin de hacer cosas ilícitas como hurto, intimidación, o cualquier otra actividad desautorizada por las personas y que las hacen de forma incógnita. Puede darse mediante la simulación, clonación o hurto de credenciales o identificadores digitales.

Virus Informático. Es un programa informático malicioso, que se instala sin autorización o aviso generando alguna modificación de su funcionamiento o de la data que este almacena. Es un tipo de programa maligno diseñado para dañar la integridad de un equipo o sistema.

Marco Legal

En este punto se es necesario citar algunas normas internacionales y algunos procesos autorizados para la ciberseguridad:

Se explicarán las normas internacionales más relevantes y prácticas para la prevención de ataques de ingeniería social. Dado que estamos implementando nuevos procesos debido al crecimiento de la ciberseguridad, es importante recordar la necesidad de priorizar ciertos servicios que contribuyan a mejorar la recesión económica. Sin embargo, estas buenas prácticas también pueden ayudarnos a mejorar nuestra compañía y asegurar la información. Para ello, podemos tomar como referencia normas internacionales como ISO 27032, ISO 27001, ISO 27002 y marcos como el NIST Cybersecurity Framework y MAGERIT. El objetivo es establecer nuevos procesos de la mejor manera posible, optimizando la situación actual y definiendo un buen gobierno corporativo que esté alineado con el gobierno de TI. De esta manera, es posible mejorar significativamente los procesos y alcanzar los objetivos propuestos inicialmente. Para conseguir esto se recomienda lo siguiente:

El departamento de TI debe realizar inicialmente un análisis de su operación y de la infraestructura con la que cuenta en la actualidad. Posteriormente, se debe llevar a cabo una investigación a fondo del nuevo servicio de recaudos de pagos para entender cuál es el proceso o, si no existe, generar un manual de procedimientos que indique lo que se ejecutará o llevará a cabo para el nuevo servicio. Además, se debe determinar qué infraestructura se requiere para operar el nuevo servicio y, teniendo en cuenta lo anterior, identificar si con la infraestructura actual se puede continuar o si, por el contrario, se debe adquirir una nueva tecnología.

Teniendo en cuenta que los recursos son limitados y solo se tendrá en cuenta lo que realmente sea necesario, desde el departamento de TI se puede evaluar con la infraestructura, hardware o software con la que cuenta.

Una buena estrategia también sería para poder cumplir con sus objetivos de negocio y una buena ciberseguridad tener en cuenta la (ISO27032):

Que la política, los objetivos y actividades de seguridad de la información que sean claras estén alineadas con los objetivos del negocio.

Identificación de activos críticos para así realiza una evaluación exhaustiva de los riesgos de ciberseguridad que pueda enfrentar la organización.

Desarrollar procedimientos detallados para la respuesta y recuperación ante incidentes de ciberseguridad.

Implementar controles de seguridad como pueden ser:

- Controles Técnicos: Implementa controles técnicos como firewalls, sistemas de detección de intrusos y cifrado de datos.
- Controles Administrativos: Asegura que existan controles administrativos, como la gestión de accesos y la formación en ciberseguridad para los empleados.

Promocionar la capacitación y concienciación de clientes internos y externos con un proceso de formación continua y laboratorios o simulacros para evaluar a el personal.

Implementar un sistema de monitoreo continuo que detecte y responda de forma eficaz en tiempo real.

Realizar auditorías de forma regular para evidenciar la madures de las políticas y procedimientos de ciberseguridad que la empresa implementa.

Un sistema de medición utilizado para evaluar el desempeño en la gestión de la seguridad de la información y para proporcionar sugerencias de mejora.

La ISO 27032, también conocida como “Directrices para la Ciberseguridad”, nos ayuda a gestionar y mejorar la ciberseguridad mediante diversas directrices, entre estas podemos adoptar los siguientes ejemplos:

Políticas de Seguridad

Se debe de tener en cuenta la organización de la seguridad de la información, teniendo en cuenta;

Organización interna

Dispositivos móviles y teletrabajo

Seguridad de los Recursos Humanos

Para validación se debe de tener en cuenta el personal también la contratación que sean personas responsables, medidas de seguridad ante despidos Finalización y cambio de contrato y demás.

Gestión de los Activos

Aquí podemos ver la clasificación de la información manipulación manejos de soportes de almacenamiento (gestión de soporte extraíbles, eliminación y soportes físicos en tránsito).

Responsabilidad por los activos

Clasificación de la información

Manejo de los medios de comunicación

Control de Accesos

Tener presente que se debe de definir y asegurar accesos de los usuarios permitidos, aplicaciones y sistemas.

Requisitos empresariales para el control de acceso

Gestión del acceso en usuarios

Responsabilidades del usuario

Control de acceso en sistemas y aplicaciones

Cifrado

Seguridad Física y Ambiental. Controles de entrada o acceso, controles para amenazas externas y ambientales, mantenimiento de equipos, copias de seguridad, manejo de equipos en home office, seguridad de equipos de almacenamiento políticas de seguridad de información bloqueo de pantalla, no compartir información confidencial, entre otras.

Seguridad de las Operaciones. Seguridad en los equipos sistemas operativos, procedimientos y responsabilidades, protección contra malware, antivirus, copias de resguardo, auditoria de sistemas de información.

Procedimientos y responsabilidades operativas

Protección ante programa maligno

Copias de seguridad

Registros y monitoreo

Control del software operacional

Gestión del as vulnerabilidades técnicas

Consideraciones en auditorias de sistemas

En este caso de que se expanda la empresa se debe de tener seguridad también con proveedores, adicional validando los aspectos técnicos se debería de colocar la contraseña expire por seguridad y evitar que cualquier persona pueda obtener acceso y tener confidencialidad, integridad de los datos.

Seguridad de las Comunicaciones. Seguridad de la red.

Relaciones con los Proveedores. Seguridad de la información en las relaciones con los proveedores.

Seguridad de la información en las relaciones con proveedores

Gestión de la entrega con proveedores

Se identifica que todos los equipos disponen de sistema antivirus que se actualiza con una periodicidad diaria de manera automática. Todos los equipos disponen de conexión a Internet. Se trata de una conexión ADSL con un router que dispone de funcionalidades de cortafuegos, que es algo estrictamente necesario y se está cumpliendo, con esto tendremos varios beneficios:

Tendremos una metodología de gestión de seguridad bien estructurada.

Reduciremos el del riesgo de pérdida, filtración, robo de información.

Todos los clientes internos y externos tendrán acceso limitado o por medio de permisos a las aplicaciones o accesos.

Crear un enlace de confianza de clientes y socios por la garantía de calidad y confidencialidad comercial.

Las auditorías externas nos ayudaran a mejorar y saber que se está cumpliendo, dándonos más estatus.

Posibilidad de integrarse con otros sistemas de gestión de a ISO para completar y cumplir con las normas establecidas.

Podremos disminuir el riesgo de parar la operación por algún incidente de seguridad.

Imagen de empresa y estatus a nivel internacional.

Confianza y reglas claras para las personas de la organización.

Reducción de costes y mejora de los procesos y servicio.

Aumento de la motivación y satisfacción del personal.

Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

Complementando a lo anterior y agregando otro punto de vista consideramos que es posible también aplicar el marco NIST Cybersecurity Framework, puesto que nos proporciona cierta cantidad de recomendaciones y planes ante desastres DRP, que deben ser tenidos en cuenta ante una emergencia. Adicional rectificar que este marco busca dar una reseña de las mejores prácticas con el fin de enfocar esfuerzos en ámbitos de ciberseguridad los cuales hacen énfasis en sus 5 áreas: identificación, protección, detección, respuesta y recuperación.

Diseño por Fases

El enfoque metodológico para desarrollar los objetivos es mixto, manejado por fases, pero el que más se usará será el cuantitativo que se basa en investigación en estadísticas y números, pero también se usará el segundo que se basa en lo subjetivo.

Desarrollo del Objetivo 1

Identificar las vulnerabilidades, amenazas y riesgos asociados con la ingeniería social mediante el análisis de diferentes tipos de ataques, respaldados por estadísticas, con el fin de determinar los riesgos más comunes a las empresas del sector privado.

Triada CID

Por sus siglas CIA traduce confidencialidad, integridad y disponibilidad, son atributos manejados en la ciberseguridad, si se cuidan estas tres variables se puede tener un nivel de seguridad bueno.

Para no tener ataques recurrentes y controles de seguridad adecuados se debe brindar confidencialidad, integridad y disponibilidad a los datos, estas palabras significan lo siguiente:

La confidencialidad esta es la virtud que permite restringir el acceso de personas no autorizadas a algún sistema, para así poder mantenerlos en secreto ya que solo tienen acceso a ellos las personas autorizadas.

Integridad significa que los datos son originales y que llegan tal como se envían, sin ninguna modificación ni manipulación.

La disponibilidad se refiere a que los datos sean accesibles cuando se requieran.

Ingeniería Social

A diferencia de otros ataques, la ingeniería social es tratar de influir o manipular las personas para que ellas den información o hagan cosas que no quieren, ejemplo, revelar información importante.

Ciberacoso

Se busca decir mentiras o publicar fotografías o videos vergonzosos que puede que no sean reales creados con una IA para que las personas hagan cosas que no desean en medio de manipulación y dejando a las personas en un papel vergonzoso y humillante.

Angler Phishing

Esta estafa es manejada en redes sociales, se crean cuentas de redes sociales falsas para hacerse pasar por un trabajador de una empresa, con la intención de atraer a la víctima ofreciéndole solución a sus problemas.

Pharming

Este secuestra la configuración de navegador, ejecutando al mismo tiempo un programa maligno ya que redirige a las personas de un sitio web legitimo a uno falso para obtener su información de índole confidencial, también pueden robar hasta las preguntas de seguridad.

Phishing

Las comunicaciones que realizan por correo electrónico se disfrazan para que parezca que fueran de una fuente de confianza, por ejemplo, ¿porque dudaríamos de una fuente de un amigo o familiar? No deberíamos por lo cual sucede eso.

Spear Phishing

A diferencia del phishing tradicional, el spear-phishing requiere conocimiento previo de la víctima para hacer que esta revele datos personales, financieros y otros datos confidenciales.

Sexting

Esta técnica logra obtener imágenes o vídeos de carácter sexual, en redes sociales, manipula a la persona para que no denuncie ya que serían publicadas estas imágenes.

Vishing

Mas conocido como phishing por voz, el cual falsifica los números de teléfono y llaman presentándose por el jefe o por personas conocidas, también utilizan cambiadores de voz para ocultar su identidad, pidiendo datos confidenciales a la víctima.

Vishing Tabnabbing/ Tabnabbing Reverso

Estos ataques explotan sitios web estático en el navegador, el delincuente toma el control de una pestaña recién abierta y secuestra la pestaña original desde donde se abrió, remplazando o modificando las pestañas para que se redirijan a sitios fraudulentos, robando información confidencial.

BEC (Acceso a Correos Electrónicos Comerciales)

También conocido como “Business Email Compromise” (BEC) usan un método de acceso a cuentas de correos electrónicos suplantando la identidad de empleados de alto nivel así estafando a compañeros empleados y clientes. Normalmente buscan realizar transferencias electrónicas.

Smishing

El sm1sh1ng es un ataque de phishing que llega en forma de mensaje de texto. Los atacantes piden a la víctima que realice alguna acción urgente, utilizando enlaces corruptos para robar información o manipular a la persona para que haga cosas que no desea.

Whaling

Este tipo de phishing, conocido como “fraude de los directores generales”, tiene consecuencias catastróficas ya que se dirige a objetivos de alto valor. Los atacantes adoptan un tono de voz apropiado y utilizan conocimiento interno de la industria para ser más creíbles y beneficiarse.

Baiting

El baiting es un ataque de ingeniería social en el que un atacante deja un dispositivo infectado, como un USB, en un lugar público para que alguien lo recoja y lo use, infectando así su dispositivo

Spam en el Correo Electrónico

Es un correo electrónico que es spam o basura que llega a el correo donde redirige a las personas a una estafa a un enlace que es molesto o peligroso.

Spoofing

Se llama Suplantación de identidad, el atacante usa técnicas para que la víctima crea que se trata de una entidad distinta atreves de la falsificación de datos en una comunicación.

Pretexting

El pretexting consiste en crear un escenario falso para engañar a víctimas, tienden a saber mucho de la víctima para crear un pretexto o problema urgente y las personas puedan caer en la trampa y dar información.

Scareware

Los ciberdelincuentes hacen creer a las víctimas que su computadora está infectada con programa maligno y les piden comprar un software de seguridad falso. Al hacerlo, el programa maligno se instala y aprovecha las ventanas emergentes para ejecutar el ataque.

Honey trap

En este ataque se atraen a la víctima con una situación sexual vulnerable. El atacante evidencia la situación y la oportunidad de sextorsión como chantaje con fotos o videos, estos en forma de chantaje le dicen a la víctima que las están observando por medio de cámaras, normalmente informa que comprobara la cámara web si es segura, lo mejor es negar el spam.

Suplantación DNS

Este tipo de suplantación se realiza mediante el envenenamiento de nombres de dominio (DNS), aprovechándose de vulnerabilidades del sistema. Esto desvía el tráfico de servidores legítimos a servidores falsos.

Factores Transversales

El objetivo de los ciberatacantes es lograr que la víctima crea sus afirmaciones sin cuestionarlas. Esto puede ocurrir en cualquier tipo de ataque, independientemente de la persona o el medio utilizado. Buscan minimizar cualquier duda sobre la veracidad de su mensaje o la posibilidad de que sea una estafa.

Credibilidad

Para que una persona realice una acción o proporcione información, necesita creer que la solicitud es legítima. En la ingeniería social, se utilizan detalles en los mensajes o llamadas para hacer creer que la solicitud es auténtica.

Urgencia

Los ciberatacantes a menudo crean situaciones urgentes que requieren una solución inmediata, estableciendo plazos cortos para que las víctimas actúen. Esto reduce el tiempo disponible para que la víctima piense con claridad, corrobore la información o consulte con el banco u otras personas involucradas.

Familiaridad

Los atacantes pueden hacerse pasar por familiares o amigos íntimos para engañarnos y pedirnos datos, dinero o información privada. Aprovechan nuestra compasión y confianza, haciendo que dudemos menos de sus intenciones. Por ejemplo, podríamos abrir un enlace de un supuesto familiar que dice necesitar dinero urgente sin validar antes la situación.

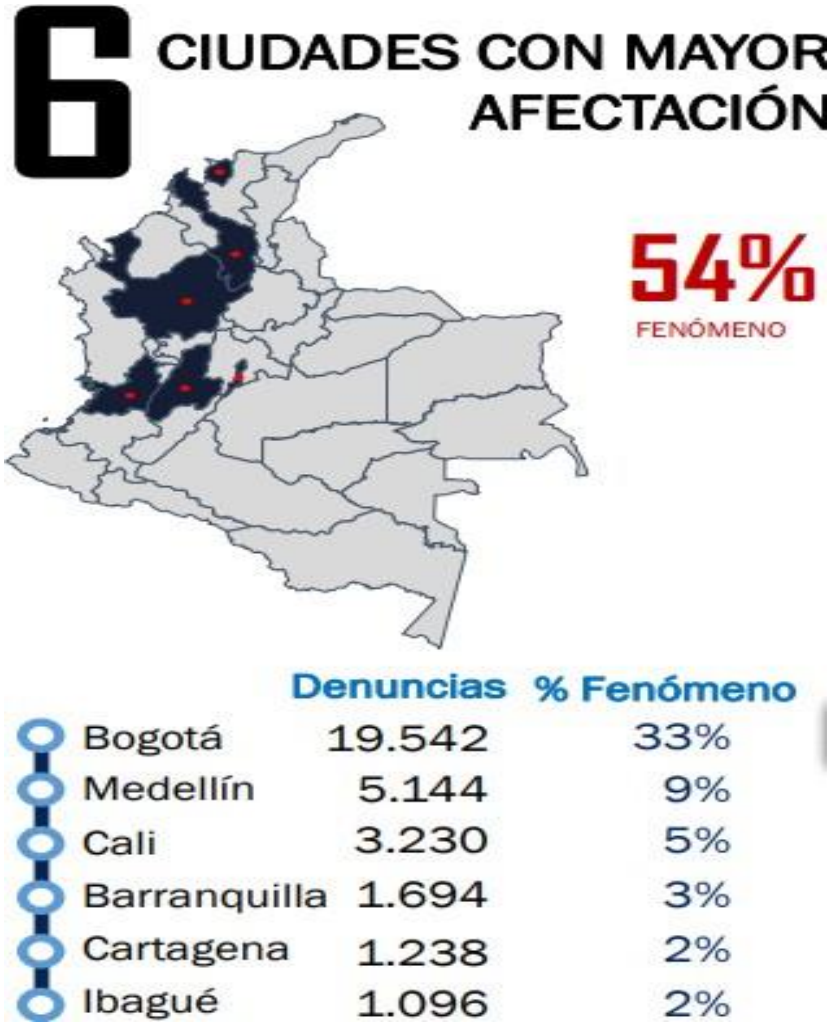
Estadísticas

Ciudades

En 2023, más de seis ciudades, incluyendo Bogotá, Medellín, Cali, Barranquilla, Cartagena e Ibagué, reportaron 59,033 denuncias por delitos informáticos, lo que representa un decremento del 10% respecto a las 65,794 denuncias de 2022.

Figura 4

Ciudades más Afectadas

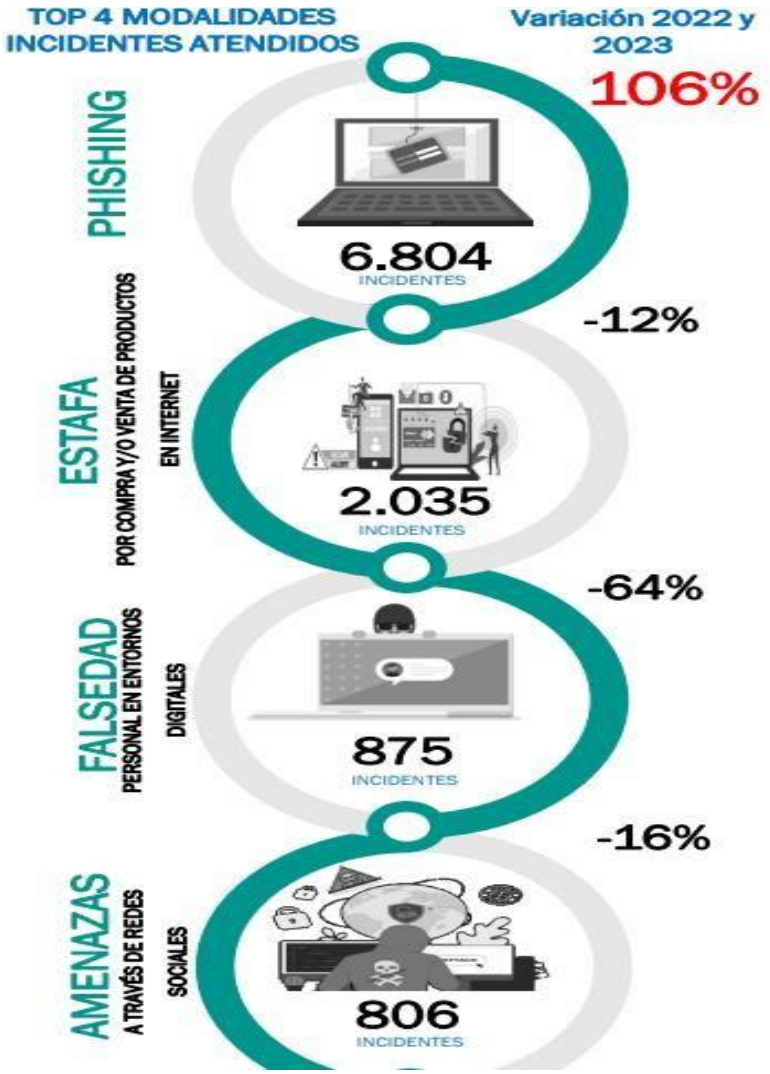


Nota. Esta imagen podemos identificar el porcentaje de ciudades que presentan más ciberataques en Colombia, Tomado de. Dirección de investigación criminal e interpol. (2022). Centro Cibernético Policial. https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202023_0.pdf

Se identifican las modalidades más presentadas en la cuales todas tiene como proceso la ingeniería social:

Figura 5

Ataques más Presentados



Nota. Podemos ver los porcentajes reportados de ataques de ingeniería social que se han presentado en las ciudades principales. Tomado de. Vector de cibercrimen que más usan los atacantes con el uso de ingeniería social *https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202023_0.pdf*

¿Cuáles son algunas de las brechas que permiten que la ingeniería social aun tenga fuerza?

Redes Sociales

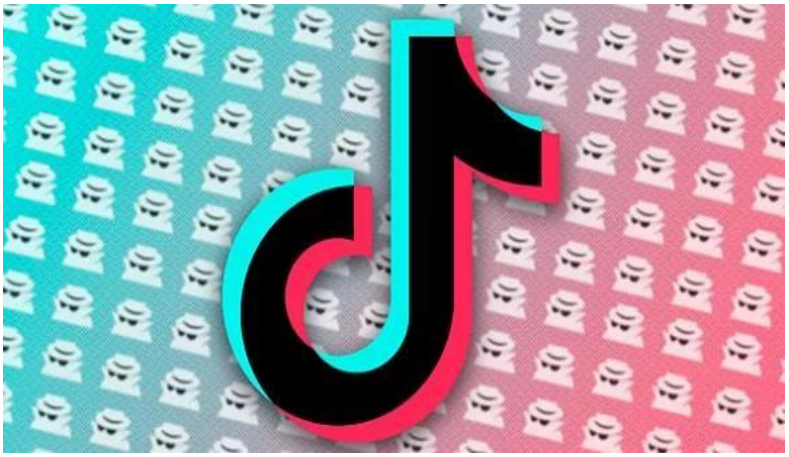
TikTok. Se identifica que la ingeniería social no reconoce edades ya que en las redes sociales desde niños hasta adultos ha caído en diferentes ataques de ingeniera social donde usan el nombre de sus padres fotografías o información confidencial como arma para lograr que las personas hagan lo que no deben: El gobierno y organizaciones legales están preocupados por la proliferación de pederastas en TikTok, una red social muy usada por menores de edad. Se han identificado casos donde pedófilos comentan inapropiadamente en videos de menores y modifican el contenido. Desde 2019, TikTok enfrenta demandas por alojar y almacenar ilegalmente videos de menores de 13 años, que luego son vendidos a redes de pedofilia. Esta situación ha llevado a la prohibición de TikTok en varios países, como el Reino Unido, y a multas significativas, aunque las demandas continúan.

Una investigación del diario The Telegraph realiza el análisis del uso de la red social indicando que hay perfiles de adulto que solo observan actividades de menores de edad.

La validación de los términos de uso de TikTok muestra que permite el acceso a mayores de 13 años, pero verificar la edad real de los usuarios es imposible. Se estima que el 70% de los usuarios tiene entre 13 y 24 años, y el 30% restante posiblemente son menores. Este problema no es exclusivo de TikTok, ya que muchas redes sociales tienen un gran número de menores que, por curiosidad o interés en el contenido, se exponen y comparten información confidencial.

Figura 6

Logo Red Social TikTok



Nota. Logo de la red social TIK TOK. Tomado de. Toledano, B. (2020, July 23). TikTok, en el punto de mira por la presencia de pederastas en su red social. ELMUNDO. https://www.elmundo.es/tecnologia/2020/07/23/5f18329921efa04b168b4620.html

¿Como podemos minimizar el riesgo de ingeniería social tanto en la vida personal como en las empresas?

Gobierno y Herramientas de Inteligencia Digital. El Ministerio TIC, no solo ha creado capacitaciones campañas y boletines para que se fortalezca el conocimiento de forma de manejo y herramientas útiles de seguridad para el cuidado de los niños, sino que también creo una campaña llamada 1, 2, 3 por TIC este a través de charlas videos gratuitos muestra el mejor uso del internet y la forma de aprovecharlo de forma segura.

Esta página nos muestra como ingresar a la plataforma y por medio de videos claros y juegos para los niños el cuidado y la actualidad del internet y redes sociales.

Figura 7

Mintic 123 por TIC

Nota. Página de la mintic donde permite generar capacitaciones personales o empresariales. Tomado de. Inicio - 1,2,3 por TIC. (n.d.). 1,2,3 Por TIC. https://123portic.gov.co/829/w3-channel.html

Informe de delitos

En 2022, el Informe sobre Delitos en Internet del FBI reportó 800.944 ciberdelitos, destacando los ataques de phishing como el más frecuente, con 300.497 denuncias y pérdidas que superaron los 10.300 millones de dólares (Techopedia, 2024).

Figura 8

Tipos de Cibercrimen

By Victim Count			
Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		
*Descriptors**			
Cryptocurrency	31,310	Cryptocurrency Wallet	20,781

Nota. En la imagen podemos ver los ataques presentados y la cantidad de víctimas demandantes, debemos de tener presente que no todas las victimas demandan, por lo cual el porcentaje debería de ser mayor. Tomado de. Techopedia. (2024.). Estadísticas de ciberseguridad. Techopedia. https://www.techopedia.com/es/estadisticas-ciberseguridad

Ataques de Ingeniería Social más Presentados

Podemos identificar varios ataques de ingeniería social, los cuales son los más presentados en América Latina. Esto puede deberse a la desinformación y a la falta de control sobre los riesgos a tiempo.

Phishing

Los ataques de phishing, que representan el 90% de las violaciones de datos, siguen siendo los más comunes, con aproximadamente 3.400 millones de correos electrónicos no

deseados diarios. Estos ataques utilizan técnicas engañosas para obtener información sensible al hacerse pasar por entidades fiables en correos electrónicos o sitios web falsos.

Spear Phishing

Los atacantes ajustan sus métodos para que los correos electrónicos o mensajes fraudulentos parezcan extremadamente auténticos y confiables, para así poder suplantar identidades.

Clone Phishing

Implica la creación de una réplica falsa o clon de un correo electrónico o sitio web legítimo.

Whaling

Está orientado a directivos de alto nivel o a individuos en posiciones de autoridad dentro de una organización, pueden ser unos de los siguientes ejemplos:

- Directores ejecutivos (CEO)
- Presidentes de empresas
- Directores de la cadena de suministro (CSCM)
- Vicepresidentes de la empresa

Pop-up

Ocurre a través de ventanas emergentes o cuadros de diálogo falsos que engañan al usuario, cuando este le da en ese enlace lo redirige a un sitio malicioso.

Ataques de Ingeniería Social de Marca

De acuerdo con estadísticas de ciberseguridad, alrededor del 88% de las organizaciones experimentan ataques de spear phishing anualmente, lo que sugiere que las empresas son atacadas casi a diario.

LinkedIn (relating to 52% of all phishing attacks globally)

DHL (14%)

Google (7%)

Microsoft (6%)

FedEx (6%)

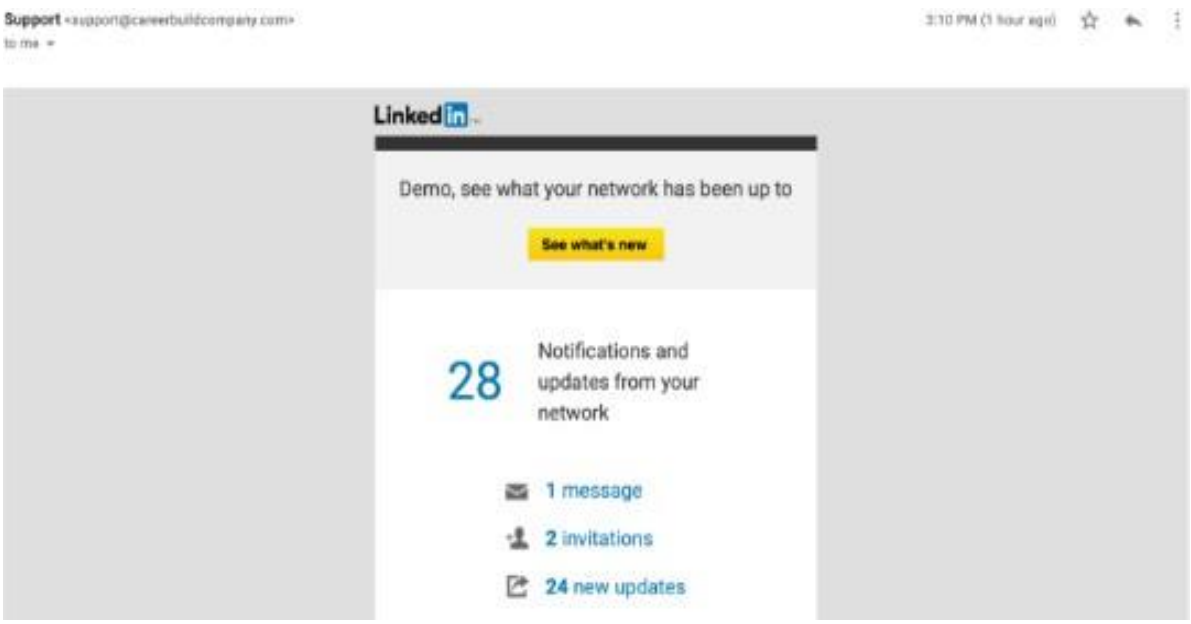
WhatsApp (4%)

LinkedIn

Un ejemplo representativo de un correo electrónico de phishing de LinkedIn se ve así como la imagen de laboratorio realizado en la UNAD:

Figura 9

Phishing Linkedln



Nota. En la imagen vemos como se presentaban los correos electrónicos fraudulentos. Tomado de. Techopedia. (2024.). Estadísticas de ciberseguridad. Techopedia. https://www.techopedia.com/es/estadisticas-ciberseguridad

Yahoo

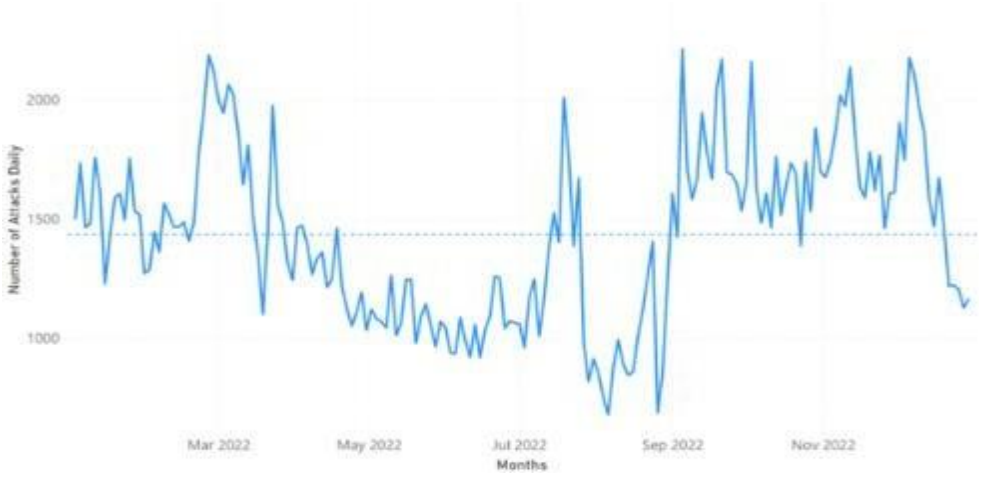
En el cuarto trimestre de 2022, Yahoo subió 23 posiciones, alcanzando un incremento del 20% en ataques de phishing, debido a una campaña efectiva en el trimestre anterior. LinkedIn, por su parte, descendió al quinto lugar con un 5,7% de intentos de phishing de marcas. El aumento del teletrabajo ha llevado a un crecimiento en las estafas de compromiso de correo electrónico empresarial (BEC), donde los estafadores utilizan técnicas de phishing para obtener información confidencial o realizar transferencias de dinero no autorizadas.

Microsoft

En 2023, Microsoft neutralizó un promedio de 1.435 ataques DDoS por día. El 22 de septiembre alcanzó el mayor número de ataques diarios con 2.215, mientras que el 22 de agosto se registró el mínimo con 680. En total, la compañía mitigó más de 520.000 ataques únicos durante el año.

Figura 10

Grafica Número de Ataques DDoS



Nota. En la imagen gráfica vemos representadas de ataques DDoS que sin generados también en su mayoría por ingeniería social. Tomado de. Techopedia. (2024.). Estadísticas de ciberseguridad. Techopedia. https://www.techopedia.com/es/estadisticas-ciberseguridad

Google

Según un informe de Cloudflare, los ataques DDoS de rescate aumentaron un 67% interanualmente y un 24% intertrimestralmente. Las industrias en línea vieron un incremento significativo en los ataques DDoS en la capa de aplicación, con un aumento del 131% en el trimestre y del 300% en el año. En septiembre de 2017, se registró un ataque DDoS récord contra Google con un tamaño de 2,54 Tbps, revelado por Google Cloud en octubre de 2020, y atribuido a China. Los ataques involucraron el envío de paquetes falsos a 180.000 servidores web. En marzo de 2023, el sitio web de la Asamblea Nacional francesa fue temporalmente interrumpido por un ataque DDoS de hackers rusos, quienes justificaron su acción como respuesta al apoyo francés a Ucrania.

Datos de Ciberataques

En 2023, se generaban diariamente 300.000 nuevas instancias de programa maligno, de las cuales el 92% se distribuían por correo electrónico, con un promedio de 49 días para su detección. El programa maligno se emplea para acceder sin autorización a sistemas, robar datos, interrumpir servicios o dañar redes. Aproximadamente 4,1 millones de sitios web están infectados con programa maligno, y el 18% de estos presentan amenazas críticas para la ciberseguridad.

De acuerdo con el Informe sobre Ciberamenazas 2023 de SonicWall, el programa maligno vio su primer incremento desde 2018, alcanzando los 5.500 millones de ataques, lo que supone un aumento del 2% en comparación con el año anterior. Aunque el aumento es moderado, el crecimiento significativo se debe principalmente a las elevadas tasas de criptojacking y programa maligno dirigido a dispositivos IoT.

A pesar del aumento en los ataques cibernéticos, las empresas colombianas han incrementado significativamente su inversión en ciberseguridad. Entre 2023 y 2024, el 85% de las empresas elevaron sus presupuestos para proteger sus sistemas. Se estima que para 2025, la inversión en ciberseguridad en Colombia crecerá un 19%, posicionando al país entre los cinco primeros en la región en este ámbito.

Sectores de Empresas Privadas más Afectados

Además del aumento en la frecuencia de los ciberataques, estos se han vuelto más sofisticados, enfocándose en objetivos más cercanos a los usuarios y en industrias vulnerables, lo que permite a los atacantes obtener mayores ganancias. Los sectores más afectados son el financiero, grupos empresariales, empresas legales y el gobierno.

Tabla 1

Sectores Afectados

Sector	Porcentaje Afectado
Financiero	35%
Grupos Empresariales	27%
Empresas Legales	14%
Gobierno	11%

Nota. En esta tabla podemos observar el porcentaje de sectores en las empresas con más afectación de acuerdo con los grupos empresariales. Modificado de. Infobae. (2024, 22 de agosto). https://www.infobae.com/colombia/2024/08/22/finanzas-de-los-colombianos-podrian-tener-problemas-por-ciberataques-empresas-tuvieron-que-tomar-millonaria-decision/#:~:text=Sin%20embargo%2C%20a%20junio%20de,en%20la%20inversi%C3%B3n%20en%20ciberseguridad.

En 2019, el 80% de las violaciones de datos fueron causadas por contraseñas comprometidas, resultando en grandes pérdidas financieras para empresas y usuarios. Al cambiar sus contraseñas, el 49% de los usuarios solo modifica una letra o un dígito en sus contraseñas

habituales. Los hackers pueden probar 2,18 billones de combinaciones de contraseñas y nombres de usuario en solo 22 segundos. Incorporar una sola letra mayúscula a una contraseña puede aumentar significativamente su seguridad. Por ejemplo, una contraseña de ocho caracteres puede ser descifrada en un segundo, pero añadir una letra mayúscula puede extender este tiempo a 22 minutos.

Figura 11

¿Qué tan Fuerte es tu Contraseña?

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

*Nota.*En esta tabla podemos identificar que tan fuerte es nuestra contraseña de acuerdo con las respuestas dadas. Tomado de. Techopedia. (2024.). Estadísticas de ciberseguridad. Techopedia. https://www.techopedia.com/es/estadisticas-ciberseguridad

Métodos más Usados para Ataques de Contraseñas

Brute Force: Examinar de manera metódica todas las posibles combinaciones de contraseñas hasta dar con la correcta.

Dictionary: Se emplea una lista de contraseñas comunes o términos de un diccionario para intentar acceder a la autenticación.

Hybrid : Combina elementos de los ataques de fuerza bruta y de diccionario.

Credential Stuffing: Se fundamenta en el empleo de amplios conjuntos de nombres de usuario y contraseñas que han sido sustraídos.

Desarrollo del Objetivo 2

Observar las buenas prácticas de seguridad identificando posibles brechas relacionadas con la ingeniería social, con el objetivo de formular recomendaciones adecuadas para las empresas del sector privado.

Inicialmente se hablará de las leyes y normativas que aplican para el sector privado:

Ley 1266 de 2008 (Habeas Data)

Regula el manejo de datos personales, estableciendo derechos para los titulares de datos y obligaciones para quienes los manejan. Asegura el consentimiento para el tratamiento de datos.

Ley 1581 de 2012 (Protección de Datos Personales)

Desarrolla principios y derechos en el manejo de datos personales, obligando a las empresas a implementar políticas de privacidad y medidas de seguridad para proteger la información.

Ley 1273 de 2009 (Delitos Informáticos)

Tipifica y sanciona delitos informáticos, como el acceso no autorizado a sistemas, la interceptación de datos y el daño a sistemas informáticos.

Código de Comercio

Regula aspectos comerciales en general, incluyendo la obligación de las empresas de llevar registros contables y conservar documentos, lo que implica la protección de información sensible.

Ley 527 de 1999 (Comercio Electrónico)

Establece normas para el uso de la firma digital y la validez de documentos electrónicos, promoviendo la seguridad en las transacciones en línea.

Resolución 000100 de 2015 (Autoridad Nacional de Protección de Datos)

Proporciona lineamientos sobre la gestión de datos personales y las medidas de seguridad que las empresas deben implementar.

Decreto 1377 de 2013

Complementa la Ley 1581, regulando la autorización de uso de datos personales en bases de datos existentes, con especial énfasis en la protección de la información.

Norma ISO/IEC 27001

Proporciona un marco internacional para la gestión de la seguridad de la información, ayudando a las empresas a establecer y mantener un sistema de gestión de seguridad.

Políticas Internas de Seguridad de la Información

Las empresas deben desarrollar políticas que incluyan formación en ciberseguridad, gestión de incidentes, y control de acceso a sistemas y datos.

Lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)

Ofrecen recomendaciones para fortalecer la ciberseguridad en organizaciones, incluyendo la evaluación de riesgos y la adopción de buenas prácticas.

Guía para la Protección de Datos Personales en Línea

Proporcionada por la Superintendencia de Industria y Comercio, establece buenas prácticas para el tratamiento de datos personales en entornos digitales.

ISO27001:2022

Normalmente las empresas presentan un crecimiento exponencial, por lo cual tendrá varias sucursales, por lo que se recomendaría aplicar diferentes planes o acciones para poder cumplir con sus objetivos de negocio con la (ISO27001:2022):

Que la política, los objetivos y actividades de seguridad de la información estén alineadas con los objetivos del negocio

Un enfoque y un marco para el diseño, ejecución, seguimiento, mantenimiento y mejora de la seguridad de la información en consonancia de la cultura de la organización

El apoyo visible y el compromiso de todos los niveles de la Dirección, especialmente de alta Dirección

El conocimiento y entendimiento de los requisitos de protección de los activos de información obtenido mediante la aplicación de la gestión del riesgo de la seguridad de la información (véase la Norma ISO/IEC 27005)

Un programa efectivo de concienciación, formación y educación sobre seguridad de la información, informando a todos los empleados y otras partes interesadas de sus responsabilidades en seguridad de la información establecidas en las políticas de seguridad de la información, normas, etc.

Un proceso eficaz de gestión de incidentes de seguridad de la información.

Un enfoque efectivo de gestión de la continuidad del negocio.

Un sistema de medición utilizado para evaluar el desempeño en la gestión de la seguridad de la información y para proporcionar sugerencias de mejora.

El fin de esta norma es cumplir con la triada de ciberseguridad de la cual hablamos anteriormente: confidencialidad, integridad, disponibilidad y una nueva no repudio, Ahora se darán las recomendaciones más básicas para poder complementar estas buenas prácticas:

Evita entrar a webs de dominios desconocidos, o que se ven prometedores que regalan cosas u ofrecen muy fácil.

Precaución con las conexiones wifi gratis o públicas:

- Instalar un antivirus o manejar diferentes activos físicos como FW de nuevo generación, WAF, dmz entre otros.
- Utiliza claves fuertes y seguras
- Sistema de copias de seguridad

ISO 31000

La gestión de riesgos es muy importante en las empresas, para poder determinar el estado de ciberseguridad con la evaluación que se siguen diferentes puntos como la identificación de los activos con sus vulnerabilidades, amenazas y riesgos de seguridad en las organizaciones, la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, nos puede ayudar a realizar esta evaluación este se maneja con una serie de análisis de los activos identificando su nivel de madures y sus mejoras, para así aplicar controles los cuales pueden ser por requerimiento legal, obligación contractual, requerimiento de negocio, análisis de riesgo o si se decide excluir el control y aceptar el riesgo.

¿Cuál es una de las metodologías más recomendados para identificar los riesgos y poder aplicar las buenas prácticas en las empresas del sector privado?

Existen varios framework y metodologías los cuales nos permiten identificar tareas y organizarlas de forma adecuada, pero en cuanto a los riesgos brechas o vulnerabilidades de la empresa se debe de tener conocimiento de los diferentes controles los cuales se deben aplicar en cuanto a las vulnerabilidades de cada activo, esto nos permite analizar a profundidad donde se encuentra la brecha empresarial y trabajarla.

Existe una que se llama MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es una metodología desarrollada en España para analizar y gestionar los riesgos asociados al uso de tecnologías de la información y comunicaciones.

Tabla 2

Evaluación de Riesgos

Evaluación de riesgos realizados en los pasos anteriores				
Activos	Nombre del activo	Amenazas	Vulnerabilidades	NA
Claves	Contraseña	[E19] Fugas de información	Contraseñas fuertes	A
Software_	IDS-IPS Suricata	[A8] Difusión de software dañino	CVE-2000-0562	M
Instalaciones_	Sede en Bogota	[N*] Desastres naturales	No tener mantenimiento	I
Media_	Hojas de vida de proveedores	[I2] Daños por agua	No realizar revisión en la sede física	I
Datos_	Datos alojados en NextCloud	[A29] Extorsión	No tener políticas de DLP o de acceso	I

Nota. Tabla de ejemplo donde se muestra el análisis que se realiza.

Para esto, debemos conocer las recomendaciones legales aplicables y las guías que podemos seguir. La ISO 31000 se complementa con la ISO 27001, especialmente con el Anexo A de esta última. En este anexo, encontramos diversas recomendaciones sobre controles y calificaciones que deben aplicarse a los activos según los riesgos identificados. A continuación, se presentará un ejemplo de análisis utilizando la metodología MARGERIT, que facilita el análisis de activos, permitiendo profundizar en amenazas, vulnerabilidades, riesgos y controles a

aplicar, ya sean requisitos o complementarios. Los activos pueden clasificarse como físicos, software, entre otros. Se incluirá un ejemplo de evaluación de riesgos con esta metodología, que las empresas privadas pueden utilizar para identificar brechas de ingeniería social y aplicar las remediaciones a tiempo.

Estadísticas de Ataques Cibernéticos

Como ya sabemos, existe una constante evolución en la ciberseguridad y, con ello, los ataques, riesgos, brechas y amenazas que nos obligan a buscar las mejores pautas para disminuir tanto las pérdidas financieras como la pérdida reputacional, Lo que nos lleva a preguntar: **¿**Cuántos ataques de ciberseguridad se producen diariamente en la actualidad?

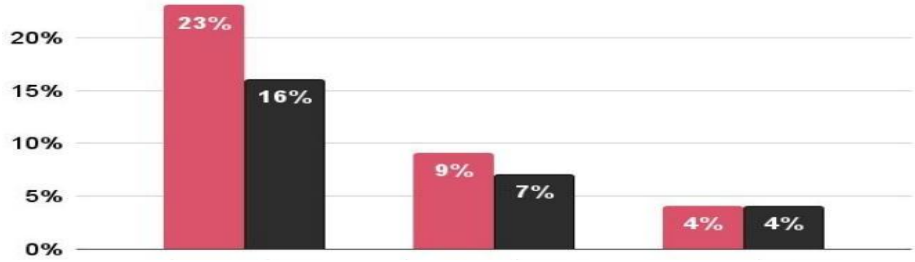
En 2022, se detectaron 493,33 millones de ataques de ransomware globalmente. El phishing sigue siendo el ciberataque más común, con aproximadamente 3.400 millones de correos spam diarios. El coste medio mundial de las violaciones de datos fue de 4,35 millones de dólares, y las brechas por credenciales robadas alcanzaron un coste medio de 4,50 millones de dólares. El sector sanitario, por su parte, ha sido el más afectado por filtraciones durante 12 años consecutivos, con un coste medio de 10,10 millones de dólares en 2022.

Costos de Violación de Datos

De acuerdo con el Informe sobre el costo de una violación de datos de IBM, el costo promedio global de una violación de datos subió de 4,24 millones de dólares en 2021 a 4,35 millones de dólares en 2022. El phishing fue responsable del 16% de los principales vectores de ataque en cibercrimen, con un costo promedio de 4,91 millones de dólares por brecha. Además, las brechas originadas por credenciales robadas o comprometidas tuvieron un costo de 4,50 millones de dólares.

Figura 12

Costos Estimados de las Filtraciones de Datos en los Últimos Años

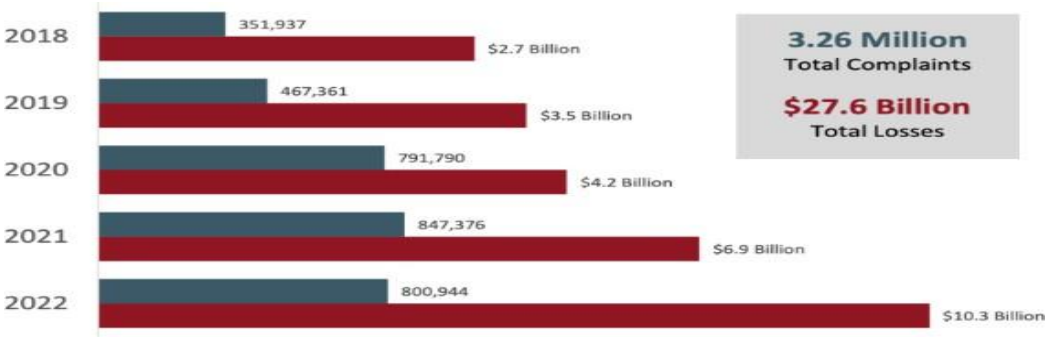


Nota. En esta imagen podemos ver que los incidentes de ciberseguridad suelen ser más costosos que la solución, el porcentaje que dice haber sufrido un incidente de más de un millón de dólares: total en 2024 = 36 %, total en 2023 = 27 %. Tomado de. (2024, 22 de agosto). Finanzas de los colombianos podrían tener problemas por ciberataques: empresas tuvieron que tomar millonaria decisión. https://www.infobae.com/colombia/2024/08/22/finanzas-de-los-colombianos-podrian-tener-problemas-por-ciberataques-empresas-tuvieron-que-tomar-millonaria-decision/#:~:text=Sin%20embargo%2C%20a%20junio%20de,en%20la%20inversi%C3%B3n%20en%20ciberseguridad

En los últimos cinco años, el FBI IC3 (Centro de Quejas por Delitos en Internet) ha recibido un promedio anual de 652,000 denuncias.

Figura 13

Comparación de Quejas y Costos Anuales



Nota. En esta imagen podemos ver la cantidad de quejas dada a el FBI.Tomado de.Techopedia. (2024.). Estadísticas de ciberseguridad. Techopedia. https://www.techopedia.com/es/estadisticas-ciberseguridad

Brechas que Facilitan Ataques de Ingeniería Social

Las empresas dependen cada vez más de soluciones SaaS, utilizando múltiples plataformas en la nube y herramientas colaborativas como Slack y Google Workspace. Una encuesta a líderes de seguridad reveló que más del 70 % de las organizaciones utilizan al menos 50 soluciones SaaS, y un tercio cuenta con 200 o más aplicaciones. Esta amplia adopción ha llevado a un aumento en los incidentes de seguridad de datos. Según el Informe de investigaciones de violaciones de datos de 2024 de Verizon, el 68 % de las violaciones de datos involucraron errores humanos, como ser víctimas de ataques de ingeniería social.

Refuerzos de Seguridad de Datos

Todas las empresas, sin importar su tamaño, deben implementar "firewalls humanos" en su equipo de seguridad, especialmente si utilizan aplicaciones de trabajo colaborativo. Esto implica capacitar a los empleados para que comprendan las amenazas a la seguridad de los datos y puedan identificar actividades sospechosas. Educar a la fuerza laboral sobre riesgos cibernéticos y emplear herramientas de seguridad que envíen alertas en tiempo real son pasos esenciales para proteger la información. Además, es crucial establecer políticas claras sobre el uso de aplicaciones SaaS. Un 62% de los CISO mencionó tener políticas que requieren la aprobación del equipo de seguridad para el uso de aplicaciones.

Productividad y Seguridad

La productividad de una organización está estrechamente ligada al uso de aplicaciones SaaS colaborativas, pero estas también pueden introducir vulnerabilidades que los cibercriminales suelen explotar. Por ello, es crucial implementar una estrategia de "firewall humano", que capacite a los empleados para detectar riesgos de seguridad y permita a los

equipos de seguridad utilizar herramientas que integren a toda la fuerza laboral en la protección de datos.

Los CISO reconocen que los incidentes de ciberseguridad son inevitables, con ataques de programa maligno, phishing y violaciones de datos como los más comunes, a menudo provocados por errores humanos. Ante esto, el 79% de los encuestados planea priorizar la capacitación en seguridad en el próximo año. Sin embargo, además de la formación, es vital adoptar estrategias de firewall humano y herramientas que ofrezcan visibilidad en entornos SaaS para garantizar un plan de seguridad integral, manteniendo altos niveles de productividad sin comprometer la seguridad de los datos.

Violaciones por Elemento Humano

Según el Informe de investigaciones de violaciones de datos de 2024 de Verizon, la explotación de vulnerabilidades como punto de entrada inicial casi se triplicó en comparación con el año anterior, representando el 14% de todas las infracciones. El informe analizó un récord de 30,458 incidentes de seguridad y 10,626 infracciones confirmadas en 2023.

El 68% de las infracciones, ya sea que involucren a terceros o no, están relacionadas con errores humanos no maliciosos, como errores de los empleados o víctimas de ataques de ingeniería social. Este porcentaje se mantiene similar al del año pasado. Sin embargo, se observa una mejora en las prácticas de denuncia: el 20% de los usuarios identificaron y reportaron casos de phishing en simulaciones, y el 11% de quienes hicieron clic en correos electrónicos maliciosos también los denunciaron.

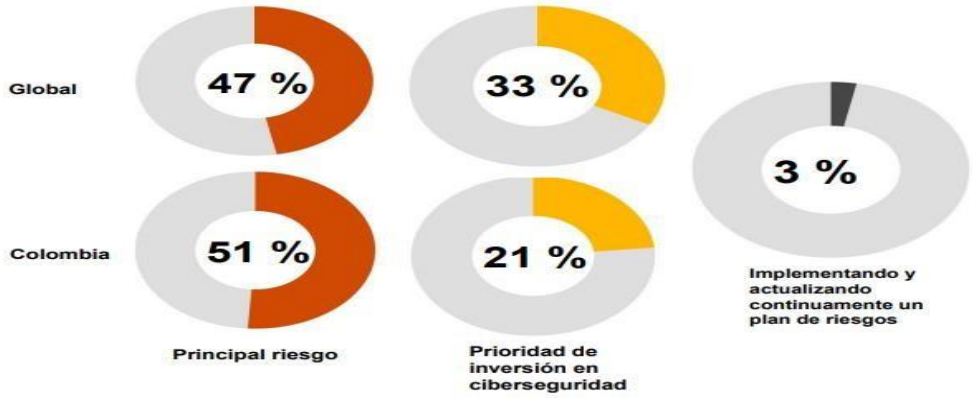
Seguridad en la Nube

La seguridad en la nube es la principal preocupación en ciberseguridad para más del 51% de los encuestados en Colombia. Los métodos de infiltración por parte de actores maliciosos son

casi ilimitados, lo que obliga a las organizaciones a implementar controles exhaustivos en diversas áreas, como identidad y acceso, correos electrónicos, y dispositivos conectados. Sin embargo, el 97% de las organizaciones presenta brechas en sus planes de gestión de riesgos en la nube, y solo el 3% tiene planes actualizados que cubren las nueve áreas de seguridad esenciales.

Figura 14

Seguridad en la Nube



Nota. En la figura podemos identificar la principal amenaza. Tomado de. Techopedia. (2024.). Estadísticas de ciberseguridad. Techopedia. https://www.techopedia.com/es/estadisticas-ciberseguridad

En Colombia, la situación es aún más crítica: cerca del 70% de las empresas no han gestionado el riesgo de terceros, más del 60% no tiene un plan para mitigar riesgos relacionados con datos, y casi la mitad (51%) carece de un plan probado de respaldo y recuperación ante desastres frente a las amenazas actuales.

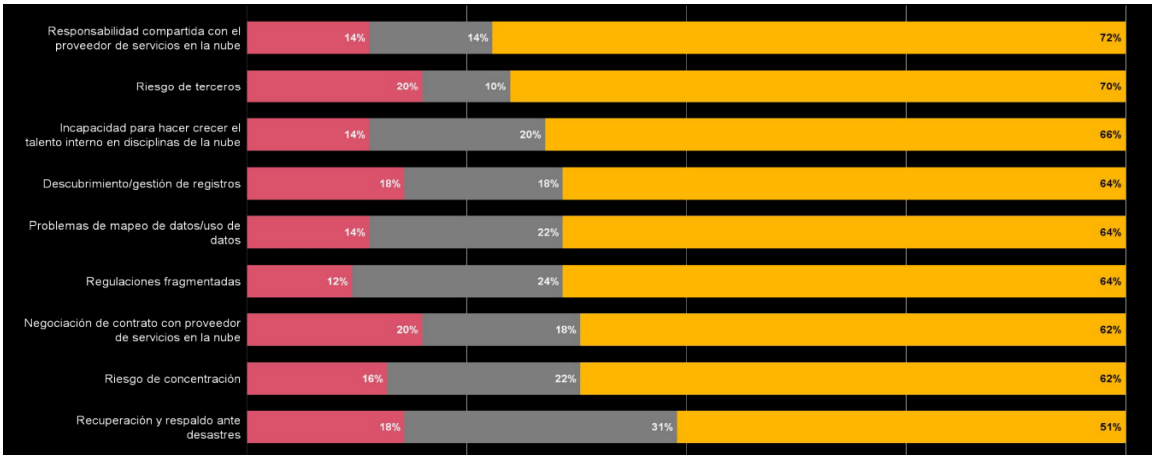
Riegos en la Nube

Podemos observar que existen numerosos riesgos asociados a la seguridad en la nube, pero son escasas las estrategias implementadas para gestionarlos adecuadamente. Esta situación se debe, en gran parte, a la falta de capacitación y conocimiento entre los usuarios.

El uso de la nube ha estado vinculado a la innovación empresarial, facilitando la colaboración entre desarrolladores en diferentes partes del mundo, promoviendo nuevas formas de trabajo más flexibles, y creando modelos de negocio innovadores. La rápida adopción de la nube ha llevado a la migración de datos que antes estaban en infraestructuras locales hacia servicios de almacenamiento en la nube. En este contexto, un 21% de los ejecutivos colombianos encuestados mencionaron que su empresa utiliza múltiples proveedores en la nube.

Figura 15

Seguridad en la Nube en Colombia



Nota. En la figura vemos los riegos de la nube vs los planes para gestión. Tomado de. Techopedia. (2024.). Estadísticas de ciberseguridad. Techopedia. https://www.techopedia.com/es/estadisticas-ciberseguridad

Otros Riesgos de la Ingeniería Social

Los riesgos asociados con la ingeniería social son representativos ya que es una de las amenazas más significativas para la seguridad de la información. La ingeniería social explota la vulnerabilidad humana, manipula a las personas para que revelen información confidencial o realicen acciones que no quieren realizar comprometiendo la seguridad de sistemas y datos.

Tabla 3

Brechas de Ingeniería Social

Riesgo	Descripción
Pérdida de Información Sensible	Los atacantes pueden obtener datos confidenciales como contraseñas, información financiera, y datos personales a través de técnicas de manipulación
Instalación de Programa maligno	Mediante engaños, los atacantes pueden inducir a las víctimas a descargar software malicioso que compromete la seguridad de sus dispositivos
Daño a la Reputación	Las empresas pueden sufrir daños significativos a su reputación si se descubre que han sido víctimas de un ataque de ingeniería social, lo que puede afectar la confianza de sus clientes y socios
Costos Financieros	Los ataques de ingeniería social pueden resultar en pérdidas económicas directas, como el robo de fondos, y costos indirectos, como la recuperación de datos y la implementación de medidas de seguridad adicionales
Robo de Identidad	A través de técnicas como el phishing, los atacantes pueden obtener suficiente información para suplantar la identidad de una persona y realizar actividades fraudulentas en su nombre
Acceso No Autorizado	Los ciberdelincuentes pueden obtener acceso físico o remoto a sistemas y redes, lo que puede llevar a la sustracción de datos o la interrupción de servicios
Fraude y Estafas	Los atacantes pueden engañar a las víctimas para que realicen transferencias de dinero o proporcionen información que permita realizar fraudes a largo plazo

Nota. En esta tabla se identifica riesgos comunes en ataque de ingeniería social, *Fuente.* Propia

Top 10 de Riesgos en Colombia

De acuerdo a revista Semana (2024), “se han identificado los siguientes riesgos en ataques de ciberseguridad: los incidentes cibernéticos (36 %) se sitúan como el riesgo más importante a nivel mundial por tercer año consecutivo”.

Figura 16

Top 10 de Riesgos en Colombia

Ranking		Porcentaje	Ranking 2023	Tendencia
1	Fuego, explosión.	46%	8 (11%)	↑
2	Catástrofes naturales (por ejemplo, tormentas, inundaciones, terremotos, incendios forestales, fenómenos meteorológicos extremos).	43%	NUEVO	↑
3	Interrupción del negocio (incluida la interrupción de la cadena de suministro).	41%	2 (39%)	↓
4	Incidentes cibernéticos (por ejemplo, ciberdelincuencia, interrupciones de redes y servicios informáticos, malware / ransomware, violación de datos, multas y sanciones).	30%	1 (72%)	↓
5	Riesgos políticos y violencia (por ejemplo, inestabilidad política, guerra, terrorismo, golpe de Estado, conmoción civil, huelgas, disturbios, saqueos).	27%	NUEVO	↑
6	Cambio climático (por ejemplo, riesgos físicos, operativos y financieros como consecuencia del calentamiento global).	22%	3 (28%)	↓
7	Desarrollos macroeconómicos (por ejemplo, inflación, deflación, políticas monetarias, programas de austeridad).	19%	4 (22%)	↓
8	Robo, fraude, corrupción.	14%	8 (11%)	→
9	Crisis energética (por ejemplo, escasez/corte del suministro, fluctuaciones de precios).	11%	4 (22%)	↓
10	Evolución del mercado (por ejemplo, competencia intensificada/nuevos participantes, fusiones y adquisiciones, estancamiento del mercado, fluctuación del mercado).	11%	NUEVO	↑

Nota. Esta imagen podemos identificar la seguridad de la llave cifrada, en este caso con método SFTP, en la capa 3, Tomado de. Ramon Invarato. (2019). Cómo funcionan los Servidores y Servicios de Hosting. jarroba.com. https://jarroba.com/como-funcionan-los-servidores-y-servicios-de-hosting/

Desarrollo del Objetivo 3

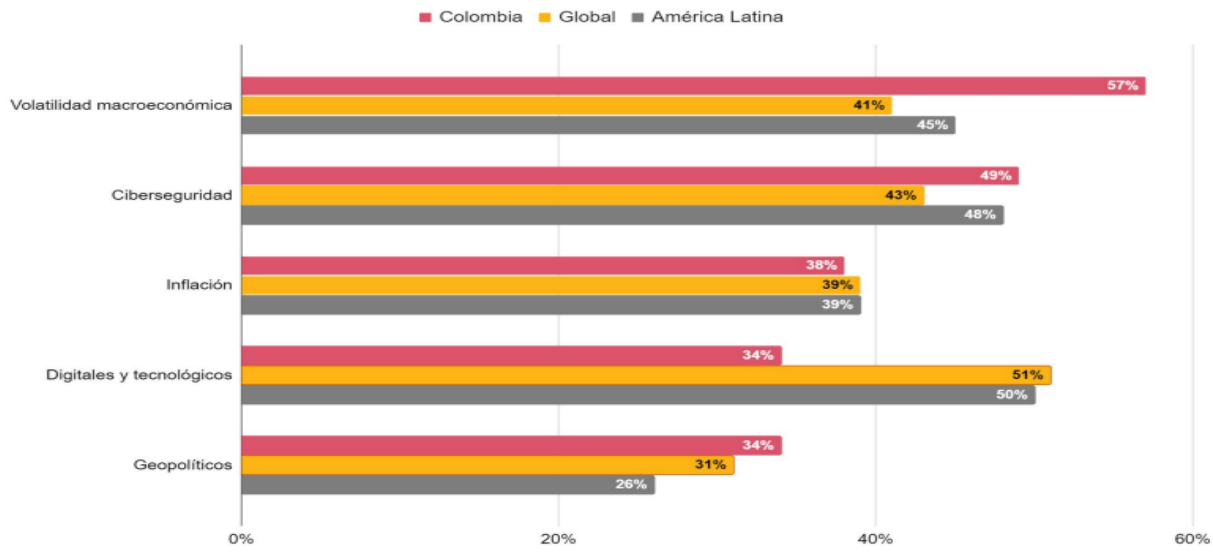
Seleccionar controles de seguridad recomendados según las mejores prácticas, orientados a la reducción del riesgo relacionado con la ingeniería social.

En Colombia, los riesgos de ciberseguridad son percibidos como menos importantes que los relacionados con la volatilidad macroeconómica. A nivel global, el riesgo cibernético se sitúa detrás de los riesgos digitales y tecnológicos. Los líderes en Colombia están enfocados en enfrentar los problemas económicos actuales, lo que, podría aumentar la exposición a ciberataques.

En contraste, se considera que los riesgos digitales, tecnológicos y de ciberseguridad están más interconectados.

Figura 17

Comparativo Colombia, Global y América Latina

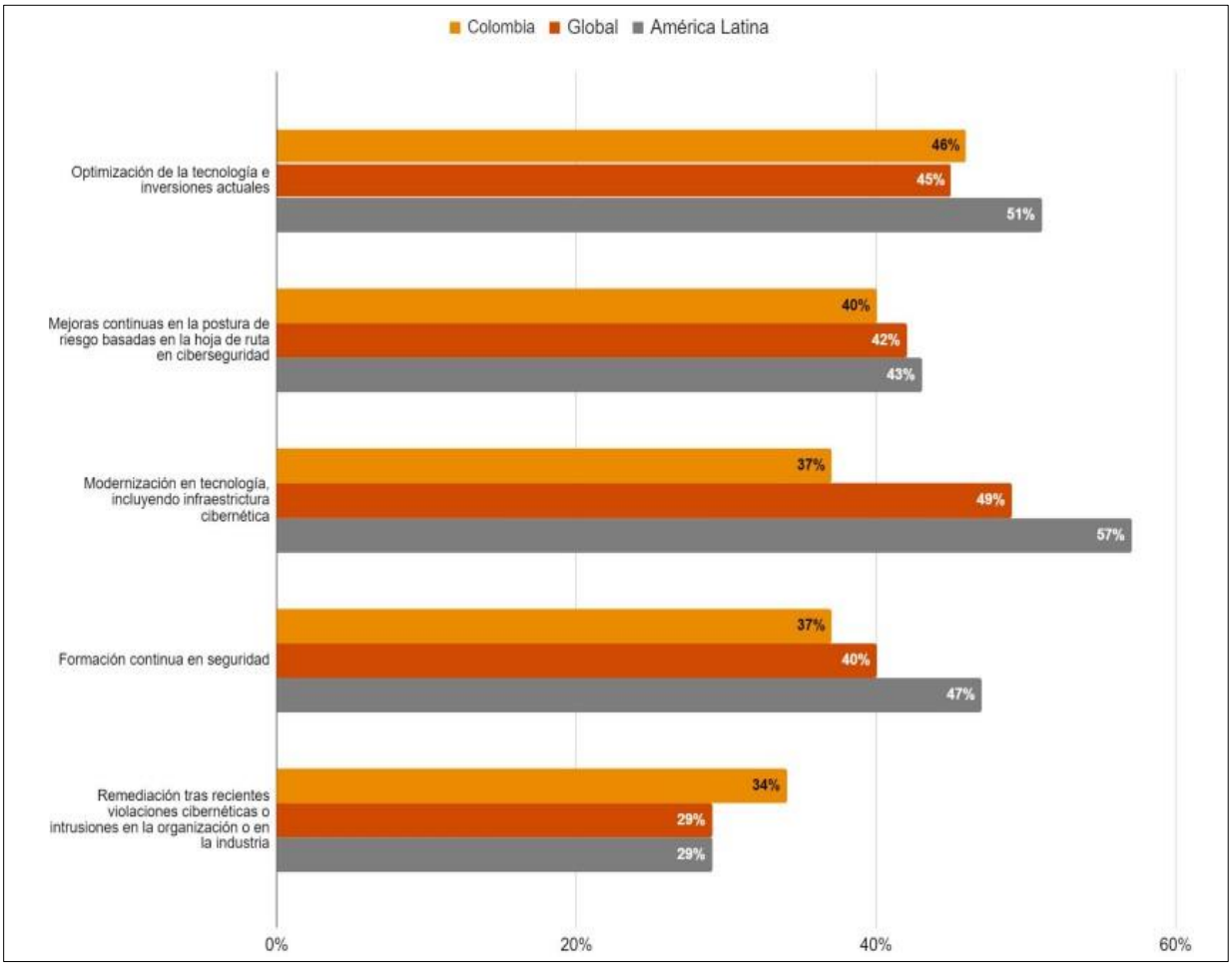


Nota. En la imagen podemos observar Riesgos priorizados para las empresas a corto plazo Tomado de. PwC Colombia. (2024). Digital trust insights 2024. https://www.pwc.com/co/es/publicaciones/digital-trust-insights/2024/digital-trust-insights-2024-pwc-colombia.pdf

La modernización y optimización son las principales prioridades de inversión en ciberseguridad para 2024. Casi la mitad de los líderes empresariales a nivel mundial (49%) y el 37% en Colombia priorizan la modernización tecnológica, que abarca la infraestructura cibernética. Además, el 45% de los encuestados globalmente y el 46% en Colombia se enfocan en optimizar las tecnologías e inversiones ya existentes.

Figura 18

Modernización Tecnológica



Nota. Imagen de presupuesto para ciberseguridad en 2024 tiene como objetivo aprovechar al máximo las herramientas existentes. Tomado de. PwC Colombia. (2024). Digital trust insights 2024. https://www.pwc.com/co/es/publicaciones/digital-trust-insights/2024/digital-trust-insights-2024-pwc-colombia.pdf

En la encuesta de Global Digital Trust Insights de 2024 de PwC Colombia del 2024, el 44% de los participantes a nivel global y el 28% en Colombia señalaron que utilizan un conjunto integrado de soluciones de ciberseguridad. Además, el 39% a nivel mundial y el 45% en Colombia tiene la intención de adoptar un conjunto integrado en los próximos dos años. Esto indica que casi el 20% de los encuestados considera que tiene demasiadas soluciones y que es necesario consolidarlas.

Controles de la Ingeniería Social

La prevención de la ingeniería social en una empresa requiere políticas de seguridad sólidas, capacitación regular de empleados, uso de tecnologías avanzadas y una cultura organizacional que valore la seguridad de la información. La educación es clave para que los empleados reconozcan y resistan intentos de manipulación.

La seguridad organizacional es un esfuerzo continuo que combina tecnología y participación de los empleados, la ingeniería social en empresas implica la manipulación psicológica para obtener información confidencial o acceso no autorizado, explotando debilidades en la seguridad de la información a través de interacciones con empleados, clientes o colaboradores.

A continuación, se presentará un ejemplo de algunos ataques de ingeniería social, junto con sus riesgos y controles. Esto nos permitirá comprender cómo podemos enfrentarlos antes y después de que ocurran, teniendo en cuenta diversas recomendaciones y aplicándolas adecuadamente.

Tabla 4

Controles y Riesgos de la Ingeniería Social

Técnicas	Descripción	Riesgos	Controles
Phishing	El envío de correos electrónicos falsos que parecen legítimos, para engañar a los destinatarios para que revelen información confidencial.	*Filtración de información confidencial *Daño a la reputación *Violación de la privacidad *Pérdida financiera *Suplantación de identidad *Acceso no autorizado a sistemas y redes *Riesgos operativos *Correo malicioso y programa maligno *Acosos sexuales online o físicos	Educación y Concientización Programas de Capacitación Simulacros de Phishing Políticas de Seguridad Controles de Acceso Autenticación de Dos Factores (2FA) -MFA Filtros de Correo Electrónico Antivirus y Antimalware Contraseñas fuertes y difíciles Revisión y Monitoreo de Accesos Restricciones en el Uso de USB Actualizaciones y Parches Mantenimiento Regular de Hardware y Software Promoción de la Seguridad Pruebas de Penetración Evaluaciones Regulares de conocimientos básicos en seguridad
Ingeniería social telefónica	Llamadas fraudulentas para obtener información confidencial.		
Suplantación de identidad	Pretender ser quien no es, con el fin de obtener acceso autorizado o información sensible.		
Infiltración física	Acceder físicamente a instalaciones sin autorización aprovechando descuidos.		

Técnicas	Descripción	Riesgos	Controles
USB drops	Dispositivos USB infectados que se dejan en lugares estratégicos para que la persona que los encuentre los conecte a sus sistemas críticos.		

Nota. Tabla donde podemos identificar riesgos y controles de la ingeniería social.

Para mitigar estos riesgos, es crucial implementar medidas de seguridad sólidas, educar a los empleados, fomentar la conciencia de seguridad y usar tecnologías avanzadas. La ciberseguridad debe abordar tanto la tecnología como el factor humano.

ISO27002

Con la ISO27002 es un complemento que se puede llevar con al ISO27001 lo que aplicaremos será recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

Políticas de Seguridad

Organización de la Seguridad de la Información: teniendo en cuenta; la organización interna y los dispositivos móviles y teletrabajo

Seguridad de los Recursos Humanos

Para validación se debe de tener en cuenta el personal también la contratación que sean personas responsables, medidas de seguridad ante despidos Finalización y cambio de contrato y demás.

Gestión de los Activos

Aquí podemos ver la clasificación de la información manipulación manejos de soportes de almacenamiento (gestión de soporte extraíbles, eliminación y soportes físicos en tránsito).

Responsabilidad por los activos

Clasificación de la información

Manejo de los medios de comunicación

Control de Accesos

Los accesos de los usuarios son muy necesario no solo para ingresar a la sede sino también para poder usar; aplicaciones y sistemas:

Requisitos empresariales para el control de acceso

Gestión del acceso en usuarios

Responsabilidades del usuario

Control de acceso en sistemas y aplicaciones

Cifrado

Seguridad Física y Ambiental

Controles de entrada o acceso, controles para amenazas externas y ambientales, mantenimiento de equipos, copias de seguridad, manejo de equipos en home office, seguridad de equipos de almacenamiento políticas de seguridad de información bloqueo de pantalla, no compartir información confidencial, entre otras.

Seguridad de las Operaciones

Seguridad en los equipos sistemas operativos, procedimientos y responsabilidades, protección contra malware, antivirus, copias de resguardo, auditoria de sistemas de información.

Procedimientos y responsabilidades operativas

Protección ante programa maligno

Copias de seguridad

Registros y monitoreo

Control del software operacional

Gestión del as vulnerabilidades técnicas

Consideraciones en auditorias de sistemas

En este caso como se ha expandido la empresa se debe de tener seguridad también con proveedores, adicional validando los aspectos técnicos se debería de colocar la contraseña expire por seguridad y evitar que cualquier persona pueda obtener acceso y tener confidencialidad, integridad de los datos.

Seguridad de las Comunicaciones

Seguridad de la red, lo que podemos recomendar, es que el servidor sea Linux o windows envíe un archivo cifrado con la llave publica al servidor SFTP en la nube, para así tener más seguridad manejando un cifrado asimétrico.

Ambos servidores cuentan con un router y firewall a nivel de capa 3, en el siguiente diagrama se visualiza la infraestructura propuesta para la transferencia segura de la información.

Relaciones con los Proveedores

Seguridad de la información en las relaciones con los proveedores.

Seguridad de la información en las relaciones con proveedores

Gestión de la entrega con proveedores

Se identifica que todos los equipos disponen de sistema antivirus que se actualiza con una periodicidad diaria de manera automática. Todos los equipos disponen de conexión a Internet. Se

trata de una conexión ADSL con un router que dispone de funcionalidades de cortafuegos, que es algo estrictamente necesario y se está cumpliendo.

La empresa puede realizar copias de seguridad del servidor semanalmente en cintas magnéticas o en un servidor web. Estas copias deben almacenarse de forma segura, siguiendo las recomendaciones de la ISO 27032 y la ISO 27002, que sugieren buenas prácticas de almacenamiento de información. Es importante considerar posibles pérdidas de datos debido a desastres ambientales, extravío de discos o fallos en el método de almacenamiento. Se recomienda utilizar una nube paga que cumpla con las normas de seguridad ISO para mayor protección.

Desarrollo del Objetivo 4

Proponer estrategias para contrarrestar la ingeniería social que fortalezcan las capacidades del talento humano en las empresas del sector privado.

Nuevas Estrategias Ciberdefensa IA

La inteligencia artificial generativa está abriendo nuevas oportunidades para las organizaciones y sus estrategias de ciberseguridad, como lo indican los más de 3,800 ejecutivos que participaron en nuestra encuesta este año. Sin embargo, su adopción debe estar respaldada por un adecuado gobierno, responsabilidad y gestión del riesgo. Según el estudio, el 69% de los altos directivos planea implementar la IA generativa en sus estrategias de ciberseguridad en el próximo año. No obstante, es probable que su uso también genere un aumento en las ciberamenazas y facilite ataques a gran escala. De hecho, el 52% de los encuestados anticipa que la implementación de IA generativa provocará ciberataques de alto impacto en el próximo año.

Figura 19

IA Generativa Para la Ciberdefensa

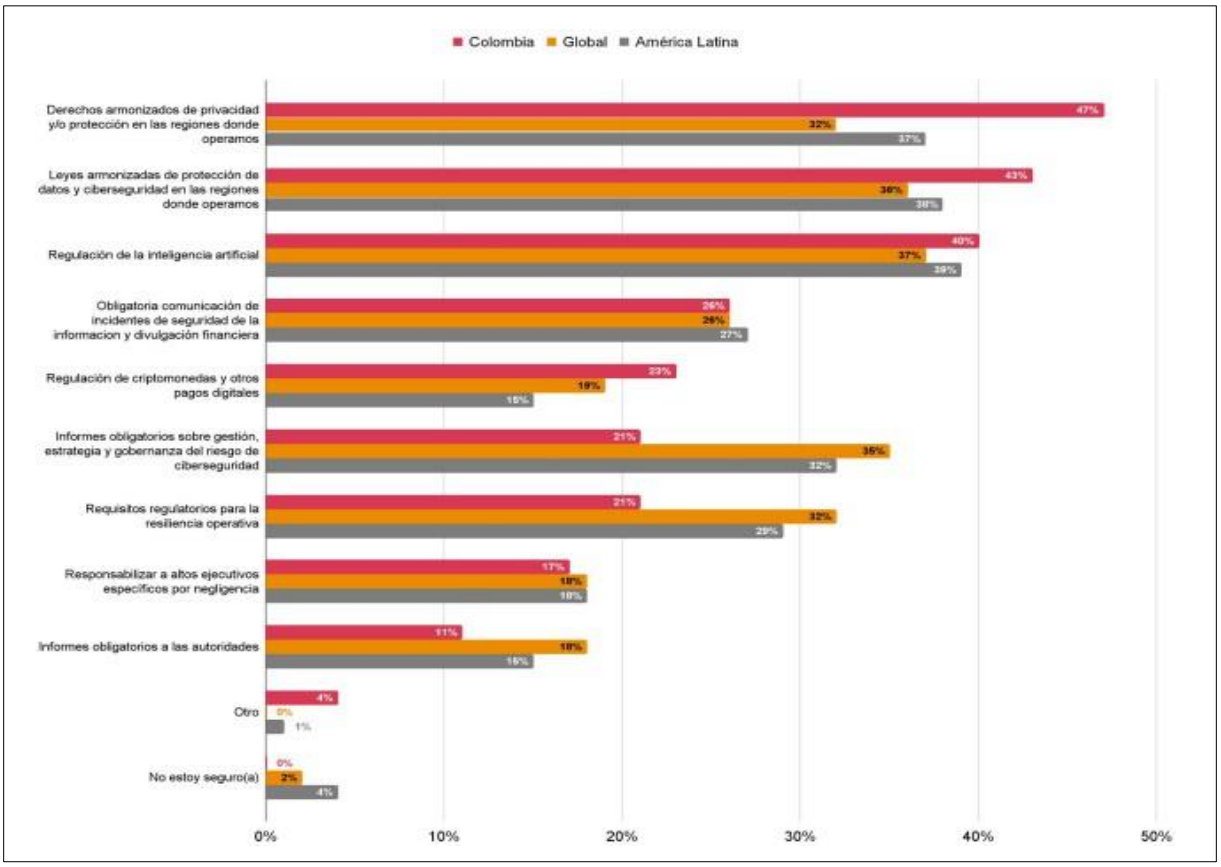
Nota. Esta imagen podemos identificar la IA como generativa para la ciberdefensa, oportunidad para Colombia, *Fuente.* PwC Colombia. (2024). Digital trust insights 2024. https://www.pwc.com/co/es/publicaciones/digital-trust-insights/2024/digital-trust-insights-2024-pwc-colombia.pdf

Posibles Estrategias para Contrarrestar la Ingeniería Social

Cerca de un tercio de los encuestados este año señala que cuatro tipos de regulación serán clave para el crecimiento futuro de sus organizaciones: regulación de la inteligencia artificial (37%), armonización de leyes de ciberseguridad y protección de datos (36%), informes obligatorios sobre ciberseguridad, gestión de riesgos y gobernanza (35%), y requisitos de resiliencia operativa (32%).

Figura 20

Regulaciones que Podrían Cambiar la Ciberseguridad



Nota. Esta imagen podemos ver objetivo y principios regulatorios con mayor impacto en el crecimiento futuro de los ingresos de la organización la IA como generativa para la ciberdefensa, oportunidad para Colombia, Tomado de. PwC Colombia. (2024). Digital trust insights 2024. https://www.pwc.com/co/es/publicaciones/digital-trust-insights/2024/digital-trust-insights-2024-pwc-colombia.pdf

La transparencia se está convirtiendo en un enfoque regulatorio más fuerte a nivel mundial. Las nuevas normativas de la SEC requieren la divulgación pública de incidentes de ciberseguridad que puedan afectar a los inversionistas. Asimismo, la Ley de Mercados Digitales y la Ley de Servicios Digitales demandan transparencia en el manejo de datos y en la toma de decisiones algorítmicas. También se están desarrollando regulaciones sobre la IA, incluyendo una ley de IA de la Unión Europea en elaboración y normativas específicas para la IA generativa.

Capacitación de Recurso Humano

El hurto más denunciado en Colombia es el Hurto por medios informáticos, cuentas bancarias, dispositivos que se relacionan con la banca, entre otras. Aquí viene la capacitación del recurso humano en los conocimientos básicos del cuidado o privacidad de su información, lo que se publica, la facilidad de contraseñas, saber a quién se le abrirá la puerta para que conozca lo que tiene y lo que es, la identidad o reputación virtual es muy importante en la actualidad ya que todo lo que se realiza en el ciberespacio se puede ver, un ciber atacante lo puede ver y usar a su antojo, por ello es tan importante que las personas tengan conocimiento de cómo pueden hacer que su data este a salvo.

De acuerdo a González Guzmán, D. A. (2017), Señala que: “Es un estudio del dato y la información como objeto material en el tipo penal hurto por medios informáticos”.

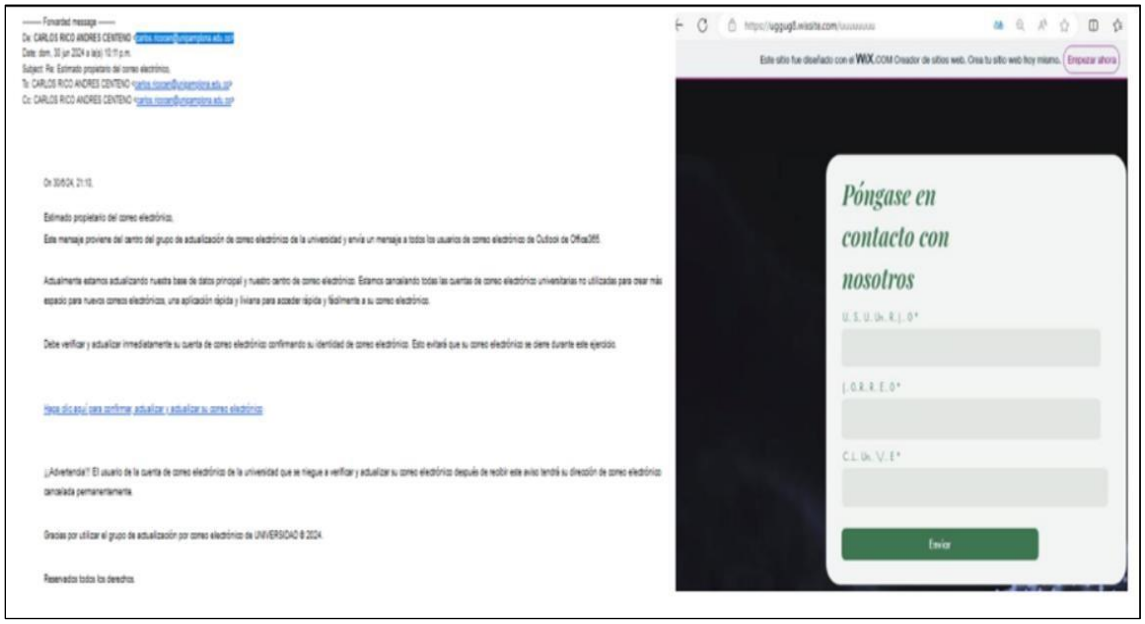
Pruebas con Ejemplos de Correo Malicioso

Como se observó anteriormente, la ingeniería social incluye varios ataques significativos, siendo uno de ellos el correo malicioso. Se han identificado algunos ataques que se utilizarán como ejemplos para ilustrar este tipo de amenaza. Según MITRE, el código T1566 es correspondiente a la técnica de correo malicioso.

Es preciso indicar que la técnica de correo malicioso es un tipo de ataque cibernético en el cual los adversarios intentan engañar a los usuarios para que revelen información confidencial. Por lo tanto, se recomienda no ingresar sus credenciales cuando reciba mensajes que le soliciten acceder supuestamente al correo electrónico de Outlook de Office 365 y lo redirijan a una página sospechosa electrónico de Outlook de Office 365 y lo redirijan a una página sospechosa, como este ejemplo:

Figura 21

Ejemplo Phishing Office 365



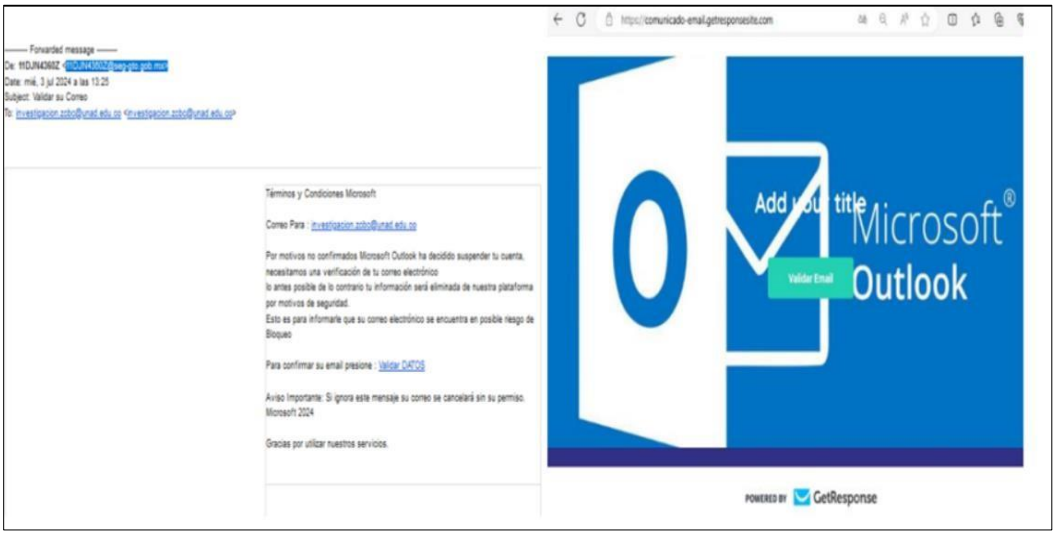
Nota. Esta imagen podemos ver un ejemplo de correo malicioso de Office. Tomado de. Universidad Nacional Abierta y a Distancia. (n.d.). Alertas de ciberseguridad. CSIRT UNAD. Recuperado de https://csirt.unad.edu.co/alertas-de-ciberseguridad

Al igual que con otros servicios, se recomienda no ingresar sus credenciales cuando reciba mensajes que le soliciten acceder supuestamente al correo electrónico de Microsoft Outlook y lo redirijan a esta página: h##ps://comunicado-email.getresponsesite.com#/. Como se

puede ver en la imagen, la URL no corresponde a Microsoft Outlook, o más abajo la de Google donde llegan mensajes con supuestas ratificaciones de persecución de delitos electrónicos de la policía adjuntando un pdf que redirecciona a otra página que solicita las credenciales con URL https://accounts.google.com/v3/signin/identifier?continue=https%3A%2F%2Fmail.google.com%##2#

Figura 22

Correo Malicioso de Outlook



Nota. Esta imagen podemos ver un ejemplo de correo malicioso de Outlook, Tomado de. Universidad Nacional Abierta y a Distancia. (n.d.). Alertas de ciberseguridad. CSIRT UNAD. Recuperado de https://csirt.unad.edu.co/alertas-de-ciberseguridad

En otro ejemplo, en este podemos evidenciar que llegan notificaciones de Facebook que redirigen a la cuenta h##ps://feedbackissue-recheck-service.web.app#/, como se ve en la imagen, la cual es completamente diferente. Por lo tanto, se recomienda no ingresar sus credenciales cuando reciba mensajes de una supuesta “Notificación de desactivación de cuenta publicitaria - Solicita una revisión ahora” de Facebook o como en la segunda imagen notificación de demanda judicial que adjunta un pdf que pide todos los datos personales.

Figura 23

Correo Malicioso Facebook

Nota. Esta imagen podemos ver un ejemplo de correo malicioso de Facebook que nos redirige a otra página diferente para solicitar datos personales. Tomado de. Universidad Nacional Abierta y a Distancia. (2024.). Alertas de ciberseguridad. CSIRT UNAD. Recuperado de https://csirt.unad.edu.co/alertas-de-ciberseguridad

Figura 24

Correo Malicioso Notificación de Demanda

Nota. Esta imagen podemos ver un ejemplo de correo informa que es una notificación de demanda judicial, *Fuente.* Universidad Nacional Abierta y a Distancia. (2014.). Alertas de ciberseguridad. CSIRT UNAD. Recuperado de https://csirt.unad.edu.co/alertas-de-ciberseguridad

Monitoreo de la Dark Web

Los servicios de monitoreo de la Dark Web son esenciales para descubrir datos personales robados y protegerse contra el robo de identidad, se realiza con un escaneo de sitios web alojados en rincones ocultos, a estos sitios solo se puede acceder a través del navegador Tor, lo que hace que el monitoreo sea crucial.

En abril de 2024, se filtraron datos personales de 2.900 millones de ciudadanos estadounidenses en la Dark Web.

Ranking de Empresas más Suplantadas

El correo malicioso es un tipo de fraude informático muy común que puede comprometer la privacidad tanto de personas como de empresas.

Los avances tecnológicos han llevado a los ciberdelincuentes a buscar nuevas estrategias para obtener datos personales de los usuarios y cometer delitos informáticos, como vaciar cuentas bancarias, con poco esfuerzo.

A continuación, se presenta el último ranking de correo malicioso de marcas correspondiente al segundo trimestre de 2024. Una de las empresas más conocidas por la suplantación es Check Point Research, la división de Inteligencia de Amenazas de Check Point Software Technologies Ltd. (Check Point Research, 2024).

Microsoft (57 %)

Apple (10 %)

LinkedIn (7 %)

Google (6 %)

Facebook (1,8 %)

Amazon (1,6 %)

DHL (0,9 %)

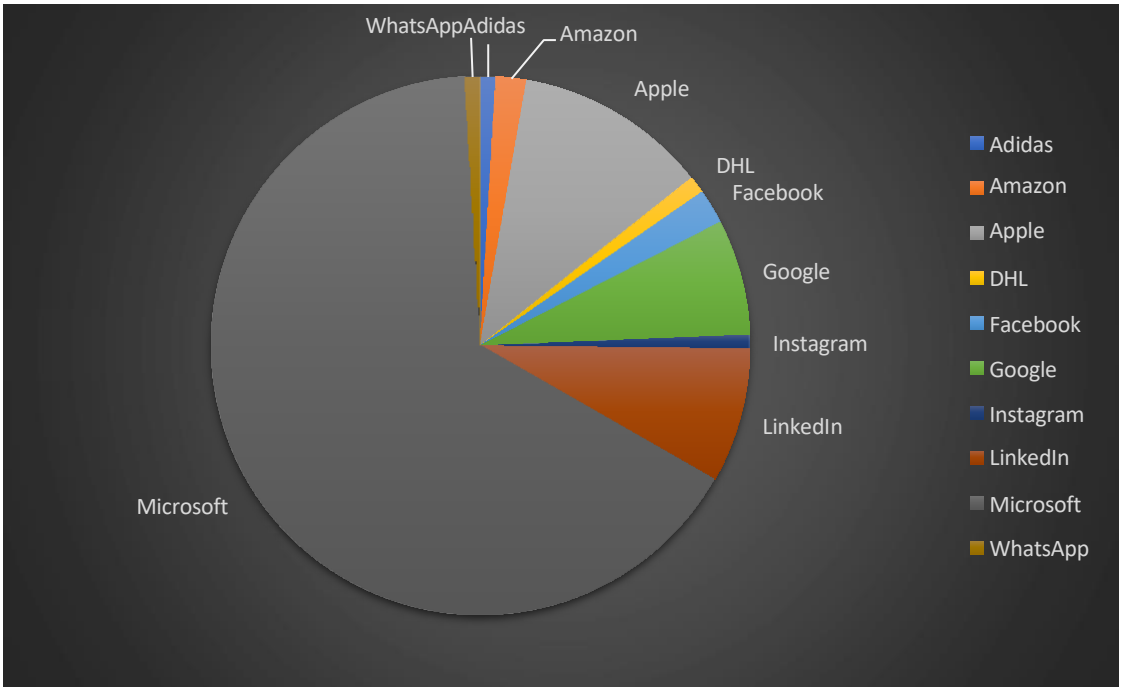
Adidas (0,8 %)

WhatsApp (0,8 %)

Instagram (0,7 %)

Figura 25

Top 10 Correo Malicioso 2024



Nota. Esta imagen nos permite tener una visual más amplia del top 10 de marcas de phishing para el segundo trimestre de 2024. Tomado de. Semana. (2024, septiembre 13). ¿Qué marcas encabezan el ranking de las más suplantadas por los ciberdelincuentes en 2024? Semana. https://www.semana.com/tecnologia/articulo/que-marcas-encabezan-el-ranking-de-las-mas-suplantadas-por-los-ciberdelincuentes-en-2024/202410/

Algunos Servicios de Monitoreo

Existen muchas empresas que pueden prestar servicios de monitoreo a estas páginas entre los cuales están:

eSentire: Ofrecen monitoreo continuo de la dark web para proteger datos sensibles de empleados, ejecutivos y clientes.

Aura: Proporcionan monitoreo de la dark web para detectar datos personales filtrados y ofrecen alertas en tiempo real.

CyberSecOp: Su plataforma de inteligencia cibernética monitorea la deep web y dark web para detectar credenciales robadas y otros datos sensibles.

Capacitaciones de Personal

Se recomienda tener capacitaciones al personal de ciberseguridad, cibercuidado y herramientas de inteligencia digital, para poder disfrutar del internet y sacarle provecho, entre esto podemos realizar boletines informativos, podcast y capacitaciones.

Entre estas se pueden adquirir certificados gratuitos en la MINTIC, en DOJA y aún existen campañas en varios universidad des con el ice tex para poder tener estos conocimientos sin costos.

Herramientas Tecnológicas para Evitar Riesgos de Autenticación

La ciberseguridad es crucial en la era digital debido al aumento de amenazas cibernéticas, por esto debemos de proteger los sistemas y datos de una organización requiere herramientas tecnológicas y buenas prácticas.

Métodos de Autenticación MFA

Un factor de autenticación es una categoría de credencial utilizada para verificar la identidad. En la autenticación multifactor (MFA), cada factor adicional aumenta la seguridad, existen tres categorías MFA combina dos o más de estos factores para mejorar la seguridad, las más comunes que son:

Factor de conocimiento: Se maneja con preguntas de seguridad, pin o OTP

Factor de posesión: como una insignia, un token, un llavero o una tarjeta de módulo de identidad de suscriptor (SIM) de teléfono.

Factor de herencia: Cualquier rasgo biológico único de cada usuario:

- Escaneo de retina o iris
- Escaneo de huellas dactilares
- Autenticación por voz
- Geometría de la mano
- Escáneres de firmas digitales
- Reconocimiento facial
- Geometría del lóbulo de la oreja

Conclusiones

En cuanto al primer objetivo específico, se identificaron las características de los riesgos de ciberseguridad organizacional. Esto facilitará a los responsables de los procesos estratégicos, misionales, de apoyo y de evaluación y control, precisar las medidas de seguridad que podrían ser factibles para contrarrestar el impacto de la materialización de estos riesgos, con relación al segundo objetivo específico, se establecieron medidas de control que permiten garantizar la ciberseguridad organizacional. Estas medidas se desarrollaron mediante las recomendaciones y políticas, que, armonizadas con la gestión del conocimiento y la auditoría forense, blindan a las empresas modernas frente a cualquier ciberataque.

En cuanto al tercer objetivo específico, se analizaron las competencias del talento humano para la administración de la ciberseguridad organizacional. Se determinó que la gestión del conocimiento es la principal fuente que provee los perfiles idóneos. Al conjugarse con el seguimiento de recomendaciones de las normas internacionales y buenas prácticas de seguridad informática y ciberseguridad, se garantiza la capacidad instalada para la efectiva implementación de las medidas de control de prevención frente al nivel de exposición de los riesgos en los procesos de la organización.

Por último, en relación con el objetivo de valor agregado de la investigación, se formularon lineamientos para el mejoramiento de la ciberseguridad organizacional. A partir de la gestión del conocimiento del talento humano y la implementación de medidas como la encriptación de contraseñas y el uso de autenticación de doble factor, se puede fortalecer significativamente la seguridad de la información en las organizaciones del sector privado, los responsables de los procesos sujetos a riesgos por ciberataques podrán implementar políticas y procedimientos para prevenir la materialización de estos.

Los ataques de ingeniería social tienen un mayor éxito debido al error humano, la confianza o la falta de capacitación de las personas, lo cual aumenta el impacto de estos ataques. Al manejar buenas prácticas, tendremos una metodología de gestión de seguridad bien estructurada.

Con las prácticas de la ISO 27001 y la ISO 27032 reduciremos el riesgo de pérdida, filtración y robo de información. Si se desea que todos los clientes internos y externos tengan acceso limitado o mediante permisos a las aplicaciones o accesos, debemos implementar varias prácticas de seguridad documentadas en este informe.

El análisis realizado ha permitido identificar diversas vulnerabilidades, amenazas y riesgos asociados con la ingeniería social que afectan a las empresas del sector privado en Colombia. Se ha evidenciado que los ataques más comunes, respaldados por estadísticas, incluyen técnicas como el phishing y el pretexting, que explotan la confianza y el comportamiento humano.

La revisión de la normativa vigente ha revelado la existencia de buenas prácticas de seguridad que, aunque están establecidas, presentan brechas en su implementación. Es fundamental que las empresas del sector privado adopten estas prácticas y realicen auditorías periódicas para asegurar el cumplimiento y la efectividad de sus políticas de seguridad.

Se ha destacado la importancia de seleccionar e implementar controles de seguridad adecuados basados en las mejores prácticas reconocidas internacionalmente. Estos controles deben ser orientados específicamente a mitigar los riesgos asociados con la ingeniería social, lo que incluye capacitación continua para los empleados y el uso de tecnologías de seguridad avanzadas.

Las propuestas de estrategias para contrarrestar la ingeniería social subrayan la necesidad de fortalecer las capacidades del talento humano dentro de las organizaciones. La formación y sensibilización de los empleados son cruciales para crear una cultura de seguridad sólida, que permita a los trabajadores reconocer y responder adecuadamente a posibles intentos de manipulación.

Finalmente, el estudio concluye que la gestión de la ciberseguridad y los riesgos relacionados con la ingeniería social debe ser un proceso dinámico y continuo. Las empresas deben estar dispuestas a adaptarse a las nuevas amenazas y a revisar y actualizar sus estrategias y metodologías de manera regular para mantener altos niveles de seguridad.

Recomendaciones

Una de las enseñanzas que nos ha dejado la pandemia es la necesidad de aprender y capacitarnos para cuidar nuestra información. Es prioritario realizar campañas de concientización sobre el cuidado que se debe tener al usar el ciberespacio. Las compañías deben optar por estrategias de ciberseguridad enfocadas en la protección de datos personales, empresariales y cualquier otro activo valioso.

Así como existen riesgos en el mundo físico al mostrar lo que poseemos, en el mundo virtual ocurre lo mismo. Cuanto más discretos seamos y menos información compartamos, mejor podremos proteger nuestros activos.

Es fundamental contar con un plan de acción robusto para evitar brechas de seguridad y contrarrestar los ataques. Todas las compañías y personas tienen un alto riesgo de sufrir ataques que puedan filtrar información confidencial. Por ello, es importante clasificar los datos y documentos, establecer quiénes deben garantizar su seguridad e implementar políticas internas para protegerlos. Con una correcta clasificación de la información y el uso de herramientas adecuadas, las compañías podrán detectar fácilmente cualquier fuga de información y tomar medidas correctivas.

La mayoría de las empresas prefieren mantener en confidencialidad la pérdida de información para no dañar su reputación. Sin embargo, muchas han sufrido pérdidas o ataques por robo de información. Por lo tanto, es esencial que todas las empresas, ya sea que trabajen desde casa o en oficina, implementen programas para salvaguardar la información, también se recomienda:

Capacitación continua: Realizar entrenamientos regulares para empleados sobre las últimas amenazas y técnicas de ingeniería social.

Autenticación multifactor: Implementar autenticación de doble factor para acceder a sistemas críticos.

Políticas de acceso: Limitar el acceso a la información sensible solo a aquellos empleados que realmente lo necesiten.

Auditorías regulares: Realizar auditorías internas y externas para asegurar el cumplimiento de las políticas de seguridad.

Actualización constante: Mantener todos los sistemas y software actualizados para protegerse contra vulnerabilidades conocidas.

Simulaciones de ataques: Realizar simulaciones de ataques de ingeniería social para evaluar la preparación de la empresa y mejorar las respuestas.

Estas prácticas no solo ayudarán a proteger la información, sino que también fortalecerán la confianza de clientes y socios, mejorando la reputación y la seguridad general de la empresa.

Referencias

Revista El Mundo Cambio. (2024, septiembre 10). Colombia, tercer país en Latinoamérica con más ataques de ingeniería social. *Revista El Mundo Cambio*. https://revistaelmundocambio.com/2024/09/10/colombia-tercer-pais-en-latinoamerica-con-mas-ataques-de-ingenieria-social/

Brush, K., Rosencrance, L., & Cobb, M. (2021). Asymmetric cryptography (public key cryptography). https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography

TechTarget. (n.d.). Asymmetric cryptography (public key cryptography). TechTarget. https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography

Córdoba, D. (2016, noviembre 8). RSA: ¿Cómo funciona este algoritmo de cifrado? Junco TIC. https://juncotic.com/rsa-como-funciona-este-algoritmo/

El Heraldo. (2017, mayo 15). Ciberataque golpeó a 11 empresas y una entidad pública en Colombia. El Heraldo. https://www.elheraldo.co/ciencia-y-tecnologia/ciberataque-golpeo-11-empresas-y-una-entidad-publica-en-colombia-361747

Durán, A. M. (2017, junio 28). En Colombia hay 12 empresas afectadas por ciberataque mundial. El Tiempo. http://www.eltiempo.com/tecnosfera/novedades-tecnologia/numero-de-empresas-afectadas-en-colombia-por-ciberataque-mundial-103550

El Tiempo. (2018, octubre 23). Los temas claves de cita de Duque con el secretario general de la OTAN. El Tiempo. https://www.eltiempo.com/politica/gobierno/los-temas-claves-de-cita-de-duque-con-el-secretario-general-de-la-otan-284598

Arango, M. P. (2019, octubre 30). Reporte de ciberataques en Colombia 2019 de Policía Nacional y CCIT. El Tiempo. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790

Méndez, A. L. (2020, abril 23). Coranavirus, fraude bancario: le robaron sus ahorros con una llamada. El Tiempo. https://www.eltiempo.com/justicia/servicios/coranavirus-fraude-bancario-le-robaron-sus-ahorros-con-una-llamada-487340

Cruz, A. (2020, abril 15). Millones de cuentas de Zoom se venden en la dark web. El Universal. https://www.eluniversal.com.mx/techbit/millones-de-cuentas-de-zoom-se-venden-en-la-dark-web

GeeksforGeeks. (n.d.). RSA algorithm in cryptography. GeeksforGeeks. https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

INCIBE. (n.d.). Phishing. INCIBE. https://www.incibe.es/protege-tuempresa/tematicas/phishing

Jiménez Arteaga, A. (n.d.). https://documen.site/download/lectura-10-ing-aldo-jimenez-arteaga_pdf

Jimenez, J. (2020). Ataque de puerta trasera: qué es, cómo afecta y cómo evitarlo. RedesZone. https://www.redeszone.net/tutoriales/seguridad/puertas-traseras-evitar-problemas/

KRIPKIT. (2022). Ataque con texto cifrado elegido. https://kripkit.com/ataque-con-texto-cifrado-elegido/

Anónimo. (n.d.). LAB: Reflected XSS into HTML context with nothing encoded. Web Security Academy. PortSwigger. https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded

Normas ISO. (2019). ISO 27000. https://www.normasiso.net/wp-content/uploads/2016/10/iso-27000.pdf

Invarato, R. (2019). Cómo funcionan los servidores y servicios de hosting. Jarroba. https://jarroba.com/como-funcionan-los-servidores-y-servicios-de-hosting/

Segu-info. (2024). Detección de intrusiones en tiempo real. http://www.segu-info.com.ar/proteccion/deteccion.htm

Velimirovic, A. (2021). 16 encryption key management best practices. PhoenixNAP. https://phoenixnap.com/blog/encryption-key-management-best-practices

Buja, A. G., Low, N. N. M. A., Zolkeplay, A. F., Azam, N. A., & Isa, F. M. (2024). Analysis of web vulnerability using open-source scanners on different types of small entrepreneur web applications in Malaysia. Journal of Advanced Research in Applied Sciences and Engineering Technology, 40(1), 174–188. https://doi.org/10.37934/araset.40.1.174188

Carrillo, M. R. (2023). The European Union strategy for cybersecurity. In Law, governance and technology series (pp. 173–192). https://doi.org/10.1007/978-3-031-40516-7_10

Chiara, P. G. (2024). Towards a right to cybersecurity in EU law? The challenges ahead. Computer Law and Security Report, 53, 105961. https://doi.org/10.1016/j.clsr.2024.105961

Fernández, R. (2024). Evaluation of trust service and software product regimes for zero-knowledge proof development under eIDAS 2.0. Computer Law and Security Report, 53, 105968. https://doi.org/10.1016/j.clsr.2024.105968

Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. Journal of Industrial Information Integration, 39, 100604. https://doi.org/10.1016/j.jii.2024.100604

Pérez, S. R. (2024). Litigios sobre difamación por internet. Comentarios a la SAP Madrid 10 febrero 2023. Cuadernos De Derecho Transnacional, 16(1), 900–915. https://doi.org/10.20318/cdt.2024.8454

Dirección de Investigación Criminal e Interpol. (2023). Centro Cibernético Policial. https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202023_0.pdf

Kabul, E. G., Çalık, B. B., Özcan, N. T., & Gürsoy, S. (2024). Investigation of the adaptation of older adults to online learning and artificial intelligence. Revista Española De Geriatría Y Gerontología, 59(4), 101477. https://doi.org/10.1016/j.regg.2024.101477

Toledano, B. (2020, July 23). TikTok, en el punto de mira por la presencia de pederastas en su red social. EL MUNDO. https://www.elmundo.es/tecnologia/2020/07/23/5f18329921efa04b168b4620.html

Jimenez, J. (2020). Ataque de puerta trasera: qué es, cómo afecta y cómo evitarlo. https://www.redeszone.net/tutoriales/seguridad/puertas-traseras-evitar-problemas/

KRIPKIT. (2022). Ataque con texto cifrado elegido.https://kripkit.com/ataque-con-texto-cifrado-elegido/

LAB: REFLECTED XSS into HTML context with nothing encoded | Web Security Academy [Anónimo]. Web Application Security, Testing, & Scanning - PortSwigger [página web]. [Consultado el 6, octubre, 2022]. https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded

Normas ISO. (2019). ISO 27000. https://www.normasiso.net/wp-content/uploads/2016/10/iso-27000.pdf (pp 2-5).

Ramon Invarato. (2019). Cómo funcionan los Servidores y Servicios de Hosting. jarroba.com. https://jarroba.com/como-funcionan-los-servidores-y-servicios-de-hosting/

Segu-info. (2024) Detección de intrusiones en tiempo real. http://www.segu-info.com.ar/proteccion/deteccion.htm

Velimirovic, A. (2021). 16 Encryption Key Management Best Practices. https://phoenixnap.com/blog/encryption-key-management-best-practices

Buja, A. G., Low, N. N. M. a. A., Zolkeplay, A. F., Azam, N. A., & Isa, F. M. (2024). Analysis of web vulnerability using Open-Source scanners on different types of small entrepreneur web applications in Malaysia. Journal of Advanced Research in Applied Sciences and Engineering Technology, 40(1), 174–188. https://doi.org/10.37934/araset.40.1.174188

Carrillo, M. R. (2023). The European Union Strategy for Cybersecurity. In *Law, governance and technology series* (pp. 173–192). https://doi.org/10.1007/978-3-031-40516-7_10

Chiara, P. G. (2024). Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law and Security Report/Computer Law & Security Report*, *53*, 105961. https://doi.org/10.1016/j.clsr.2024.105961

Fernández, R. (2024). Evaluation of trust service and software product regimes for zero-knowledge proof development under eIDAS 2.0. *Computer Law and Security Report/Computer Law & Security Report*, *53*, 105968. https://doi.org/10.1016/j.clsr.2024.105968

Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: a cybersecurity frameworks review. *Journal of Industrial Information Integration*, *39*, 100604. https://doi.org/10.1016/j.jii.2024.100604

Pérez, S. R. (2024). Litigios sobre difamación por internet. Comentarios a la SAP Madrid 10 febrero 2023. *Cuadernos De Derecho Transnacional*, *16*(1), 900–915. https://doi.org/10.20318/cdt.2024.8454

Dirección de investigación criminal e interpol. (2023). Centro Cibernetico Policial. https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202023_0.pdf

Kabul, E. G., Çalık, B. B., Özcan, N. T., & Gürsoy, S. (2024). Investigation of the adaptation of older adults to online learning and artificial intelligence. *Revista Española De Geriatría Y Gerontología*, *59*(4), 101477. https://doi.org/10.1016/j.regg.2024.101477

Toledano, B. (2020, July 23). TikTok, en el punto de mira por la presencia de pederastas en su red social. *ELMUNDO*. https://www.elmundo.es/tecnologia/2020/07/23/5f18329921efa04b168b4620.html

Universidad Nacional Abierta y a Distancia. (2024). Alertas de ciberseguridad. CSIRT UNAD. https://csirt.unad.edu.co/alertas-de-ciberseguridad

Semana. (2024, septiembre 13). ¿Qué marcas encabezan el ranking de las más suplantadas por los ciberdelincuentes en 2024? Semana. https://www.semana.com/tecnologia/articulo/que-marcas-encabezan-el-ranking-de-las-mas-suplantadas-por-los-ciberdelincuentes-en-2024/202410/

Techopedia. (2024). Estadísticas de ciberseguridad. https://www.techopedia.com/es/estadisticas-ciberseguridad

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). 1,2,3 por TIC. https://123portic.gov.co/829/w3-channel.html

Plan de Recuperación, Transformación y Resiliencia Gobierno de España. (2021). Qué es la inteligencia artificial. https://planderecuperacion.gob.es/noticias/que-es-inteligencia-artificial-ia-prtr

Centro Criptológico Nacional. (n.d.). MAGERIT - Versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. https://www.ccn-cert.cni.es/es/documentos-publicos/1789-magerit-libro-i-metodo/file?format=html

Grupo Atico34. (n.d.). Ingeniería social: Riesgos para los datos del individuo. https://protecciondatos-lopd.com/empresas/ingenieria-social/

Dongee. (2023). ¿Qué es la ingeniería social? Técnicas, riesgos, consejos. https://www.dongee.com/tutoriales/que-es-ingenieria-social/

Syneidis. (2018). Descubre qué es la ingeniería social, conoce sus riesgos. https://www.syneidis.com/es/social-engineering-risk/

Pirani Risk. (2022). Ingeniería social, ciberataques más comunes y cómo prevenirlos. https://www.piranirisk.com/es/blog/ingenieria-social-ciberataques-y-prevencion

Help Net Security. (2024, septiembre 6). *SaaS environments: Human firewall strategies*. https://www.helpnetsecurity.com/2024/09/06/saas-environments-human-firewall-strategies/

PwC Colombia. (2024). *Digital trust insights 2024*. https://www.pwc.com/co/es/publicaciones/digital-trust-insights/2024/digital-trust-insights-2024-pwc-colombia.pdf

Glosario

Amenaza: Objeto o acción que puede impactar negativamente la seguridad informática.

Ciberataque: Acción que normalmente usa medios digitales para atentar o causar un perjuicio a otra persona o entidad.

Ciberdelito: Es toda acción usando como objeto o medio un sistema informático, como la palabra lo dice es cibernético por (ciber) y es delictivo por (delito).

Ciberseguridad: Buenas prácticas o técnicas que permiten cuidar o no permiten que este en riesgo un activo en el ciberespacio.

Confidencialidad: Este es el significado de tener la seguridad de que algo es privado que se usa únicamente de forma que se autorice y no nadie debería de tomarla sin permiso o sin consentimiento propio las personas no autorizadas no tendrán acceso a ella.

Controles: Permite verificar, constatar, palpar, medir, si la actividad, proceso, unidad, elemento o sistema seleccionado está cumpliendo y/o alcanzando o no los resultados que se esperan.

Datos: Es información que el programador manipula en la construcción de una solución o en el desarrollo de un algoritmo.

Firewall: Dispositivo o software que se encarga de monitorear el tráfico a través de una red en la cual es posible crear reglas o permisos para controlar los paquetes o el tráfico que pueden o no permitirse.

Hacker: Persona con avanzados conocimientos en el campo de la informática y en especial de la seguridad que se dedica a descubrir fallos en sistemas.

IA: La Inteligencia Artificial (IA) se refiere a la capacidad de una máquina o sistema informático para realizar tareas que normalmente requerirían inteligencia humana, como

aprendizaje, razonamiento, percepción sensorial, reconocimiento del habla, toma de decisiones y comprensión del lenguaje natural

Información: Conjunto organizado de datos que construyen un mensaje que permiten reducir la duda o incrementar el conocimiento de algún tema.

Ingeniería Social: Conjunto de técnicas de ciber atacantes para engañar a personas y atreves de la manipulación obtener información o que esas personas hagan algo que ellos no desean hacer.

Integridad: Es el término que se le da cuando algo es original, no ha sido alterado ni modificado, cuando es integro y todo en si es original, nadie ha modificado nada de él.

Redes: Conjunto de ordenadores interconectados y que les permite compartir diferentes tipos de recursos.

Riesgos: probabilidad de que una vulnerabilidad haya sido expuesta y se estalle generando así una amenaza, es la probabilidad de que ocurra algo.

Seguridad informática: Protege sistema informático de amenazas puede que sean externas o internas.

VPN: Red virtual privada que permite establecer conexión entre dos redes diferentes de forma segura.

VPS: Es un servidor virtual privado donde un mismo servidor físico es dividido en varios servidores virtuales.

Vulnerabilidad: Toda aquella debilidad presente en un sistema informático que produce un riesgo para la seguridad de la información comprometiendo con esto la integridad

Apéndices

Apéndice A

Estructura del Documento para la Estructura del Resumen Analítica Especializado -RAE

Fecha de Realización:	26/09/2024
Programa:	Especialización de seguridad Informática
Línea de Investigación:	Investigación análisis cualitativo
Título:	Análisis de metodologías para la gestión de la ciberseguridad y la gestión de riesgos relacionados con ingeniería social en empresas del sector privado
Autor(es):	Andrea A. Cortes Angarita
Palabras Claves:	Ciberataques, Seguridad informática, Controles, Ingeniería social.
Descripción:	La digitalización y el aumento de ciberataques han impulsado la necesidad de adoptar mejores prácticas de ciberseguridad, especialmente frente a ataques basados en ingeniería social. Este estudio presenta un análisis profundo de los riesgos asociados con la ingeniería social y la seguridad informática en empresas del sector privado, proponiendo estrategias para mitigar dichos riesgos. A través de una revisión documental y técnica, se identifican vulnerabilidades comunes y se sugieren controles y prácticas que pueden aplicarse en organizaciones para detectar y gestionar brechas de seguridad. El trabajo también enfatiza la importancia de educar a los empleados en ciberseguridad y en la implementación de políticas robustas que permitan minimizar el impacto de ataques cibernéticos.
Fuentes bibliográficas destacadas:	

American Psychological Association. (2020). *Publication manual of the American Psychological Association* (7th ed.). https://doi.org/10.1037/0000165-000

Techopedia. (2024). *Estadísticas de ciberseguridad*. Techopedia. https://www.techopedia.com/es/estadisticas-ciberseguridad

Syneidis. (2018). Descubre qué es la ingeniería social, conoce sus riesgos y …. https://www.syneidis.com/es/social-engineering-risk/

Pirani Risk. (2022). Ingeniería social, ciberataques más comunes y cómo prevenirlos. https://www.piranirisk.com/es/blog/ingenieria-social-ciberataques-y-prevencion

Help Net Security. (2024, septiembre 6). SaaS environments: Human firewall strategies. https://www.helpnetsecurity.com/2024/09/06/saas-environments-human-firewall-strategies/

Semana. (2024, septiembre 13). ¿Qué marcas encabezan el ranking de las más suplantadas por los ciberdelincuentes en 2024? Semana. https://www.semana.com/tecnologia/articulo/que-marcas-encabezan-el-ranking-de-las-mas-suplantadas-por-los-ciberdelincuentes-en-2024/202410/

Toledano, B. (2020, July 23). TikTok, en el punto de mira por la presencia de pederastas en su red social. *ELMUNDO*. https://www.elmundo.es/tecnologia/2020/07/23/5f18329921efa04b168b4620.html

Contenido del documento: La creciente dependencia de tecnologías digitales en el ámbito empresarial ha aumentado los riesgos de ciberataques, en particular aquellos que explotan la falta de conocimiento y desinformación, como la ingeniería social. Este fenómeno representa un reto clave para la seguridad de la información, ya que busca manipular a individuos para obtener acceso no autorizado a datos sensibles. A través de este trabajo, se analiza cómo las empresas del sector privado pueden mitigar estos riesgos, implementando controles y estrategias de gestión de

ciberseguridad que fortalezcan su postura defensiva.

Objetivo General

Analizar las metodologías para la gestión de ciberseguridad y la gestión de riesgos relacionados con la ingeniería social, a partir de una revisión bibliográfica y técnica, para mejorar los niveles de seguridad en las empresas del sector privado de Colombia.

Objetivos Específicos

A. Identificar las vulnerabilidades, amenazas y riesgos asociados con la ingeniería social, analizando diferentes tipos de ataques respaldados por estadísticas, con el fin de determinar los riesgos más comunes que enfrentan las empresas del sector privado.

B. Observar las buenas prácticas de seguridad identificando posibles brechas relacionadas con la ingeniería social, con el objetivo de formular recomendaciones adecuadas para las empresas del sector privado.

C. Seleccionar controles de seguridad recomendados según las mejores prácticas, orientados a reducir los riesgos relacionados con la ingeniería social.

D. Proponer estrategias que contrarresten la ingeniería social, enfocadas en el fortalecimiento de

	las capacidades del talento humano en las empresas del sector privado.
Marco Metodológico:	**Diseño Metodológico** El enfoque metodológico es mixto, combinando fases cuantitativas y cualitativas. El componente cuantitativo se basará en estadísticas y datos concretos obtenidos de estudios sobre ciberataques y vulnerabilidades en el sector privado, mientras que el cualitativo se centrará en el análisis subjetivo de prácticas, políticas y controles de seguridad implementados en dichas organizaciones. **Fases del Estudio** **1.** Fase de Investigación Documental: Revisión de literatura técnica y estudios previos que aborden la ingeniería social y la ciberseguridad en el sector privado. **2.** Fase Cuantitativa: Recopilación y análisis de datos estadísticos sobre los tipos de ataques más frecuentes, incluyendo phishing, vishing y otras variantes de ingeniería social. **3.** Fase Cualitativa: Evaluación de las normativas y políticas vigentes en el sector privado de Colombia, destacando brechas y posibles áreas de mejora. **4.** Fase de Propuestas: Elaboración de recomendaciones y estrategias de control basadas en los resultados obtenidos en las fases anteriores.
Conceptos adquiridos:	Se obtuvieron muchos aprendizajes de este trabajo, entre ellos la importancia de llevar a cabo una correcta gestión de ciberseguridad y los riesgos

asociados con la ingeniería social. Se destacó la relevancia de la concienciación en ciberseguridad, ya que la ingeniería social, uno de los ataques más comunes, se aprovecha del desconocimiento o la falta de preparación de las personas. También se subrayó la importancia de identificar vulnerabilidades comunes, lo que permite saber qué áreas necesitan mayor atención y cuáles son los vectores de ataque más utilizados por los ciberdelincuentes. Además, se reconoció que, aunque las amenazas no se pueden eliminar por completo, es posible mitigarlas de manera significativa mediante la implementación de estrategias preventivas efectivas y buenas prácticas de seguridad. Finalmente, se destacó el rol fundamental de la capacitación continua en todos los niveles, ya que las amenazas evolucionan rápidamente, creando nuevas amenazas cibernéticas.

Conclusiones: Este estudio resalta la importancia de identificar y gestionar los riesgos de ingeniería social en empresas del sector privado mediante la implementación de metodologías de ciberseguridad y controles adecuados. Las organizaciones deben adoptar una postura proactiva, educar a sus empleados y establecer políticas que protejan sus activos digitales. Además, es esencial realizar auditorías regulares y actualizar los sistemas de seguridad conforme evolucionen las amenazas.