INVESTIGAR Y DOCUMENTAR ATAQUES INFORMATICOS MAS COMUNES PRESENTADOS A HERRAMIENTAS DE TRABAJO COLABORATIVO EN EL CONTEXTO ORGANIZACIONAL COLOMBIANO

AUTOR: LUIS HUMBERTO LOPEZ SUAREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2020

INVESTIGAR Y DOCUMENTAR ATAQUES INFORMATICOS MAS COMUNES PRESENTADOS A HERRAMINETAS DE TRABAJO COLABORATIVO EN EL CONTEXTO ORGANIZACIONAL COLOMBIANO

LUIS HUMBERTO LOPEZ SUAREZ

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

ING. MATIN CANCELADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Este proyecto primero que todo está dedicado a DIOS, ya que siempre me ha guiado a lo largo de mi carrera, para realizarme como un excelente profesional, a mis padres que me inculcaron el reto de la superación y a mi familia que siempre estuvieron apoyándome en todo.

AGRADECIMIENTOS

Agradezco a la universidad Nacional Abierta y a Distancia, porque me ofreció la oportunidad de poderme formar en mi carrera como Ingeniero de sistemas y ahora como especialista, ya que por temas laborales nunca hubiera podido hacerlo, pero gracias al método de estudio pude realizar mis estudios, espero dejar el nombre de la universidad muy en alto**.**

CONTENIDO

pág.

LISTA DE TABLAS

pág.

GLOSARIO

Lista de palabras o expresiones organizadas alfabéticamente en mayúscula sostenida, que se encuentran enmarcadas sobre el tema o contenido del trabajo de grado y es un complemento para la comprensión del documento.

Adware: Es un software que habitualmente es patrocinado por publicidad que normalmente puede aparecer en la barra o en las ventanas emergentes, en la mayoría de las ocasiones es utilizado para la recopilación de información.

Botnet: Es un red de equipos informáticos que ha sido secuestrada por un delincuente informático, esto con el fin de robar información, realizar ataques de denegación de servicio (DDoS) , enviar spam, entre otras muchas actividades.

DDOS: (ataque de denegación de servicio). Consiste en dejar un servicio o recurso inaccesible a los usuarios.

Exploit: Es un programa que permite al atacante aprovechar las vulnerabilidades que presente un ordenador.

Gusano informático: Son programas maliciosos que se pasan de equipo en equipo, teniendo como propiedad poderse replicar a todos los demás ordenadores, estos consumen gran parte de la memoria de los equipos y del ancho de banda.

Hoax. Son noticias falsas que son propagadas a través de correo electrónico las cuales se encuentran con contenido engañoso, normalmente se propaga muy rápido debido a sus contenidos de interés.

Suplantación de identidad: Es uno de los más utilizados, consiste en engañar a una persona para que entregue información como usuarios, contraseñas, etc., se

utilizan métodos como el de infringir miedo. También se utilizan método utilizado es el de simular un correo de una figura de autoridad como un jefe, gerente, director, el cual solicita enviar las credenciales y de esta forma el delincuente informático pueda ingresar al sistema informático.

Trojan-DDoS: este programa envía peticiones contra una dirección Web especifica

Phishing: amenaza que se propaga a través de correo electrónico busca poder engañar al usuario para que entregue información sensible como contraseñas, datos bancarios, datos de interés personal, entre otros.

Pretexto: modo de operar de un atacante, los delincuentes informáticos apelan al pesar que se pueda causar en una persona, utilizando el correo para enviar historias trágicas como el fallecimiento de una persona, esto con el fin de buscar que el remitente envié dinero.

Pro Quo: Es un tipo de estafa que se envía a través del correo electrónico con promociones, premios, productos, con el fin que el destinatario diligencia formularios y de esta forma el delincuente pueda obtener la mayor cantidad de datos personales para ser utilizados en robo de identidad.

Puerta trasera: Técnica que permite al atacante realizar modificaciones en el ordenador como modificar, eliminar, entre otras.

Ransomware wannacry: Técnica que se utiliza cifrando la información del usuario para luego solicitar dinero para poder recuperar su información, es usado a través de un correo electrónico adjunto el cual contiene un ejecutable, en el momento que se abre bloquea las carpetas y deja un mensaje con los pasos a seguir si el usuario quiere recuperar su información.

Rootkit: La función principal es la de ocultar programas maliciosos que se puedan estar ejecutando en un ordenador

Troyano: Software malicioso, que se presenta ante el usuario como un programa, archivo adjunto, interesante o útil, algo inofensivo, para que se pueda acceder a él realizando la instalación en el sistema

RESUMEN

En la actualidad las herramientas de trabajo colaborativo son muy utilizadas en el contexto organizacional colombiano ya que integran todas las líneas de comunicación entre los empleados, independientemente del lugar donde se encuentren, permitiendo videoconferencias con intercambio de documentos, almacenar en la nube, edición de textos en línea, entre otras.

El crecimiento continuo de esta clase de herramientas de trabajo colaborativo a hecho que también se aumenten los riesgos, generando como consecuencia que los delincuentes informáticos pongan su mirada sobre esta clase de herramientas, haciendo que estas se vuelvan uno de los mayores focos de vectores de ataques de seguridad.

En el momento existen una gran diversidad de productos de trabajo colaborativo que pueden variar según las necesidades y características de una organización, herramientas como OneDrive, Exchange, Skype, Zoom, Trello, Wrike, SharePoint, Team, Zoho projects, slack, Workplace, entre otras, estas son adquiridas en las organizaciones para su operación, esto hace que sea necesario recopilar información sobre los ataques mas comunes presentados a estas herramientas y de esta forma poder proponer un esquema básico de aseguramiento para el uso de estas herramientas el cual nos ayudara en la reducción de incidentes que puedan afectar los activos de información de una organización.

ABSTRACT

Currently collaborative work tools are widely used in the Colombian organizational context as they integrate all lines of communication between employees, regardless of where they are, allowing videoconferences with document exchange, cloud storage, text editing online, among others.

The continuous growth of this class of collaborative work tools has also increased the risks, generating as a consequence that computer criminals set their sights on this class of tools, making them become one of the main sources of attack vectors. of security.

At the moment there is a great diversity of collaborative work products that may vary according to the needs and characteristics of an organization, tools such as OneDrive, Exchange, Skype, Zoom, Trello, Wrike, SharePoint, Team, Zoho projects, slack, Workplace, among others, these are acquired in organizations for their operation, This makes it necessary to collect information about the most common attacks presented to these tools and in this way to be able to propose a basic assurance scheme for the use of these tools which will help us in reducing incidents that may affect the information assets of an organization

INTRODUCCIÓN

Las herramientas de trabajo colaborativo en la actualidad se están utilizando de una forma acelerada en casi todas las organizaciones Colombianas ya que permiten la interacción con todos los empleados desde cualquier parte donde se encuentren, este crecimiento a hecho que se incremente significativamente los riesgos, generando como consecuencia que los delincuentes informáticos pongan su mirada sobre esta clase de herramientas, haciendo que estas se vuelvan uno de los mayores focos de vectores de ataques de seguridad.

En la mayoría de las situaciones no se tienen claros los esquemas básicos de aseguramiento para el uso de estas herramientas de trabajo colaborativo, este desconocimiento por parte de los usuarios y de las compañías en el contexto general, hace que sea mucho más fácil engañarlos y de esta forma ejecutar un ataque.

El presente trabajo tiene como objetivo, investigar y documentas los ataques informáticos más comunes que se presentan a las herramientas de trabajo colaborativo en el contexto organizacional Colombiano, igualmente se analizara estado actual de la ciberseguridad en las organizaciones, para de esta forma propone un esquema de aseguramiento para el uso de las herramientas más comunes de trabajo colaborativo que permita aportar en la reducción de incidentes que afecten los activos de información de una organización.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Anteriormente las herramientas de trabajo colaborativo no se utilizaban con mucha frecuencia, teniendo en cuenta que la mayoría de las personas trababan al interior de las compañía, por lo cual estas herramientas no se presentaban mayor riesgo, pero en la actualidad este contexto cambio y la demanda de uso de estas herramientas se elevó significativamente, ocasionando que el riesgo se elevara igualmente, como lo revela el programa SAFE, donde en Enero y Junio de 2020, se incrementó en un 364% la suplantación a sitios web, con el fin de obtener información y un 72 % la violación a los datos personales. [1]

En la mayoría de las situaciones no se tienen claros los esquemas básicos de aseguramiento para el uso de estas herramientas de trabajo colaborativo, este desconocimiento por parte de los usuarios hace que sea mucho más fácil engañarlos y de esta forma ejecutar un ataque.

1.2 FORMULACIÓN DEL PROBLEMA

¿Es posible realizar un esquema de aseguramiento para el uso de herramientas mas comunes de trabajo colaborativo que nos permita aportar en la reducción de incidentes que afecten los activos de información de una organización?

---

[1] COMPUTERWORLD. Operaciones seguras en internet, [En línea]. 2019. Disponible en: https://computerworld.co/operaciones-seguras-en-internet/

2. JUSTIFICACIÓN

En este apartado se presenta el pára qué del trabajo planteado, con qué propósito se realiza éste, beneficios.

Los seres humanos son los eslabones más débiles en las cadenas de seguridad de las compañías, es por esta razón que los delincuentes informáticos han aumentado los ataques con técnicas novedosas, efectivas y rápidas, técnicas como el de engañar a una persona para que esta entregue información personal, contraseñas, datos de tarjetas y /o para que abra un correo, un chat, una invitación, el cual puede contener un software malicioso.[2]

En la actualidad las herramientas de trabajo colaborativo son muy utilizadas en el contexto organizacional colombiano por lo cual esto ha hecho que se incremente los riesgos, generando como consecuencia que los delincuentes informáticos pongan su mirada sobre esta clase de herramientas, haciendo que estas se vuelvan uno de los mayores focos de vectores de ataques de seguridad.

El propósito de este estudio es Proponer un esquema básico de aseguramiento para el uso de las herramientas más comunes de trabajo colaborativo que permita aportar en la reducción de incidentes que afecten los activos de información de una organización.

---

[2] CCN-CERT. Ciberamenazas y Tendencias, , [En línea]. 2019. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html

3. OBJETIVOS

OBJETIVOS GENERAL

Investigar los ataques informáticos más comunes presentados a herramientas de trabajo colaborativo en el contexto organizacional colombiano.

OBJETIVOS ESPECÍFICOS

Recopilar información relacionada con las herramientas más comunes de trabajo colaborativo usadas en las organizaciones.

Analizar el estado actual de la ciberseguridad en las organizaciones colombianas

Proponer un esquema básico de aseguramiento para el uso de las herramientas más comunes de trabajo colaborativo que permita aportar en la reducción de incidentes que afecten los activos de información de una organización

2 MARCO REFERENCIAL

Abarca los aspectos que fundamentan la investigación, por ejemplo: marco teórico, marco conceptual, marco legal, entre otros.

2.1 MARCO TEÓRICO

Dentro de este marco se procederá con la documentación de los ataques mas comunes presentados a herramientas de trabajo colaborativo.

4.1.1. Uncunc path injection: este es un ataque de seguridad que afecta herramientas de videoconfencias como Zoom, el cual consiste en robar todas las credenciales de los usuarios de Windows a través de enlaces enviados a los participantes de la conferencia, buscando igualmente que ellos abran este enlace y poder robar las credenciales. [3]

4.1.2 Hoax. Son noticias falsas que son propagadas a través de correo electrónico las cuales se encuentran con contenido engañoso, normalmente se propaga muy rápido debido a sus contenidos de interés, son conocidos igualmente con el nombre de hoaxes o bulos, generalmente buscan que los usuarios entren en un estado de confusión, algunos Hoaxes más extendidos: Evocash dbgmgr.exe, kachus ball.exe, Pandemic Computer Virus, Buddylst.zip y Big Brother. [4]

---

[3] WELIVWSECURITY-ESET. Un repaso por los últimos problemas de seguridad y privacidad que se descubrieron en Zoom. Disponible en: https://www.welivesecurity.com/la-es/2020/04/09/repaso-ultimos-problemas-seguridad-privacidad-descubrieron-zoom/

[4] GDATA. ¿Qué es realmente un Hoax? [En línea]. 2020. Disponible en: https://www.gdata.es/guidebook/what-actually-is-a-hoax

Estos Hoax tratan de engañar a quienes los reciben, intentando que se reenvíen a todos los contactos que se tengan en el correo, existen muchos tácticas para engañar a los usuarios como el de cadenas millonarias que buscan que estas se reenvíen a nuestros contactos, otra táctica es la de causar pesar en la persona que recibe el correo, por ejemplo el estado de salud de una persona, para lo cual se pide reenviarlo en cadena. (Panda Segurity, 2018). [5]

4.1.3 Phishing. Es una amenaza que busca poder engañar al usuario para que entregue información sensible como contraseñas, datos bancarios, datos de interés personal, entre otros, también lo puede hacer dirigiendo al usuario aun sitio web falso, Estos mensajes de phishing aparentemente normalmente provienen de entidades legítimas, pero en realidad no es así, son suplantaciones. [6]

Normalmente pueden llegas a través de un mensaje de chat, correo, invitación informándole que debe actualizar alguna clase de información, por lo cual la persona da clic en link en el enlace y este es redirigido a una url falsa, en ese momento es donde la persona ingresa la información confidencial, la cual queda almacenada en una base de datos del atacante. [7]

---

[5] PANDA SEGURITY. El email, una puerta de entrada de amenazas para tu empresa, [En línea]. 2018. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/ataque-empresas-correo electronico/ 8

[6] MALWAREBYTES. Suplantación de identidad (phishing) [En línea]. 2020. Disponible en: https://es.malwarebytes.com/phishing/

[7] AVAST. Guía esencial del phishing: cómo funciona y cómo defenderse [En línea]. 2020. Disponible en: https://www.avast.com/es-es/c-phishing

4.1.4 Ransomware wannacry. Es un ataque que se utiliza cifrando la información del usuario para luego solicitar dinero para poder recuperar su información, es usado a través a través de un ejecutable contiene un ejecutable, el cual se envía a un usuario, en el momento que se abre bloquea las carpetas y deja un mensaje con los pasos a seguir si el usuario quiere recuperar su información. El ransomware se encuentran creciendo de forma alarmante en el mundo, su auge se da por todos los avances en los desarrollos de las tecnologías.

El ransonware puede afectar cualquier tipo de negocio o actividad comercial, ya que puede afectar desde un usuario conectado a la internet, como a una red de computadoras conectadas a una LAN dentro de una compañía, como multinacionales y/o hospitales, ocasionando la pérdida parcial o total de la información, interrupciones en las funciones, pérdidas económicas, puede incluso llegar a generar perdida de reputación corporativa. [8]

En la mayoría de las situaciones que se han presentado en los ámbitos corporativos cuando un equipo queda encriptado se exige por parte del atacante un rescate por la información que quedo comprometida, lo cual debe ser pago con la moneda bitcoin, esto con el fin de que el atacante siempre este oculto de cualquier transacción que se pueda realizar. [9]

---

[8] KASPERSKY. ¿Qué es el ransomware? [En línea]. 2020. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware

[9] BBC. El virus que secuestra tu computadora y te pide rescate. [En línea]. 2015. Disponible en: https://www.bbc.com/mundo/noticias/2015/12/151215_tecnologia_virus_ransomware_crece_egn

El ransomware busca aprovechar los huecos de seguridad que puedan llegar a presentar los sistemas operativos y las diferentes aplicaciones con el fin de utilizarlas para poder ingresar el malware. Una de las técnicas que utilizan los atacantes, una de ellas es mediante el spam, lo que se hace es buscar que el destinatario abra el correo enviado el cual se puede encontrar con contenidos web maliciosos, ficheros o archivos con ejecutables. [10]

4.1.5 Ataques a sistemas operativos por ausencia de antivirus y/o Detección temprana de vulnerabilidades

La seguridad informática encierra una serie de aspectos a tener en cuenta en una organización, debido a que un sistema informático cuenta con varios servicios, es indispensable adecuar una serie de controles a cada servicio, adicional contar con métodos que permitan establecer la seguridad en el manejo adecuado de la información, esta seguridad debe establecerse debido a que cada servicio cuenta con una serie de vulnerabilidades, que de no corregir a tiempo, pueden ser utilizadas por atacantes para vulnerar el sistema, es indudable que cada día es más el número de ataques que se generan en busca de analizar a sistemas con seguridad frágil. [11]

Los ataques se han ido perfeccionado y buscan cada día ampliar su rango. Existen ataques que se concentran en un sola victima atacando de manera directa, otros buscan lanzar ataques de manera distribuida atacando a varios victimas a la vez.

---

[10] WELIVESECURITY-ESET. Análisis del código fuente de un ransomware, [En línea]. 2020. Disponible en: https://www.welivesecurity.com/la-es/2020/07/29/analisis-codigo-fuente-ransomware-escrito-python/

[11] SECURITIC. Análisis de Vulnerabilidades [En línea]. 2020. Disponible en: https://www.securitic.com.mx/reportaje-especial/1348-analisis-de-vulnerabilidades

Una de las amenazas más frecuentas son los ataques de tipo malware, este tipo de software malicioso actúan de diversas formas y están a la orden del día, por tal razón se debe disponer de una serie de herramientas que permitan auditar el sistema informático de la organización con el fin de establecer cuáles son las vulnerabilidades del sistema, realizar pruebas de intrusión controladas para determinar la reacción del sistema y si corrige esa fallas, cuya finalidad es asegurar el sistema informativo minimizando el riesgo de ataque, en la actividad que se plantea, se abordaran una serie de temáticas relacionadas con seguridad informática, vulnerabilidades, tipos de amenazas, herramientas y dispositivos de protección, políticas de uso, legislación, planes de contingencia para prevenir y afrontar los impactos ocasionados por un ataque. [12]

4.1.6 Pharming. Es un tipo de ataque que explota vulnerabilidades en servidores DNS o en equipos clientes, consiste en redirigir un sitio legal a un sitio falso, en muchas de las ocasiones es difícil diferencias estos sitios. Estos sitios falsos pueden instalar virus y/o troyanos en el computador, pueden igualmente robar información financiera con la finalidad de hacer un robo financiero. [13]

La organización se puede proteger de este tipo de ataques, es necesario que el proveedor de servicio de internet filtre los redireccionamientos falsos. El pharming es una técnica muy similar a la del phishing, siempre aprovecha los principios de navegación, modificando el tráfico legítimo de un sitio, en muchas de las ocasiones es difícil distinguir el sitio web falso. El pharming se puede presentar de 2 maneras:

---

[12] UNIVERSIDAD VIU. Tres tipos de seguridad informática que debes conocer [En línea]. 2018. Disponible en: https://www.universidadviu.com/tres-tipos-seguridad-informatica-debes-conocer/

[13] AVAST. Pharming. [En línea]. 2020. Disponible en: https://www.avast.com/es-es/c-pharming

1. Es en el cual el virus lo redirige a un sitio falso.
2. Cuando es infectado el servidor de DNS. [13]

4.1.7 DDOS: (ataque de denegación de servicio). Consiste en dejar un servicio o recurso inaccesible a los usuarios, sobrecarga los recursos de los sistemas atacados, este ataque satura los puertos, en la mayoría de los casos los atacantes ocultan su identidad por lo cual es difícil encontrar un culpable. [14]

Esta clase de ataques pueden consumir los recursos de máquinas, alterar información, cambiar configuraciones, interrupciones y demás temas de inaccesibilidad. Este ataque es un problema bastante delicado ya que no solo los

clientes se pueden quedar sin servicios, también todos los empleados de la compañía. Este ataque puede ser lanzado desde múltiples equipos distanciados geográficamente. [15]

Tipos de ataques **DDOS**:

- Ping de la muerte: Consiste en el aprovechamiento de un fallo de protocolo con el fin de enviar múltiples pings que superar los 64KB.

- Ataque Smurt: Este tipo de ataque busca falsear las IP'S de origen de servidores broadcast.

---

[14] OSI. OFICINA DE SEGURIDAD DE INTERNAURA. ¿Qué son los ataques DoS y DDoS? [En línea]. 2020. Disponible en: https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos

[15] INCIBE. Medidas de protección frente ataques de denegación de servicio (DoS) [En línea]. 2018. Disponible en: https://www.incibe-cert.es/blog/medidas-proteccion-frente-ataques-denegacion-servicio-dos

- SYN Flood: Este tipo de ataque envía peticiones SYN y no devuelve las ACK, ocasionando que el servidor se quede esperando la respuesta de una manera indefinidad.

- Ataque LAND: Este tipo de ataque consiste en enviar un paquete SYN, el cual se ha modificado.

- Ping Flood: Este ataque consistente en inundar el servidor de peticiones ICMP.

- UDP Flood: Este tipo de ataque consiste en enviar peticiones falsas al servidor UDP modificados con datos falsos. [16]

4.1.8 Troyano. Es un software malicioso, que se presenta ante el usuario como un programa, archivo adjunto, interesante o útil, algo inofensivo, para que se pueda acceder a él realizando la instalación en el sistema, pero lo que hace este software es directa o indirectamente abrir un backdoor o puerta trasera, para que un tercero no autorizado, tome control del sistema, a partir de allí puede realizar una serie de procesos como registro de información que se pulsa a través del teclado, usar el dispositivo como proxy para que todas las peticiones antes de salir de la red se redirijan a el sirviendo de filtro y verificando así el tráfico, o a través del acceso no autorizado puede robar o suplantar identidades para escalar privilegios en el sistema . [17]

---

[16] DRAUTA ¿Qué es un ataque de denegación de servicio? [En línea]. 2017. Disponible en: https://www.drauta.com/que-es-un-ataque-de-denegacion-de-servicio

[17] KASPERSKY ¿Qué es un troyano? [En línea]. 2020. Disponible en: https://latam.kaspersky.com/resource-center/threats/trojans

Los ciberdelincuentes han visto en los troyanos unas de las mejores herramientas para realizar el robo de datos personales, bancarios, dando empuje a la creación de un nuevo malware llamado troyano bancario. [18]

Los troyanos son clasificados según la acción que pueda llegar a realizar en el computador:

- Rootkit: La función principal es la de ocultar programas maliciosos que se puedan estar ejecutando en un ordenador

- Trojan-DDoS: este programa envía peticiones contra una dirección Web especifica

- Trojan-Downloader: Su función es la descarga de programas maliciosos y mantenerlos actualizados.

- Trojan-FakeAV: Esta clase de programa realiza simulaciones a las actividades de los antivirus.

- Trojan-IM: Esta clase de programas roban las credenciales de programas de mensajería.

- Trojan-Ransom: Consiste en modificar los datos del ordenador con el fin de no dejarlos accesibles a los usuarios.

- Trojan-Spy : Esta clase de programas realizan un seguimiento a las actividades que se realizan en un ordenador.

---

[18] PANDASECURITY. KASPERSKY. Metamorfo: el troyano bancario con una letanía de trucos. [En línea]. 2020. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/metamorfo-troyano-bancario/

4.1.9 Spyware: Es un tipo de malware que recopila información sin el consentimiento del usuario, información como:

- Historial de navegación
- Información personal
- Datos bancarios
- Pulsaciones realizadas desde el teclado

El spyware puede llegar adjunto a través de correo electrónico como un adjunto, donde el usuario puede caer en la trampa y abril el adjunto. [19]

2.2 MARCO CONCEPTUAL

Con el fin de Proponer un esquema básico de aseguramiento para el uso de las herramientas más comunes de trabajo colaborativo que permita aportar en la reducción de incidentes es necesario entender los conceptos para la elaboración del mismo y saber que tipos de herramientas colaborativas existen.

2.2.1 Tipos de ataques

Carnada: Muchos de los usuarios son curiosos por lo cual esto es utilizado por los delincuentes informáticos, por ejemplo, alguien puede dejar una USB desatendida en cualquier parte para que una persona la tome y la conecte a su computador para revisar que contiene, al realizar esto ya se introdujo un software malicioso. [20]

---

[19] SOFTWARELAB ¿Qué es spyware? La definición y los 5 ejemplos principales [En línea]. 2020. Disponible en: https://softwarelab.org/es/que-es-spyware/

[20] TICPYMES. Ingeniería social: cómo los ciberdelincuentes hackean tu mente. [En línea]. 2019. Disponible en: https://www.ticpymes.es/formacion/noticias/1113908049404/ingenieria-social-ciberdelincuentes-hackean-mente.1.html

Suplantación de identidad: Es uno de los más utilizados, consiste en engañar a una persona para que entregue información como usuarios, contraseñas, etc., se utilizan métodos como el de infringir miedo. También se utilizan métodos como el de simular un correo de una figura de autoridad como un jefe, gerente, director, el cual solicita enviar las credenciales y de esta forma el delincuente informático pueda ingresar al sistema informático. [21]

Pretexto: el modo de operar de un delincuente informático para este ataque es utilizando el pesar o tristeza que se pueda causar en una persona, utilizando el correo para enviar historias muy trágicas como el fallecimiento de una persona, una enfermedad terminal, entre otras, esto con el fin de buscar que el remitente envié dinero.

Quid Pro Quo: Con este tipo de estafa se envía a través del correo electrónico promociones, premios, productos, con el fin que el destinatario diligencia formularios y de esta forma el delincuente pueda obtener la mayor cantidad de datos personales para ser utilizados en robo de identidad.

Spear phishing: Se base en recopilar información de empleados como paginas a las cuales ingresan frecuentemente, con el fin de saber que gustos tienen como por ejemplo le gusta las compras, está buscando empleo, le gusta la comida, cuando el delincuente ha recopilado esta información procederá con el envió de correos atractivos según los gustos de este, con el fin que el destinatario lo abra y de esta forma descargue software malicioso. [22]

---

[21] GODADDY. ¿Qué es la suplantación de identidad ("phishing")? [En línea]. 2020. Disponible en: https://co.godaddy.com/help/que-es-la-suplantacion-de-identidad-phishing-346

[22] NORTON. Amenazas emergentes. [En línea]. 2020. Disponible en: https://co.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html

2.2.2 Ciclo de vida de un ataque de phishing a través de correo electrónico.

Los correos electrónicos se constituyen como el principal vector de amenaza para la información de las compañías, actualmente todas las empresas se encuentran bajo amenaza a diario. En los siguientes pasos se describe como una persona y/o compañía puede sufrir un ataque por parte de un delincuente informático por correo electrónico.

Paso 1: Las compañías actualmente cuentan con soluciones de seguridad para el bloqueo de correos con contenido malicioso, pero en muchos de los casos estas soluciones no son suficientes para impedir el ingreso de correos no confiables, ya que estos pueden venir de muchas maneras con el fin de engañar a cualquier dispositivo de seguridad que se tenga para el control de correo.

Paso 2: Cuando una de estas amenazas de correos electrónico penetra los dispositivos de seguridad que se tengan en la compañía este llegara llegara a la bandeja de entrada del buzón del destinatario, una vez este correo ingrese lo más posible es que el usuario proceda a abrirlo, teniendo en cuenta todos los engaños el usuario no podrá identificarlo como un correo sospechoso por lo cual se abrirá y este instalara el software malicioso.

Paso 3: Una vez ejecutado el paso 2, el malware tendrá acceso al equipo por lo cual el atacante podrá obtener usuarios, contraseñas, páginas, correos e información del usuario, además que este malware instalado podrá monitorear todas las acciones que ejecute desde el equipo, esto representa un agravante si se tienen en cuenta que este mismo usuario pudo abrir su correo desde un equipo personal. [33]

Paso 4: A través de este malware ingresado por correo electrónico, y una vez obtenido las credenciales el atacante procederá con el acceso a toda la información confidencial, corporativa, administrativa, personal, etc, que se tenga guardada en el computador y posiblemente de toda la red, esta información frecuentemente es

vendida en mercados negros con temas de daños reputacionales, competencias desleales, entre otras.

4.2.3 Recopilar información relacionada con las herramientas más comunes de trabajo colaborativo usadas en las organizaciones.

Office365: Es una herramienta que nos permite crear, acceder compartir documentos de Excel, Word, porwerPoint, Onenote, con una gran ventaja que nos permite poder acceder a ellos en línea y desde cualquier dispositivo y desde donde no encontremos, tienen una seria de herramientas de trabajo colaborativo para trabajar con videoconferencias, almacenamiento, entre otros. [23]

Algunas de las herramientas que trae Office365 para todo el tema de trabajo colaborativo son:

SharePont: sirve para que las compañías creen sus sitios Web, portales, interfaces corporativas, se puede compartir información configurándolo como repositorios con permisos a los usuarios, para ser accedido desde cualquier dispositivo, permite configurar flujos de trabajo, se adapta muy bien y para ser usada en todos los temas de inteligencia empresarial. [24]

Microsoft Teams: es una excelente herramienta para integrar todos los colaboradores de una misma organización, puede configurarse para interactuar

---

[23] NORTON. Amenazas emergentes. [En línea]. 2020. Disponible en: https://www.profesionalreview.com/2018/04/29/que-es-office-365/

[24] NORTON. Amenazas emergentes. [En línea]. 2020. Disponible en:

https://www.profesionalreview.com/2018/04/29/que-es-office-365/

igualmente con cliente, proveedores y demás parte externas que necesiten ser involucradas, Permite realizar reuniones privadas, audio llamadas, compartir información, entre otras. [25]

Yammer: es una red social de comunicación para las compañías, permite ayudar con todos los temas de gestión de proyecto, permite notificar noticias en línea para tener informado a los empleados y a los clientes, permite participar grupos de trabajo, permite la realizar eventos en vivo, se puede configurar para trabajar en las gestiones de resolución de problemas. [26]

Zoho: es un conjunto de softwarede trabajo colaborativo que nos permite interactuar con empleados y clientes para gestionar cualquier tipo de negocio, nos permite realizar flujos de trabajo, proyectar ventas, centralizar todo tipo de información comercial como contactos, tareas, acuerdos, tienen un software de seguimiento de clientes que permite tomar decisiones. [27]

---

[25] SOFTENG. La nueva herramienta de colaboración de Office365. [En línea]. 2020. Disponible en: https://www.softeng.es/es-es/blog/microsoft-teams-la-nueva-herramienta-de-colaboracion-de-office-365.html

[26] CONSULTEK . que es como usar Microsoft yammer. [En línea]. 2020. Disponible en: https://blog.conzultek.com/teletrabajo/que-es-como-usar-microsoft-yammer

[27] NUVA. Aumenta la productividad en ventas a través de la automatización del marketing. [En línea]. 2020. Disponible en: https://www.nuva.co/zoho-crm-colombia/l

Edmodo: Es una plataforma que se puede utilizar en el ámbito corporativo con el fin de realizar cursos para todos los empleados permitiendo realizar la gestión de aulas y de trabajo colaborativos grupales, los empleados podrán acceder de forma externa a los cursos y presentarlos en línea desde donde se encuentren, ya que permite la conexión externa. [28]

WordPress: Es una herramienta que se esta utilizando ahora para publicar documentos directamente, ya que sus nuevas versiones permite realizar ediciones colaborativas simultaneas, lo cual es muy importante para realizar reuniones en línea con documentos que se deban presentar y estos se requiera de realizar ajustes al instante. [29]

Google Hangouts: Es una herramienta de trabajo colaborativo que permite realizar videoconferencias de Google Meet, permite el almacenamiento de archivos en la nube y la utilización de documentos colaborativos, tienen igualmente un sistema de mensajería que permite la integración con todos los integrantes de una compañía, se puede ingresar desde cualquier dispositivo. [30]

---

[28] EDMODO. [En línea]. 2020. Disponible en: https://www.educaciontrespuntocero.com/recursos/edmodo-que-es-clase-educacion/

[29] FAYERWAYER. WordPress ya soporta edición colaborativa mediante Google Docs [En línea]. 2020. Disponible en: https://www.fayerwayer.com/2017/03/wordpress-ya-soporta-edicion-colaborativa-mediante-google-docs/

[30] GSUITE Herramientas de colaboración modernas para optimizar el trabajo en equipo. Disponible en: https://gsuite.google.com/intl/es-419/essentials/?utm_source=google&utm_medium=cpc&utm_campaign=latam-CO-all-es-dr-bkws-all-all-trial-b-latam-1009103-LUAC0010719-GoogleMeet&utm_content=text-ad-none-none-DEV_c-CRE_443002492496-ADGP_Hybrid%20%7C%20AW%20SEM%20%7C%20BKWS%20~%20BMM%20%7C%20Hangouts-KWID_43700055116978654-kwd-37418430954-userloc_1003659&utm_term=KW_%2Bhangout-ST_%2Bhangout&gclid=EAIaIQobChMIl7mej_7S6wIVJ4FaBR25mgcREAAYASAAEgIXwvD_BwE&gclsrc=aw.ds

Marqueed: Es una herramienta de trabajo colaborativo que permite a las persona acceder a un proyecto, visualizar contenidos, imágenes, y textos, permitiendo poder cambiarlos en línea, se utiliza mucho para todos los temas de diseño, permite crear chat para interactuar en el ámbito empresarial, con el fin de realizar cambios en línea. [31]

Voxopop: Es una herramienta que sirve para interactuar con muchas personas, permite realizar grabaciones de voz, algo que la hace exclusiva es que solo utiliza voz en lugar de texto, es una excelente herramienta de proyectos colaborativo y proyecto de presentación oral, ya que permite interactuar desde cualquier sitio y desde cualquier dispositivo. [32]

Dropbox: Es una herramienta de almacenamiento grupal, que permite interactuar de una forma inteligente ya que reúne equipos herramientas y contenidos, se puede compartir hojas de cálculo en línea, presentaciones de Google, archivos de Microsoft office, puede interactuar con otras herramientas de trabajo colaborativo. [33]

---

[31] NORTON. Amenazas emergentes. [En línea]. 2020. Disponible en: https://wwwhatsnew.com/2013/08/09/marqueed-la-solucion-web-perfecta-para-discutir-disenos-entre-varias-personas/

[32] VOXOPOP. [En línea]. 2020. Disponible en: https://gisell89.wordpress.com/voxopop/#:~:text=Voxopop%20es%20una%20es%20una,voz%20en%20lugar%20de%20texto.

[33] DROPBOX. [En línea]. 2020. Disponible en: https://www.dropbox.com/business/landing-t68fl?_tk=paid_sem_goog_biz_b&_camp=1019580883&_kw=dropbox|e&_ad=401450399913||c&gclid=EAIaIQobChMIr-qvybvT6wIVB2-GCh2RVAx5EAAYASAAEgIVbPD_BwE

Google Drive: Esta herramienta colaborativa permite almacenar, crear, modificar, compartir y ingresar a documentos en línea de forma centralizada sincronizándolos desde cualquier dispositivo, permite mantener actualizados todos los archivos automáticamente, permite compartir archivos con otras personas para que se puedan modificar en cualquier tipo de reunión. [34]

Jumpshare: Es una herramienta que permite compartir en línea cualquier trabajo a través de enlaces, se puede compartir archivos con todos los usuarios de una compañía con el previo permiso dado por el dueño del documento, permite realizar videos que luego se podrán compartir. Se puede igualmente tomar capturas de pantalla. [35]

Hightrack: es una apalicacion colaborativa que permite combinar gestores de tareas como eventos en línea, permitiendo que estos se puedan consultar en línea en cualquier momento y desde cualquier sitio, consiguiendo que estemos actualizados con todas las actividades y estar enterados de las disponibilidad del tiempo con el que podemos contar. [36]

---

[34] SITES GOOGLE. ¿Qué es Google Drive? [En línea]. 2020. Disponible en: https://sites.google.com/a/upaep.mx/gapps_nuevo/inicio/googledocs/google-drive/que-es-google-drive

[35] JUMPSHAR. Comparta su trabajo en segundos. Visualmente. [En línea]. 2020. Disponible en: https://jumpshare.com/

[36] GENBETA. La nueva aplicación pensada para hacer que ser productivo sea sencillo. [En línea]. 2020. Disponible en: https://www.genbeta.com/web/hightrack-la-nueva-aplicacion-pensada-para-hacer-que-ser-productivo-sea-sencillo

MARCO HISTÓRICO

Los ataques informáticos a las organizaciones en los últimos 10 años se han incrementado significativamente, han pasado de ser un simple malware a un ataque cibernético sofisticado, con el agravante que se han vuelto repetitivos de forma diaria, en un principio solo se escuchaba de forma aislada algunos ataques pero en este momento se están ejecutan muchos y diversos ataques a las organizaciones, a continuación se describen algunos de los ataques más importantes que han ejecutado a lo largo de la historia.

- Wikileaks: se presentó en Noviembre 2010: Se revelaron más de 250.000 telegramas diplomáticos

- Sony PlayStation Network: se presentó en Abril 2011, quedaron expuestos los datos personales de más 77 millones de personas, el servicio dejo de funcionar durante una semana.

- Dropbox: Sucedió en Agosto 2012, fueron expuestos los correos electrónicos de sus usuarios junto con las contraseñas de ingreso, más de 68 millones de usuarios quedaron afectados.

- Target: sucedió en Diciembre 2013, quedaron expuestos más de 70 millones de clientes a los cuales les robaron información personal y a unos 40 millones les
- fueron robados los datos bancarios.

- eBay: sucedió en Mayo 2014, fueron robados los datos personales de más de 140 millones de usuarios.

- Comité Republicano: sucedió en Diciembre de 2015, fueron expuestos los datos de más de 190 millones de votantes debido a un error de una empresa que habían contrato para estas elecciones.

- Friend Finder: sucedió en Noviembre 2016, fueron robadas más de 400 millones de cuentas de temas de pornografía, además que fue expuesto en el mercado negro los datos personales asociados a este sitio.

- Uber: sucedió en Noviembre 2017, Fueron robados los datos personales de mas de 50 millones de usuarios.

- Cambridge Analytica: sucedió en Marzo 2018, fueron robados datos personales para ser usados en temas de política, utilizo sin consentimiento la información de más de 50 millones de personas.

- Facebook: sucedió en Marzo 2019, quedaron expuestos los datos de teléfono y de identificación de los usuarios de Facebook.

2.3 ANTECDENTES O ESTADO ACTUAL

Un estudio realizado por la firma Sophos, informa que el 76 % de las empresas en Colombia han sufrido un ataque o incidente de seguridad relacionado con la información corporativa, al trabajar con temas de nube públicas. El panorama actual está cambiando la forma todas las formas de trabajar, debido a que se ha descentralizado muchos temas que se hacían al interior de las compañías y en este momento se hacen desde distintos puntos externos.

Un estudio llamado “El estado de la seguridad en la NUBE 2020” informa que en Colombia el 100% de las organizaciones que consultaron, informaron estar preocupados por los temas de seguridad. En este estudio se informa

El estudio realizado por Sophos indica que la tendencia de Ciberseguridad a nivel general en Colombia, está relacionado con malware con un 35% de casos, exposición de datos un 33%, robo de credenciales un 20%, y minería de criptomonedas con un 18%. [37]

Los delincuentes informáticos están cambiando todos métodos con el fin de reapuntarlos a entornos en la nube, con el fin de paralizar la infraestructura necesaria y los cuales puede incrementar la forma de pago de la información que ha sido robada.

---

[37] DINERO.COM. Incidentes de las organizaciones en Colombia Amenazas emergentes. [En línea]. 2020. Disponible en: https://www.dinero.com/tecnologia/articulo/sophos-76-de-organizaciones-en-colombia-reportaron-incidentes-en-la-nube/292849

Las preocupaciones generales en Colombia sobres los temas de seguridad son muy preocupantes por las compañías y en general por todas las personas ya que informan no sentirse seguros con todos los temas de seguridad financiera, porque sienten que en cualquier momento puede ser víctimas de un fraude bancario por intermedio de sus tarjetas.

En Colombia se ha avanzado en materia de Ciberseguririrdad y en el fortalecimiento de las instituciones, pero debido a los impactos que puede tener un incidente cibernético y todo lo que puede acarrear como perdida de información, daños de reputación, pérdidas financieras, entre otras, es necesario que se siga trabajando en el fortalecimiento en materia de riesgos en todas las compañías Colombianas

El sector de la banca es uno de los mayores sectores que invierte en todo el tema de la protección de datos personales y en todos sus sistemas de información corporativa, actualmente han incorporado temas de prácticas de ciberseguridad y de seguridad de la información, pero es muy necesario que se sigan fortaleciendo con el fin de poder anticiparse a cualquier ciberamezana.

En la actualidad la superintendencia financiera dio instrucciones para todo el tema que tienen que ver con los riesgos cibernéticos, donde se destacan temas relevantes y de mucha importancia como la inclusión de los temas de riesgos a los temas de ciberseguridad, los cuales se busca dar instrucciones claras relacionadas con todos estos temas. [38]

---

[38] ASOBANCARIA. La gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones. [En línea]. 2018. Disponible en: https://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf

Las organizaciones colombianas están adquiriendo muchas tecnologías de información, esto ha hecho que genere muchos más ingresos económicos, pero esto también con lleva a que se presenten una mayor cantidad de riesgos los cuales se encuentran asociados con temas de confidencialidad y protección de datos personales.

Es necesario que las organizaciones le den mucha más importancia al asunto de la ciberseguridad, ya que diariamente los ataques son mucho más sofisticados y diversificados, es necesario que estas compañías inviertan en recursos tanto físicos como materiales son el fin de prevenir cualquier tipo de amenaza que pueda desencadenas en un incidente mayor.

2.4 MARCO LEGAL

En el momento se vive una rápida evolución en los avances tecnológicos, lo cual ha hecho que las compañías inviertan en temas de seguridad con el fin de minimizar los riesgos de daños y/o perdidas de información, sin embargo, la parte humana sigue siendo uno de los eslabones débiles, ya que está expuesta a la manipulación psicológica por parte de los delincuentes informáticos con el fin de obtener un beneficio.

Es necesario que se apliquen normas que ayuden a nivel general a proteger la información de las personas y de las compañías, en Colombia es considerado un delito informático cuando una persona o un delincuente informático se apodera ilegalmente de información confidencial que se encuentra en un dispositivo como un computador, celular, entre otros. En nuestro país existen leyes que regulan los delitos informáticos. [39]

---

[39] ABOGADOS Y CONTADORES. Acciones que son consideradas un delito informático en [En línea]. 2020. Disponible en: https://tusabogadosycontadores.co/blog/acciones-que-son-consideradas-un-delito-informatico-en-colombia/

A continuación, se mencionarán:

2.4.1 Ley 1273 de 2009. Protección de la información y de los datos:

La ley 1273 de 2009, se tipificaron varias conductas, como el acceso abusivo a un sistema informático, este tendrá una pena de prisión hasta de 96 meses y multa de hasta 1000 salarios mínimos legales vigentes. Esta ley es muy importante para todo el tema de los delitos informáticos en Colombia, por lo cual es prioritario su aplicación en todas las empresas, ya que esto nos permitiría crear mecanismos para la protección de la información.

Esta ley incluye artículos como la interceptación de datos informáticos, obstaculización ilegitima de sistema informático o red de telecomunicación, interceptación de datos informáticos, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales, hurto por medios informáticos y semejantes, transferencia no consentida de activos, entre otros. [40]

2.4.2 Ley 1581 – ley de protección de datos personales

En esta ley se relacionan las disposiciones para la protección de datos personales, y en el cual se resumen los siguientes artículos a los cuales hace referencia el proyecto:

Artículo 4: Tratamiento de datos personales, se aplica a los siguientes principios:

a) Principio de legalidad de Tratamiento de datos: Hace referencia a una actividad reglada que está sujeta a lo establecido en ella y las disposiciones que la desarrollen.

---

[40] SECRETARIA SENADO. Ley 1273 de 2009. [En línea]. 2020. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

b) Principio de finalidad: Está sujeta una finalidad legitima según la constitución y esta debe ser informada al titular.
c) Principio de finalidad: Está sujeta una finalidad legitima según la constitución y esta debe ser informada al titular.
d) Principio de libertad: El tratamiento solo debe contar con la autorización expresa del titular, no se podrán divulgar los datos sin autorización.
e) Principio de veracidad o calidad: La información debe ser veraz, está prohibido los datos parciales que puedan llegar a inducir a un error.
f) Principio de transparencia: El titular puede solicitar al encargado de tratamiento, la información de todos los datos de este titular.
g) Principio de acceso y circulación restringida: El tratamiento solo se puede realizar por personas que se encuentren autorizadas por el titular.
h) Principio de seguridad: La información para el tratamiento deberá contar con seguridad para evitar perdida, consultas no autorizadas, fraudes, entre otros.
i) Principio de confidencialidad: se debe garantizar la confidencialidad de la información por todas las personas que tengan que ver con el tratamiento de los datos. [41]

[41] MINISTERIO DE COMERCIO, INDUCTRIA Y TURISMO. Ley de protección de datos personales. [En línea]. 2013. Disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

3 DISEÑO METODOLÓGICO

La metodología utilizada en el presente trabajo monográfico es la de recolección de información, esta se realizara sobre los ataques informáticos más comunes presentados a herramientas de trabajo colaborativo en el contexto organizacional colombiano, se realizara un análisis del estado actual de la ciberseguridad en las organizaciones, a fin de entregar un esquema básico de aseguramiento para el uso de las herramientas más comunes de trabajo colaborativo con el fin que esta nos permita aportar en la reducción de los incidentes que afecten la información de una organización.

3.1 FUENTES Y TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

La recolección de información será dada a través de la observación, análisis de documentos, tesis, artículos, libros e informes asociados con ataques informáticos más comunes presentados a herramientas de trabajo colaborativo en el contexto organizacional colombiano.

4 DESARROLLO DE LOS OBJETIVOS

4.1 DESARROLLO DE OBJETIVO 1:

Recopilar información relacionada con las herramientas más comunes de trabajo colaborativo usadas en las organizaciones.

Este objetivo fue desarrollado en el numeral 4.2.3 Recopilar información relacionada con las herramientas más comunes de trabajo colaborativo usadas en las organizaciones.

4.2 DESARROLLO DE OBJETVO 2

Analizar el estado actual de la ciberseguridad en las organizaciones Colombianas

Este objetivo fue desarrollado en el punto 4.4. Antecedes o estado actual.

4.3 DESARROLLO DE OBJETVO 2

Proponer un esquema básico de aseguramiento para el uso de las herramientas más comunes de trabajo colaborativo que permita aportar en la reducción de incidentes que afecten la información de una organización.

Este esquema básico de aseguramiento se realizó en el punto 7.

7. Esquema básico de aseguramiento para el uso de las herramientas más comunes de trabajo colaborativo que permita aportar en la reducción de incidentes que afecten la información de una organización.

Tabla 1. Esquema básico de aseguramiento

Esquema de aseguramiento para el uso de las herramientas más comunes de trabajo colaborativo.	
Herramienta de trabajo colaborativo	**Aseguramiento**
SharePont:	- No conectar ningún dispositivo a redes inseguras cuando se esté trabajando con SharePont - Verificar con quien se comparte los enlaces para compartir información. - Activar en doble factor de autenticación, con el fin de prevenir un incidente si una cuenta y contraseña se ve comprometida. - Activar mensaje de texto para que se solicite siempre que se vaya a ingresar a la cuenta de SharePoint

	- Verificar los archivos que se suben a Sharepoint, porque en caso de que se suba un archivo - infectado con malware puede afectar a los demás archivos alojados allí.
Teams	- Verificar los correos con agendas para realizar conferencias por Teams, es necesario asegurar que proviene de una fuente segura. - Activar doble factor de autenticación. - No abrir ningún correo electrónico con invitaciones de Teams desconocidas, donde traigan enlaces sospechosos. - Verificar los archivos que se suben a través de teams a Onedrive, si hay alguno que se presuma como sospechoso no se deberá subir.
Yammer	- Siempre se debe tener activado la seguridad de contenido la cual se encuentra en la configuración de la herramienta.

	- En lo posible se debe tener deshabilitada la opción de compartir con redes externas, hasta que no se comprueba la legitima de la red. - No compartir información de carácter personal para los temas de publicaciones.
Edmodo	- Implementar una correcta entrega del código de acceso para ingresar a la plataforma, con el fin de no enviarlo a las personas equivocadas. - En lo posible enviar todos los documentos bloqueados con contraseña. - Tener siempre el navegador actualizado cuando se ingrese a esta plataforma.
Google Hangouts:	- Las reuniones que se hagan a través de esta plataforma no deben ser de temas confidenciales, ya que la plataforma no tiene cifrado lo cual la hace vulnerable a los ataques.

	- Al descargar esta aplicación se deberá hacer únicamente desde un sitio oficial seguro, esto ya que la plataforma en varias ocasiones ha sido suplantada.
Hightrack	- Solo compartir los eventos de forma interna con los empleados de la misma compañía, es mejor no compartir con clientes o externos la consulta de esta opción. - El dispositivo desde donde se trabaje deberá tener actualizado el navegador.
Dropbox:	- Siempre se deberá usar una contraseña muy segura que contenga mayúsculas, minúsculas, números, caracteres especiales, y que la longitud sea mínima de 10 caracteres. - Activar la opción de confirmación de ingreso a través de código de seguridad enviado al celular. - Activar el modo de alerta con mensajes al correo electrónico con el fin de saber cuándo se presente algún acceso no autorizado.

Google Drive	- No abrir Google Drive desde equipos y/o celulares compartidos, ya que la información puede quedar legible. - Siempre se deberá usar una contraseña muy segura que contenga mayúsculas, minúsculas, números, caracteres especiales, y que la longitud sea mínima de 10 caracteres. - En lo posible todos los documentos debe estar con contraseña
Jumpshare	- No abrir Jumpshare desde equipos y/o celulares no seguros, esto debido a que la información puede quedar legible. - Usar una contraseña muy segura que contenga mayúsculas, minúsculas, números, caracteres especiales, y que la longitud sea mínima de 10 caracteres. - Los documentos deben estar con contraseña sin importar el tipo.

Fuente: Luis Humberto Lopez Suarez

8. CONCLUSIONES

Los ataques informáticos han aumentado a medida que va avanzado el tiempo, Vemos que antes se presentaban ataques pequeños aislados, pero en este momento hay muchas modalidades de ataques y técnicas sofisticadas hacia las organizaciones, las cuales pueden dejar como resultado perdidas muy grandes que se pueden ver reflejadas en la quiebra total de una organización.

Actualmente las herramientas de trabajo colaborativo son muy utilizadas en el contexto organizacional colombiano ya que integran todas las líneas de comunicación entre los empleados, esto ha hecho que se incremente los riesgos, por esta razón es tan importante tomar medidas preventivas al momento de utilizarlas.

Independientemente de la organización para la que se trabaje y/o el sector, se debe concientizar a los usuarios sobre el manejo de las herramientas colaborativas, ya que son los eslabones más débiles, además del establecimiento de un esquema básico para el uso de estas herramientas colaborativas, esto nos ayudara a prevenir incidentes que puedan afectar la información de una organización.

.

9. RECOMENDACIONES

Consultar las fuentes: Por ningún motivo se deberá abrir correos que no correspondan a fuentes de confianza, si es en un correo personal del cual no se tienen conocimiento de su procedencia, es necesario contactar a la persona que lo envió, con el fin de verificar su autenticación, en caso de que no se pueda contactar al remitente es mejor no abrirlo hasta que no se haya comprobado su origen.

No entregar ningún dato personal: Cuando estén solicitando información de carácter personal y/o empresarial, como nombres, numero de cedula, empresa en la que labora, nit, cargo, numero de contacto, departamento en el que trabaja, dirección de residencia, dirección de la empresa, usuarios, contraseñas, números de tarjetas, entre otras.

Verificar cualquier enlace interno y/o externo: En caso de que ingrese algún link, enlace, mensaje, y/o Invitación de una fuerte no conocida, a través de alguna de las herramientas colaborativas se debe desconfiar e inmediatamente verificar su procedencia, por ninguna razón abrir este enlace, ya que puede caer en un ataque de ingeniera social.

Capacitar a los usuarios: Es necesario que cuando se adquiera una herramienta de trabajo colaborativo se capacita a los usuarios sobre el manejo tanto interno como externo y se informe de todos los riesgos que con lleva trabajar información de la organización tanto escrita como hablada, esto nos ayudara a prevenir incidentes que puedan afectar organización.

10. BIBLIOGRAFÍA

ABOGADOS Y CONTADORES. Acciones que son consideradas un delito informático en [En línea]. 2020. Disponible en: https://tusabogadosycontadores.co/blog/acciones-que-son-consideradas-un-delito-informatico-en-colombia/

ASOBANCARIA. La gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones. [En línea]. 2018. Disponible en: https://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf

AVAST. Guía esencial del phishing: cómo funciona y cómo defenderse [En línea]. 2020. Disponible en: https://www.avast.com/es-es/c-phishing

AVAST. Pharming. [En línea]. 2020. Disponible en: https://www.avast.com/es-es/c-pharming

AVG ¿Qué es el adware y cómo deshacerse de él? [En línea]. 2020. Disponible en: https://www.avg.com/es/signal/what-is-adware

BARRACUDA. Tendencias de seguridad de correo electrónico 2018. [En línea]. 2018. Disponible en: https://www.barracuda.com/campaign/emailsecurityreport

BARRACUDA. Email Security trends. 2018. [En línea]. 2018. Disponible en: https://assets.barracuda.com/assets/docs/dms/Email_Security_Trends_2018_Report.pdf

CCN-CERT. Ciberamenazas y Tendencias. [En línea]. 2019. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html

CONSULTEK . que es como usar Microsoft yammer. [En línea]. 2020. Disponible en: https://blog.conzultek.com/teletrabajo/que-es-como-usar-microsoft-yammer

DROPBOX. [En línea]. 2020. Disponible en: https://www.dropbox.com/business/landing-t68fl?_tk=paid_sem_goog_biz_b&_camp=1019580883&_kw=dropbox|e&_ad=401450399913||c&gclid=EAIaIQobChMIr-qvybvT6wIVB2-GCh2RVAx5EAAYASAAEgIVbPD_BwE

DIGICERT ¿En qué consisten el malware, los virus, el spyware y las cookies? [En línea]. 2020. Disponible en: https://www.websecurity.digicert.com/es/es/security-topics/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them

DINERO.COM. Incidentes de las organizaciones en Colombia Amenazas emergentes. [En línea]. 2020. Disponible en: https://www.dinero.com/tecnologia/articulo/sophos-76-de-organizaciones-en-colombia-reportaron-incidentes-en-la-nube/292849

DRAUTA ¿Qué es un ataque de denegación de servicio? [En línea]. 2017. Disponible en: https://www.drauta.com/que-es-un-ataque-de-denegacion-de-servicio

EDMODO. [En línea]. 2020. Disponible en: https://www.educaciontrespuntocero.com/recursos/edmodo-que-es-clase-educacion/

FAYERWAYER. WordPress ya soporta edición colaborativa mediante Google Docs [En línea]. 2020. Disponible en: https://www.fayerwayer.com/2017/03/wordpress-ya-soporta-edicion-colaborativa-mediante-google-docs/

GDATA. ¿Qué es realmente un Hoax? [En línea]. 2020. Disponible en: https://www.gdata.es/guidebook/what-actually-is-a-hoax

GENBETA. La nueva aplicación pensada para hacer que ser productivo sea sencillo. [En línea]. 2020. Disponible en: https://www.genbeta.com/web/hightrack-la-nueva-aplicacion-pensada-para-hacer-que-ser-productivo-sea-sencillo

GSUITE Herramientas de colaboración modernas para optimizar el trabajo en equipo. Disponible en: https://gsuite.google.com/intl/es-419/essentials/?utm_source=google&utm_medium=cpc&utm_campaign=latam-CO-all-es-dr-bkws-all-all-trial-b-latam-1009103-LUAC0010719-GoogleMeet&utm_content=text-ad-none-none-DEV_c-CRE_443002492496-ADGP_Hybrid%20%7C%20AW%20SEM%20%7C%20BKWS%20~%20BMM%20%7C%20Hangouts-KWID_43700055116978654-kwd-37418430954-userloc_1003659&utm_term=KW_%2Bhangout-ST_%2Bhangout&gclid=EAIaIQobChMIl7mej_7S6wIVJ4FaBR25mgcREAAYASAAEgIXwvD_BwE&gclsrc=aw.ds

GODADDY. ¿Qué es la suplantación de identidad ("phishing")? [En línea]. 2020. Disponible en: https://co.godaddy.com/help/que-es-la-suplantacion-de-identidad-phishing-346

INCIBE. Ayuda ransomware [En línea]. 2020. Disponible en: https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware.

INCIBE. Medidas de protección frente ataques de denegación de servicio (DoS) [En línea]. 2018. Disponible en: https://www.incibe-cert.es/blog/medidas-proteccion-frente-ataques-denegacion-servicio-dos

IONOS. Spear phishing: ciberataques personalizados. [En línea]. 2020. Disponible en: https://www.ionos.es/digitalguide/correo-electronico/seguridad-correo-electronico/spear-phishing/

JUMPSHAR. Comparta su trabajo en segundos. Visualmente. [En línea]. 2020. Disponible en: https://jumpshare.com/

KASPERSKY ¿Qué es un troyano? [En línea]. 2020. Disponible en: https://latam.kaspersky.com/resource-center/threats/trojans

KASPERSKY ¿Qué es un botnet? [En línea]. 2020. Disponible en: https://www.kaspersky.es/blog/que-es-un-botnet/755/

MAILFENCE. 11 consejos para evitar los ataques de ingenieria social. [En línea]. 2018. Disponible en: https://blog.mailfence.com/es/11-consejos-para-evitar-los-ataques-de-ingenieria-social/

MALWAREBYTES. Suplantación de identidad (phishing) [En línea]. 2020. Disponible en: https://es.malwarebytes.com/phishing/

MICROSOFT. El ciclo de vida de un ataque al correo electrónico. [En línea]. 2016. Disponible en: https://blogs.windows.com/latam/2016/12/19/el-ciclo-de-vida-de-un-ataque-al-correo-electronico/

MINISTERIO DE COMERCIO, INDUCTRIA Y TURISMO. Ley de protección de datos personales. [En línea]. 2013. Disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

NORTON. Amenazas emergentes. [En línea]. 2020. Disponible en: https://co.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html

NORTON. Amenazas emergentes. [En línea]. 2020. Disponible en: https://wwwhatsnew.com/2013/08/09/marqueed-la-solucion-web-perfecta-para-discutir-disenos-entre-varias-personas/

NORTON. Amenazas emergentes. [En línea]. 2020. Disponible en: https://www.profesionalreview.com/2018/04/29/que-es-office-365/

NUVA. Aumenta la productividad en ventas a través de la automatización del marketing. [En línea]. 2020. Disponible en: https://www.nuva.co/zoho-crm-colombia/l

OSI. OFICINA DE SEGURIDAD DE INTERNAURA. ¿Qué son los ataques DoS y DDoS? [En línea]. 2020. Disponible en:

https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos

PANDA SEGURITY. El email, una puerta de entrada. [En línea]. 2018. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/ataqueempresascorreo-lectronico/

PANDASECURITY. KASPERSKY. Metamorfo: el troyano bancario con una letanía de trucos. [En línea]. 2020. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/metamorfo-troyano-bancario/

SECRETARIA SENADO. Ley 1273 de 2009. [En línea]. 2020. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

SECURITIC. Análisis de Vulnerabilidades [En línea]. 2020. Disponible en: https://www.securitic.com.mx/reportaje-especial/1348-analisis-de-vulnerabilidades

SITES GOOGLE. ¿Qué es Google Drive? [En línea]. 2020. Disponible en: https://sites.google.com/a/upaep.mx/gapps_nuevo/inicio/googledocs/google-drive/que-es-google-drive

SOFTENG. La nueva herramienta de colaboración de Office365. [En línea]. 2020. Disponible en: https://www.softeng.es/es-es/blog/microsoft-teams-la-nueva-herramienta-de-colaboracion-de-office-365.html

SOFTWARELAB ¿Qué es spyware? La definición y los 5 ejemplos principales [En línea]. 2020. Disponible en: https://softwarelab.org/es/que-es-spyware/

TICPYMES. Ingeniería social: cómo los ciberdelincuentes hackean tu mente. [En línea]. 2019. Disponible en: https://www.ticpymes.es/formacion/noticias/1113908049404/ingenieria-social-ciberdelincuentes-hackean-mente.1.html

VOXOPOP. [En línea]. 2020. Disponible en: https://gisell89.wordpress.com/voxopop/#:~:text=Voxopop%20es%20una%20es%20una,voz%20en%20lugar%20de%20texto.

UNIVERSIDAD VIU. Tres tipos de seguridad informática que debes conocer [En línea]. 2018. Disponible en: https://www.universidadviu.com/tres-tipos-seguridad-informatica-debes-conocer/

RESUMEN ANALITICO ESPECIALIZADO - R. A. E.

1. Información General

Tipo de documento: Tesis de Especialización	
Acceso al documento:	Universidad Nacional Abierta (UNAD)
Título del documento:	Investigar y documentar ataques informáticos más comunes presentados a herramientas de trabajo colaborativo en el contexto organizacional colombiano
Autor:	Luis Humberto Lopez Suarez
Director:	Ing. Martin Camilo Cancelado Ruiz
Palabras claves.	Adware, botnet,DDOS, exploit gusano informatico, hoax, suplantación de identidad, trojan, phishing, pretecto, Pro Quo, Puerta trasera, Ransonware, rootkit, troyano.
Año.	2021
Resumen:	En la actualidad las herramientas de trabajo colaborativo son muy utilizadas en el contexto organizacional colombiano ya que integran todas las líneas de comunicación entre los empleados, independientemente del lugar donde se encuentren, permitiendo videoconferencias con intercambio de documentos, almacenar en la nube, edición de textos en línea, entre otras. El crecimiento continuo de esta clase de herramientas de trabajo colaborativo a hecho que también se aumenten los riesgos, generando como consecuencia que los delincuentes informáticos pongan su mirada sobre esta clase de herramientas, haciendo que estas se vuelvan uno de los mayores focos de vectores de ataques de seguridad. En el momento existen una gran diversidad de productos de trabajo colaborativo que pueden variar según las necesidades y características de una organización, herramientas como OneDrive, Exchange, Skype, Zoom, Trello, Wrike, SharePoint, Team, Zoho projects, slack, Workplace, entre otras, estas son adquiridas en las organizaciones para su operación, esto hace que sea necesario recopilar información sobre los ataques mas comunes presentados a estas herramientas y

	de esta forma poder proponer un esquema básico de aseguramiento para el uso de estas herramientas el cual nos ayudara en la reducción de incidentes que puedan afectar los activos de información de una organización.
Fuentes Bibliográficas.	ABOGADOS Y CONTADORES. Acciones que son consideradas un delito informático en [En línea]. 2020. Disponible en: https://tusabogadosycontadores.co/blog/acciones-que-son-consideradas-un-delito informatico-en-colombia/ ASOBANCARIA. La gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones. [En línea]. 2018. Disponible en: https://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf AVAST. Guía esencial del phishing: cómo funciona y cómo defenderse [En línea]. 2020. Disponible en: https://www.avast.com/es-es/c-phishing AVAST. Pharming. [En línea]. 2020. Disponible en: https://www.avast.com/es-es/c pharming AVG ¿Qué es el adware y cómo deshacerse de él? [En línea]. 2020. Disponible en: https://www.avg.com/es/signal/what-is-adware BARRACUDA. Tendencias de seguridad de correo electrónico 2018. [En línea]. 2018. Disponible en: https://www.barracuda.com/campaign/emailsecurityreport BARRACUDA. Email Security trends. 2018. [En línea]. 2018. Disponible en: https://assets.barracuda.com/assets/docs/dms/Email_Security_Trends_2018_Rep ort.pdf CCN-CERT. Ciberamenazas y Tendencias. [En línea]. 2019. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia 13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html CONSULTEK . que es como usar Microsoft yammer. [En línea]. 2020. Disponible en: https://blog.conzultek.com/teletrabajo/que-es-como-usar-microsoft-yammer DROPBOX. [En línea]. 2020. Disponible en: https://www.dropbox.com/business/landing t68fl?_tk=paid_sem_goog_biz_b&_camp=1019580883&_kw=dropbox|e&_ad=401450399913||c&gclid=EAIaIQobChMIr-qvybvT6wIVB2-GCh2RVAx5EAAYASAAEgIVbPD_ BwE DIGICERT ¿En qué consisten el malware, los virus, el spyware y las cookies? [En línea]. 2020. Disponible en: https://www.websecurity.digicert.com/es/es/security topics/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates them DINERO.COM. Incidentes de las organizaciones en Colombia

	Amenazas emergentes. [En línea]. 2020. Disponible en: https://www.dinero.com/tecnologia/articulo/sophos-76-de-organizaciones-en colombia-reportaron-incidentes-en-la-nube/292849 DRAUTA ¿Qué es un ataque de denegación de servicio? [En línea]. 2017. Disponible en: https://www.drauta.com/que-es-un-ataque-de-denegacion-de servicio SECRETARIA SENADO. Ley 1273 de 2009. [En línea]. 2020. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html SECURITIC. Análisis de Vulnerabilidades [En línea]. 2020. Disponible en: https://www.securitic.com.mx/reportaje-especial/1348-analisis-de-vulnerabilidades SITES GOOGLE. ¿Qué es Google Drive? [En línea]. 2020. Disponible en: https://sites.google.com/a/upaep.mx/gapps_nuevo/inicio/googledocs/google drive/que-es-google-drive SOFTENG. La nueva herramienta de colaboración de Office365. [En línea]. 2020. Disponible en: https://www.softeng.es/es-es/blog/microsoft-teams-la-nueva herramienta-de-colaboracion-de-office-365.html SOFTWARELAB ¿Qué es spyware? La definición y los 5 ejemplos principales [En línea]. 2020. Disponible en: https://softwarelab.org/es/que-es-spyware/

2. Descripción del problema
Anteriormente las herramientas de trabajo colaborativo no se utilizaban con mucha frecuencia, teniendo en cuenta que la mayoría de las personas trababan al interior de las compañía, por lo cual estas herramientas no se presentaban mayor riesgo, pero en la actualidad este contexto cambio y la demanda de uso de estas herramientas se elevó significativamente, ocasionando que el riesgo se elevara igualmente, como lo revela el programa SAFE, donde en Enero y Junio de 2020, se incrementó en un 364% la suplantación a sitios web, con el fin de obtener información y un 72 % la violación a los datos personales. En la mayoría de las situaciones no se tienen claros los esquemas básicos de aseguramiento para el uso de estas herramientas de trabajo colaborativo, este desconocimiento por parte de los usuarios hace que sea mucho más fácil engañarlos y de esta forma ejecutar un ataque.

3. Objetivos

OBJETIVOS GENERAL

Investigar los ataques informáticos más comunes presentados a herramientas de trabajo colaborativo en el contexto organizacional colombiano.

OBJETIVOS ESPECÍFICOS

Recopilar información relacionada con las herramientas más comunes de trabajo colaborativo usadas en las organizaciones. Analizar el estado actual de la ciberseguridad en las organizaciones colombianas Proponer un esquema básico de aseguramiento para el uso de las herramientas más comunes de trabajo colaborativo que permita aportar en la reducción de incidentes que afecten los activos de información de una organización

4. Metodología

La metodología utilizada en el presente trabajo monográfico es la de recolección de información, esta se realizara sobre los ataques informáticos más comunes presentados a herramientas de trabajo colaborativo en el contexto organizacional colombiano, se realizara un análisis del estado actual de la ciberseguridad en las organizaciones, a fin de entregar un esquema básico de aseguramiento para el uso de las herramientas más comunes de trabajo colaborativo con el fin que esta nos permita aportar en la reducción de los incidentes que afecten la información de una organización.

5. Referente Conceptual

Con el fin de Proponer un esquema básico de aseguramiento para el uso de las herramientas más comunes de trabajo colaborativo que permita aportar en la reducción de incidentes es necesario entender los conceptos para la elaboración del mismo y saber que tipos de herramientas colaborativas existen.

6. Resultados

Se logro Proponer un esquema básico de aseguramiento para el uso de las herramientas más comunes de trabajo colaborativo que permita aportar en la reducción de incidentes que afecten los activos de información de una organización

7. Conclusiones

Los ataques informáticos han aumentado a medida que va avanzado el tiempo, Vemos que antes se presentaban ataques pequeños aislados, pero en este momento hay muchas modalidades de ataques y técnicas sofisticadas hacia las organizaciones, las cuales pueden dejar como resultado perdidas muy grandes que se pueden ver reflejadas en la quiebra total de una organización.

Actualmente las herramientas de trabajo colaborativo son muy utilizadas en el contexto organizacional colombiano ya que integran todas las líneas de comunicación entre los empleados, esto ha hecho que se incremente los riesgos, por esta razón es tan importante tomar medidas preventivas al momento de utilizarlas.

Independientemente de la organización para la que se trabaje y/o el sector, se debe concientizar a los usuarios sobre el manejo de las herramientas colaborativas, ya que son los eslabones más débiles, además del establecimiento de un esquema básico para el uso de estas herramientas colaborativas, esto nos ayudara a prevenir incidentes que puedan afectar la información de una organización.