CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

URIEL GARZON SANCHEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JOSÉ DEL GUAVIARE
2021

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

URIEL GARZON SANCHEZ

Proyecto de grado presentado para optar el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

ESP TUTORA. YENNY STELLA NUÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JOSÉ DEL GUAVIARE
2021

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

San José del Guaviare., 8 de diciembre de 2021

DEDICATORIA

A Dios, primeramente, por darme la oportunidad de hacer realidad ha este sueño, pero con tanta sabiduría y esfuerzo he logrado llegar hasta este momento tan especial en nuestra vida. A mi madre, por ser el pilar más importante y por demostrarme siempre su cariño y apoyo incondicional sin importar las consecuencias o dificultades que se pudiese presentar.

AGRADECIMIENTOS

Agradezco a las directivas de la universidad Nacional Abierta y a Distancia UNAD, por brindarme su apoyo y continuidad con la especialización, también a los tutores y asesores de esta plataforma que han demostrado su tiempo su apoyo para esta formación. Reconozco que si su apoyo este logro no hubiera sido posible para alcanzar con éxito a un sueño hecho realidad.

CONTENIDO

pág.

LISTAS DE FIGURAS

pág.

LISTAS DE TABLAS

pág.

GLOSARIO

ACTIVOS: Son todos aquellos elementos de información o recursos con los que cuenta la empresa, seguridad física, seguridad digital, seguridad humana.

ATAQUE CIBERNÉTICO: O ciberataque son cualquier intento sin consentimiento previo de exponer alterar, deshabilitar, destruir, robar u obtener acceso a cualquier tipo de información sin importar el dispositivo o plataforma que la custodie.

ATAQUE: Explotación de una o varias vulnerabilidades utilizando un método de ataque con el fin de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja.

BOTNET: Conjunto de ordenadores controlados remotamente por un atacante, los cuales pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de spam, ataques de DDOS y códigos maliciosos.

CIBERSEGURIDAD: Es la primera línea de defensa, abarca muchas disciplinas en materia de seguridad, su función es la práctica de proteger dispositivos, sistemas, redes y datos, y de ataques u otros propósitos maliciosos.

DENEGACIÓN DE SERVICIO (DDOS): Consiste en mantener ocupada la red consumiendo el ancho de banda con mensajes constantes que alteran la normalidad de la prestación del servicio. Rf. (gb-advisor, 2018)

INCIDENTES: Es todo acceso, todo intento, todo uso, toda divulgación, modificación, violación, destrucción al correcto funcionamiento de un sistema sin ser autorizado.

INTRUSIÓN: Es la relación de un Incidente o violación de las políticas de seguridad, Violación de los permisos de acceso a un sistema sin estar autorizado para hacerlo, como es el caso de los hackers.

PHISHING: Engaño al usuario para obtener su información confidencial mediante la suplantación de la identidad de un organismo o página web de Internet.

PUERTA TRASERA: Tipo de software de control remoto que permite ingresar en un sistema operativo, página web o aplicación a una determinada parte de los mismos

que usualmente está restringida a un usuario ajeno, evitando los métodos de autentificación usuales.

RANSOMWARE: Es un código malicioso para secuestrar datos, una forma de explotación en la cual el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado.

SPAM: Son mensajes no solicitados, comúnmente de tipo publicitario, enviados en forma masiva y reiterativa. El correo electrónico es la vía más utilizada para este tipo de ataques; pero también se da el caso de presentarse por programas de mensajería instantánea; e incluso mediante el teléfono celular.

SPYWARE: Tipo de software malicioso que al instalarse intercepta o toma control parcial de la computadora del usuario sin el consentimiento de este último.

SMS: Más conocido como mensaje de texto.

SMISHING: Se apoya en la técnica de ingeniería social, enviándole a la víctima un SMS a su dispositivo móvil.

USB CEBO: Despliegue del dispositivo, USB malicioso por las inmediaciones del objetivo.

VISHING: Consiste en suplantar la identidad del afectado mediante llamadas telefónicas, creando una voz automatizada similar a la de las entidades bancarias.

VULNERABILIDAD: Es una debilidad que puede ser explotada por un ataque cibernético para obtener acceso no autorizado o realizar acciones no autorizadas en un sistema informático. Ya sea por diseño, desarrollo, implementación, configuración de una aplicación servicios.

WORKSHOPS: son una herramienta muy utilizada en empresas, contiene temas, taller, charlas, reuniones, escenarios. No es otra que trabajo en equipo para poder desarrollar actividades, adquirir nuevos conocimientos y habilidades.

RESUMEN

Este trabajo se enfoca. Asia una investigación detalla a las metodologías de defensa y el mejoramiento de la ciberseguridad en las organizaciones en Colombia. Realizadas a través de acciones por parte de los equipos de seguridad **RT y BT**, el equipo de defensa y el equipo de ataque, al primer equipo de defensa BT inicia en la organización a lo que realizan pruebas altamente especializada de intrusión, en Preparación y defensa frente a ataques dirigidos y amenazas reales en la actualidad, se logra principalmente a las organizaciones o empresas del país como las llamadas **(PYMES)**, puesto que en ella se encuentra todos los activos de información y los datos, son el pilar más importante en una empresa. Por esta razón surge muchas implicaciones, debido el impacto de los ataques cibernéticos.

Para el ejercicio se realizara la ejecución de las cuatro faces metodologías, acompañado con los equipos estratégicos, donde se tendrá en cuenta las técnicas y tácticas en la organización, después se pone a prueba las capacidades de detección y respuestas a incidentes de la organización, se identificara vectores de ataques simulados, dirigidos y de acceso, también se va conocer los problemas de ataques cibernéticos en el futuro, se identificara las puertas más vulnerables, los impactos emergentes, al final se planteara una propuesta alineada con herramientas y acciones para mejorar y regular la ciberseguridad en las organizaciónes de los ataque reales en Colombia.

INTRODUCCIÓN

En este trabajo se detalla los principales problemas relacionados a la diversidad y novedad de ataques en la actualidad hacia organizaciones colombianas y la falta de capacidades de respuesta.

Hoy en día los ataques globales han demostrado un gran impacto en las empresas en la sociedad, haciéndose cada vez que estos intrusos son más actualizados con nuevas modalidades de ataques, a través de programas maliciosos se filtran enviando y ejecutando cualquier tipo de malware valiéndose de los medios de cualquier vector de ataques cibernéticos. Ya que esto son el causante de los impactos emergentes para las organizaciones afectando principalmente la criticidad de los activos de información y datos. Una de las técnicas más usada de los cibernéticos en Colombia son los famosos *ataques dirigidos y amenazas reales*, los Ataque dirigido son los que se enfocan hacia un objetivo, intentar lograr obtener información específica bien sea a un usuario en particular, las Amenazas reales son materializada valiéndose de los activos o recursos disponible en una organización, por medio de ellos de alguna vulnerabilidad disponible ejecutan cualquier tipo de malware.

Con los equipos de primera línea de defensa y de ataque, se enfoca a la proyección de aquellos aspectos que se definieron en los objetivos especifico alineados en el trabajo. Con el propósito de mejorar la ciberseguridad en Colombia con una propuesta argumentada basada en técnicas y acciones. Poniendo en primer lugar a prueba las capacidades de respuesta simulada frente a vectores de ataque, seguida de metodologías, técnicas existentes, y los impactos emergentes causados de los ataques cibernéticos.

1 DEFINICIÓN DEL PROBLEMA

1.1 FORMULACIÓN DEL PROBLEMA

El enfoque de este trabajo se analiza y se consolidan aquellos incidentes, y amenazas más frecuentes en Colombia, algunos casos reales han afectado a las organizaciones, así como a los usuarios. Es importante tener en cuenta de las nuevas técnicas o modalidades más sofisticados en la actualidad, esto le permitirá al equipo de seguridad optar por las mejores alternativas para contrarrestar los riesgos presentes. Ya que le ayudara a evaluar planes de mitigación que minimice el impacto que puede causar la perdida de información o el daño de los sistemas, a partir de lo anterior, se plantea la siguiente pregunta.

¿Cómo los equipos de seguridad **Red Team Blue Team** permiten mejorar las capacidades de respuesta ante incidentes y amenazas cibernéticas en las organizaciones colombianas?

1.2 ANTECEDENTES DEL PROBLEMA

En la contextualización sobre la ***Diversidad y novedad de ataques en la actualidad hacia organizaciones colombianas y la falta de capacidades de respuesta.*** Se ha consolidado que el mayor factor dirigidos han sido por.

El **cibercrimen,** ha experimentado un crecimiento durante los últimos años casi de forma paralela al uso de las nuevas tecnologías y las pérdidas generadas por los ciberataques, sitúan a esta problemática como una de las principales economías ilegales en el País. El impacto que sufren las empresas colombianas luego de un ciberataque trasciende el coste económico por pérdidas de sus activos financieros y conlleva de manera colateral afectaciones a la productividad, daños reputacionales e incluso implicaciones de carácter legal por fuga de información privilegiada y datos sensible.[1] La **ciberdelincuencia** es otro nivel global crece a un ritmo considerable con nuevas tendencias emergiendo permanentemente en la actualidad. Los ciberdelincuentes cada vez se especializan más, siendo capaces de hacer uso de las nuevas tecnologías en pro de sus intereses, adaptan sus ataques

[1] **CCIT**, Tendencia Cibercrimen en Colombia 2019 – 2020, Crecimiento durante los últimos años, del uso de las TIC P.4.

utilizando nuevos métodos y establecen redes de cooperación, dándoles la capacidad de materializar un ataque en cuestión de minutos. El incremento del uso de Internet y las tecnologías de la información y las comunicaciones, abren con ello una enorme ventana de oportunidades para que los ciberdelincuentes ataquen.[2]

También podemos visualizar y analizar en tiempo real de la página oficial de la policía, los incidentes informáticos que afectan la ciberseguridad nacional en Colombia. Al realizar una consulta de tal fecha, nos arroja estadísticamente los siguientes resultados teniendo en cuenta el tipo de delito, la modalidad y el sector.[3]

1.3 JUSTIFICACIÓN

Este trabajo tiene la finalidad de sustentar las principales incidentes y amenazas cibernéticas presentes en las organizaciones, para esto se llevara a cabo de pruebas de intrusión avanzada, en ejercicio con los equipos de seguridad **RT** y **BT**, a través de estos equipos ayudaremos a fomentar una cultura de prevención y protección de riesgo cibernético frente a amenazas dirigidas reales en Colombia, para hacer más eficaz se tiene la implementación de las metodologías que le permiten realizar detenidamente cada acción para las capacidades de detección y respuesta, así poder realizar y poner a prueba una combinación de vectores de ataques simulado en las organizaciónes, con esto logramos identificará su nivel de seguridad global de las empresas. Para los problemas presentes que se enfrenta las organizaciones hoy en día, son los mismos ataques sofisticado en la actualidad, son los que el personal de la empresa debe de conocerlo, identificarlo, e informar. Con el equipo RT se llevará a cabo la identificación de vulnerabilidades, impactos emergentes que puede ser utilizadas para comprometer los activos de información y así poder detectar y dar respuestas.

la **ciberseguridad,** un término clave en este trabajo, que será puesto en conocimiento de muchas organizaciones, la ciberseguridad es primero que todo teniendo en cuenta siempre la **integridad, disponibilidad, confidencialidad** de los datos y activos de información. También contamos con un conjunto de herramientas y acciones que nos permite defendernos de los ciberataques, ahora el problema es el **ciberespacio** donde hay que tomar cierta estrategia enfocada al mejoramiento de la ciberseguridad teniendo en cuenta la problemática que más afecte en las organizaciones en Colombia.

[2] **CAIVIRTUAL,** Balance Cibercrimen 2020, sobre los delitos penales ley 1273 del 2009 de 9 delitos sobre la tendencia cibernética p.2.
[3] **CAIVIRTUAL,** página oficial de la policía, para Reporte de Ciberincidentes informáticos reportados.

2 OBJETIVOS

2.1 OBJETIVOS GENERAL

Evaluar las técnicas, tácticas y metodologías, para los ejercicios de los equipos de seguridad RT y BT, mediante una revisión bibliográfica, para establecer una estrategia que permita mejorar los niveles de seguridad en las organizaciones colombianas.

2.2 OBJETIVOS ESPECÍFICOS

- Reconocer los problemas causados, por medio de ataques principales e incidentes a los que se ven enfrentadas las organizaciones, para identificar las puertas vulnerables, e impactos emergentes que puede ser utilizadas para comprometer los activos de información en Colombia.

- Identificar las metodologías, mediante la aplicación de técnicas o tácticas existentes, para el ejercicio de los equipos de seguridad RT y BT, para el análisis de capacidades defensiva, frente a la evolución de ataques dirigidos en la organización.

- Diseñar de una propuesta, que alinee a una estrategia para el mejoramiento de ciberseguridad en la organización, por medio de herramientas y acciones que recomiendan, para regular la diversidad de ataques reales en Colombia.

3 MARCO REFERENCIAL

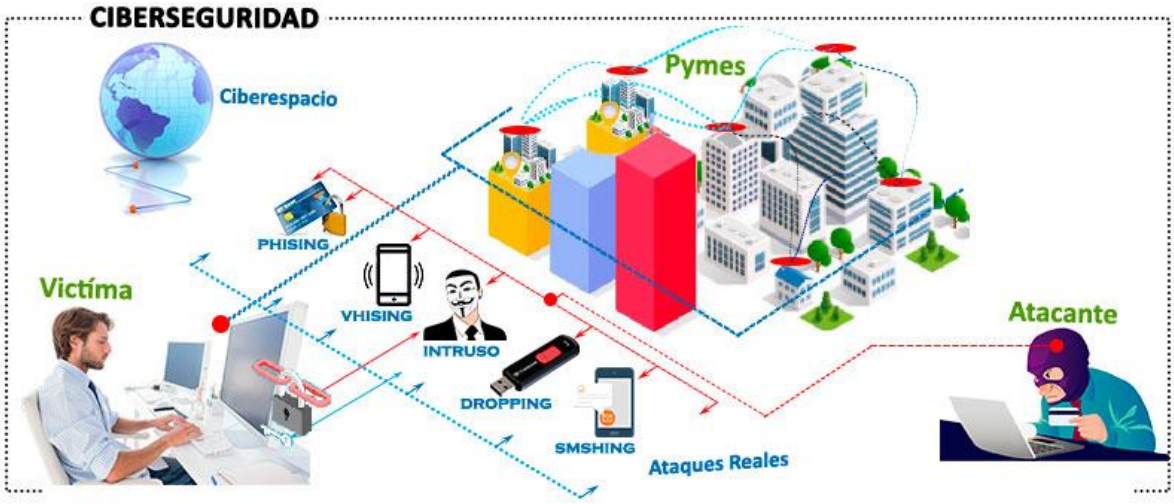
3.1 MARCO TEÓRICO

¿Cómo los equipos de seguridad RT y BT permiten mejorar las capacidades de respuesta ante incidentes y amenazas cibernéticas en las organizaciones colombianas?

3.2 CIBERSEGURIDAD Y ATAQUES EN LA ACTUALIDAD

3.2.1 PRINCIPALES ACTORES EN LAS ORGANIZACIONES

Figura 1. Actores en la Actualidad.



Fuente: Edición propia**.**

En realidad, la **ciberseguridad** es una responsabilidad de todos, claro que sí, concientizar, formar, preparar a una población que no tiene límite ni control en el **ciberespacio** es difícil**,** mucho dicen que todo lo que ocurre en la red o en las empresas son los **hackers**, es falso. Los hackers son personas que llevan la tecnología más allá de los límites que se creó, los malos son aquellos perfiles a que llamamos *cibercriminales, ciberataque, cibernético*, *cibercrimen, ciberdelito, ciberespionaje* y otros.

El auténtico **correo electrónico,** la herramienta de primer alcance de un ciberatacante, aprovechan la oportunidad de realizar ataques dirigidos a la víctima. Hoy en día ha sido un caos para la **ciberseguridad**, por supuesto en las organizaciones, empresas, usuarios de internet. El **número de celular,** otra herramienta igual al de correo electrónico. Este es uno de los vectores más peligrosos, para llegar rápido a un objetivo, a lo que hoy en día se llama la famosa técnica de **ingeniería social.**

3.2.2 CIBERSEGURIDAD PARA LAS EMPRESAS

En este proceso se tiene en cuenta los principales actores más relevantes en la actualidad, tenemos los **Administradores de seguridad, el Atacante, las pymes, los activos, y la víctima**. Se mostrará cómo proteger los activos o recursos de información en un **entorno personal y corporativa** en la organización, teniendo en cuenta para la empresa lo más importante son los clientes y proveedores ante todo la confianza plena con la empresa. Las **pymes** hoy en día es una de esa tecnología que se ocupan intercambiando información, usando todo el día los ordenadores, intercambiando información, accediendo a web de la administración, en fin. Veamos las siguientes recomendaciones.

❖ **Entorno de la información personal**

En este entorno basta con que el usuario esté enterado, preparado de las nuevas **modalidades de hurto** de la información, construir contraseñas fuertes para cada dispositivo y plataforma, y aprender a detectar los contenidos maliciosos que esperan ganarse la confianza del usuario para robar la información sensible, incluyendo números de tarjetas de crédito y claves de acceso que es el impacto emergente en Colombia. De acuerdo con un estudio realizado por **cisco**, el cibercrimen es relativamente mucho más rentable que realizar cualquier otro tipo de operaciones ilegales. **Netscout** dice que un hacker frente a un dispositivo **IOT** no protegido solo toman 5 minutos, todo tipo de herramientas profesionales de hackeo las puede encontrar en **Dark Web**. [4]

- **Primer paso - Contraseñas:** Con el fin de proteger mejor la información de los clientes, desactiva las alarmas, puerta de seguridad, vidrio puertero,

[4] **GB-ADVISORS,** Vectores de ataques en ciberseguridad, como eliminarse de ellos, con herramientas profesionales.

proteger los ordenadores, así evitar que cualquiera pueda entrarse y llevar todo lo que hay dentro de la empresa.

- **Segundo paso - Copia de seguridad:** Es obligatorio guardar copia de seguridad todos los días, mantener actualizado activas las soluciones que permita detectar ficheros a adjunto al correo o al internet.

- **Tercer paso - Actualizar la web:** Mantener y mejorar la seguridad del Portal web, cuando se ofrece nuestros servicios y para conseguir nuevos clientes, además debe cumplir con algunas Leyes como la **ley de protección de datos**. cambiar la contraseña, actualizar las herramientas que utiliza tu web.

❖ **Entorno de la Información corporativa**

En este entorno aplica directamente a todas las organizaciones y empresas del país, las siguientes listas de recomendaciones garantiza el correcto manejo y protección de la información cuando se encuentra frente a un riesgo potencial, veamos la siguiente lista.

1. Refuerza las prácticas de seguridad de tu empresa, incluyendo capacitaciones de sobre las **políticas de seguridad** en todos los niveles de la organización.

2. Realizar copias de respaldo de la información para garantizar el registro histórico de su modificación.

3. Entablar un buen hábito de construcción de contraseñas fuertes y elaboradas.

4. Encriptación de la información sensible, incluyendo las bases de datos de tus clientes.

5. Usar herramientas de ciberseguridad que apoyen el monitoreo constante del nivel de seguridad de la empresa.

6. Evaluar periódicamente las prácticas de seguridad de los proveedores con los cuales intercambia información.[5]

[5] **INTERNEXA**, Cómo protegerse contra los ciberataques, recomendaciones para adquirir buenos hábitos de ciberseguridad p.9.

3.2.3 COMO ATACAN LOS CIBERCRIMINALES EN EL FUTURO

En este modelo se muestra las 7 fases del ciclo de vida de un **modus operandi cibernético**, para apoderarse del sistema y de los activos de información en la organización.

Figura 2. Las 7 fases del ciclo de vida de un ciberataque y como protegerse.

Fuente: Edición propia.

Así operan, el **Atacante** es uno de los principales actores presente en una organización, el correo electrónico, el número telefónico. Han sido una herramienta fundamental en una empresa, así como es tan fundamental los atacantes se aprovechan de este servicio para fines delictivos como dirigir, instalar, ejecutar, engañar, y hurtar información confidencial de la víctima.

❖ **COMO ENVIAR UN ATAQUE DIRIGIDO MALICIOSO**

Existe muchos programas hoy en día, que le facilita al inexperto hacer este tipo de cosas. El **sappo: spear apps to steal oauth-tokens,** el **Tokens OAuth.**

spear apps: un software malicioso de los atacantes, que le permite enviar los correos fraudulentos a la víctima.

Tokens OAuth: Es un enlace que le llega a la víctima con información falsa, haciendo creer que es el original. Es ahí donde debemos tener precaución, que con un solo clic es lo que te permite a una persona acceder a todo lo que tiene en tu cuenta, es decir le acaba de dar un *Tokens OAuth* a la persona equivocada y tiene acceso al 100% de tu vida digital, veamos un ejemplo ilustrado.

- **Interacción 1 – Phising:** El atacante envía un E-mail a la víctima de una promoción interna con unos descuentos, que se le pide usuario y contraseña, la empresa descubre que es una suplantación de identidad Phishing lo elimina de inmediato. Y reporta al departamento de seguridad informática.

- **Interacción 2 – Vhising:** El atacante realiza una llamada a la víctima de parte de Microsoft diciendo que se ha detectado un problema en su equipo que es necesario repáralo de inmediato, la empresa descubre que es un fraude vhising cuelga de inmediato. Y reporta al departamento de seguridad informática.

- **Interacción 3 – Intruso:** El vigilante de la empresa identifica una persona que no está identificada y además está observando unos portátiles de sus compañeros, el vigilante descubre que puede ser un intruso y reporta de inmediato. al departamento de seguridad física para que confirme la identidad de la persona.

- **Interacción 4 – Media dropping:** El atacante deja una memoria USB botada en el piso, para que algún usuario de la empresa la recoja, piensa un momento si la conecto puedo infectar mi equipo, decide proporcionárselo al departamento de seguridad informática, Para que la analice.

- **Interacción 5 – Smshing:** El atacante envía un SMS al celular de la víctima donde le indica que sus contraseñas a caducado y que debe de resetearla, si la cambie hace dos días no es posible, descubre que es un ataque Smshing. Y reporta al departamento de seguridad informática.

3.2.4 PRINCIPALES TÉCNICAS Y TÁCTICAS EXISTENTES

Para un ciberatacante lo más fundamental es ir al ritmo de la tecnología digital, las técnicas y tácticas hacen que las grandes, medianas, y pequeñas empresas,

PYMES, tomen medidas pertinentes de los riesgos, así como en el **ciberespacio** veamos las ventajas que tiene estos cibercriminales hoy en día.

- **Conexión 5G:** Nos trae muchísima ventaja en cuanto la velocidad de internet, esto quiere decir que es menos controlable para los ciberataques, ya que esto le permite realizar un ataque en cuestión de segundo.

- **Ataques a dispositivos móviles:** Se incrementará los robos online a través de dispositivos móviles esto permite a que la sociedad esta muchísima más confiada cuando realiza pagos a través de nuestro dispositivo móvil, es muy importante mantener actualizado el software del dispositivo, y controlar los ajustes de seguridad y los permisos de cada aplicación.

- **Ataques SMShing:** Es el más común para los ciberdelincuentes, donde utiliza medio de mensajería como WhatsApp, Facebook etc. Consiste en enviar mensaje al usuario hacerle pinchar en determinados enlaces fraudulentos.

- **Aplicaciones de juegos:** Llevara a los ciberdelincuentes que hagan pequeños robos, ya que esta aplicación los usuarios están acostumbrados realizar pequeñas transacciones.

- **Webs bancarias:** Están en un punto de mira, porque son fáciles de duplicar, y así suplantar las identidades de los bancos para llevarlos a error y obtener información confidencial de los clientes del banco.

- **Redes sociales:** Son plataforma a lugar de fraude, llevan una suplantación de identidad de empresas copiando sus perfiles y sus páginas web para invitarnos a realizar ciertos tipos de acciones para realizar sus fraudes y engaños.

- **Inteligencia artificial:** que será utilizada para conseguir información confidencial tuya, datos, adivinar preguntas de contraseñas todo de ellos en las redes sociales, por ejemplo, la aplicación de envejecimiento de rostros.

- **Escuchas a través de los micrófonos:** escuchas no autorizadas a través de los micrófonos que incorporan los dispositivos.

3.2.5 PROBLEMAS QUE SE VEN ENFRENTADAS LAS ORGANIZACIONES

Hoy en día, la situación actual en Colombia es el **cibercrimen** ha crecido enormemente con el uso de las nuevas tecnologías TIC, esto ha puesto en paralelo las pérdidas monetarias generadas por los **ciberataques**, las empresas colocan este problema como una de las principales economías ilegales del país. **Los delitos informáticos** que más afectan a los colombianos son el hurto informático, violación de datos personales, acceso abusivo al sistema informático, transferencia no consentida de activos, uso de software malicioso estipulado en el artículo 1273 del 2006. [6]

Los cibernéticos tiene la capacidad de realizar un ataque en cuestión de minutos, por ello es importante conocer los tipos y modalidades de ataques que utilizan estos criminales hoy en dia. Para ellos, utiliza los famosos **vectores de ataques dirigidos**, siendo estos los más efectivos en infectar equipos y robar información, también se encargan de ejecutar una serie de actividades maliciosas, dejando a los equipos en un estado vulnerable, las vulnerabilidades son un primer paso para Planear un ataque, para ello necesitas técnica, táctica o ingeniería social, y así apoderarse de los activos de información, y abrir el camino a más infecciones. Esto indica que hay muchas posibilidades de sernos víctima de un **cibernético**. Sabemos que el factor principal son las vulnerabilidades de un sistema, se dividen principalmente en dos categorías, **vectores de ataque pasivos y vectores de ataque activos.** En un estudio realizado, cerca del 90% de los ciberataques que sufren las empresas en Colombia se deben a la **ingeniería social.** La siguiente tabla enumera la diversidad de ataques reales de este año 2021.

Tabla 1. Principales modalidades de ataques en Colombia 2020-2021.

	Principales modalidades de cibercrimen en Colombia	
Vectores	**Amenazas**	**Técnicas**
Ataque: BEC - (Correo Electrónico)		

[6] **CCIT,** Tendencia Cibercrimen en Colombia 2019 – 2020, información sobre crecimiento, numero incidentes, denuncias, delitos p.7.

✓ **(Phishing)** - Correos Fraudulentos Personalizados ✓ **(Watering Hole)** - Infección de sitios frecuentemente visitados por empleados	Afecta a la **cadena de suministros**, Es decir, a las comunicaciones con proveedores externos y socios de confianza.	Consiste en que los cibercriminales diseñan escenarios simulados, Utilizan técnicas de ingeniería social basados en SOCMINT y OSINT
Ataque: RANSOMWARE - (Secuestro de Datos)		
✓ **(IoT) -** Internet de las Cosas, compras, promociones, etc. ✓ **(Cryptolockers)** – para bloquear el acceso a los archivos del usuario. ✓ **(Lockscreen) -** Bloqueadores de pantalla evitan que las víctimas usen sus equipos bloqueando sus pantallas. ✓ **(Documentos con macros) -** que contienen código Visual Basic, para que el usuario de infecte.	Afecta a la integridad del usuario, como al secuestro de información en la organización, impedir la cancelación de las opciones para cerrar un programa o para apagar el dispositivo, de tipo.	Consiste que el usuario ejecute el correo fraudulento, con un **Tokens OAuth,** así lograr la información confidencial de la víctima y de la empresa.
Ataque: ATAQUE DDOS - (Denegación de servicio)		
✓ **(compañía)** – realizan un reconocimiento y escaneo de los servicios a afectar. ✓ **(servicios online)** – Uso redes de Botnet para lanzar ataques dirigidos. ✓ **(clientes)** - Interrupción de los servicios para los usuarios y terceros ✓ **(Bitcoins)** - Solicitud y demanda de pagos en criptomonedas. ✓ **(Protocolo 33)** – los atacantes explotan este protocolo para eludir la defensa. ✓ **(DCCP) –** a través de protocolo de control de congestión de datagrama.	Afecta a los servicios online de las compañías para impedir o interrumpiendo el acceso a usuarios tercero y clientes.	Consiste que el criminal aprovecha la saturación de la red, servidores, sitio web, Empleando redes maliciosas o **BOTNETS**, mediante mensajes extraños y solicitudes.
Ataque: Malware - (Software malicioso)		
✓ Correos con notificaciones ✓ suplantando entidades públicas ✓ Re direccionamiento hacia sitios web infectados por el atacante ✓ Descarga de aplicaciones maliciosas ✓ **(Media dropping)** – utiliza una memoria USB infectada. ✓ **(intruso)** – persona no identificada y sospechosa en la organización.	Afectación a la PYMES.	Consiste que el criminal utiliza un correo electrónico fraudulento como medio, para la instalación del programa malicioso.

Ataque: SIM SWAPPING - (Secuestro o cambio de SIM CARD)		
✓ **(Darknet)** - Consiguen datos de las víctimas en mercados ilegales. ✓ **(vhising)** – uso de la línea telefónica, para engañar a personas. ✓ **(Smshing)** – se produce mediante mensajería instantánea de texto fraudulentos.	Afecta al sistema financiero y obtener el código 2FA para realizar transacciones y afectar los activos económicos de las empresas.	Consiste en que los criminales utilizan técnica de persuasión y manipulación psicológica.
Ataque: CRYPTOJACKING - (Minería de criptomonedas)		
✓ Cuando acceden a sitios web infectados. ✓ Generar criptomonedas por medio de comandos computacionales de un tercero. ✓ Un malware al instalar una aplicación. ✓ Un malware al recibir un correo electrónico. ✓ Activación de un software que lo contenga.[7]	Afecta, a ordenadores, PC, teléfonos móviles reduciendo la velocidad de otros procesos aumenta la factura de la luz y acorta la vida del dispositivo. Y genera pérdidas en ventas y negocios de las pymes.	Consisten en la instalación de un software que está diseñado para permanecer oculto al usuario, así robar los recursos informáticos (malwarebytes, s.f.).

Fuente: Investigación propia.

3.2.6 IMPACTO EMERGENTES EN LAS ORGANIZACIONES

El impacto sufrido por las empresas colombianas ha permitido identificar cientos de formas de modalidades de hurto, de ciberataques y cibercrimen. Mencionado en la **(tabla 1).** A través de ellos utilizan diferentes técnicas de modalidad de ataques dirigido a través de vectores de acceso. Son tan peligrosos que ya tienen toda la información del usuario, es decir, conocen muy bien a sus víctimas. Cuando hablamos de impacto emergente, estos son los ataques con mayor impacto en incidentes y, a su vez, son los más reportados en Colombia. Estos impactos han provocado un incremento del costo económico cada año por la pérdida de sus activos financieros y colateralmente conllevan efectos en la productividad, daños reputacionales e incluso implicaciones legales por la fuga de información privilegiada, en la siguiente tabla se muestra los impactos emergentes.

[7] **REDSEGURIDAD,** ¿Qué es el cryptojacking y cómo evitar este 'malware' que mina criptomonedas? Ya que es un tipo de malware malicioso que provoca el uso no autorizado.

Tabla 2. Impactos emergentes de ataques cibernético en Colombia.

El impacto de los ataques cibernéticos en las organizaciones
✓ Pérdidas financieras ✓ Pérdida o daño de información confidencial, propiedad intelectual ✓ Continuidad del negocio ✓ Daño de reputación ante clientes ✓ Transacciones ilícitas con la información hurtada ✓ Incidentes de estado ✓ Ciberguerras (Grupos radicales o estados completos) ✓ Violencia ✓ Afectaciones mentales (cyberbulling, cyberstalking) ✓ Indisponibilidad de canales de atención a los clientes, sumando a ello sitio web, redes sociales y plataformas de soporte.

Fuente: "http://www.internexa.com/" [8]

3.2.7 COMO DEFENDERNOS DE CIBERATAQUES CON VECTORES

Para evitar ser sorprendido por un ataque cibernético, tanto con la **información personal** como con la **información corporativa** veamos la siguiente tabla.

Tabla 3. Recomendaciones para defendernos ante vectores de ataques.

Víctima de ataque	Recomendaciones ante vectores
✓ **Spoofing,** ✓ **DDoS,** ✓ **Sniffing,** ✓ **Vishing,** ✓ **phishing,** ✓ **Antimalware,** ✓ **Ransomware,** ✓ **ingeniería social** ✓ **SIM scaping** ✓ **SMShing** ✓ **USB cebo,** ✓ **Media dropping** ✓ **Intruso**	✓ Evita compartir accesos de las redes sociales. ✓ Actualiza todos los parches de seguridad. SO, Driver. ✓ Entrena a todo el personal de la empresa, sobre las buenas prácticas y políticas de seguridad. ✓ Emplea firewalls, IDS/IPS, DMZ, WAF, de una red privada o pública. ✓ Haz respaldos o Backups periódicos de tus datos sensibles, en caso de fallos o ataques en el sistema. ✓ Mantén informado sobre las últimas tendencias en seguridad digital. ✓ Aprende a detectar y diferenciar los contenidos maliciosos

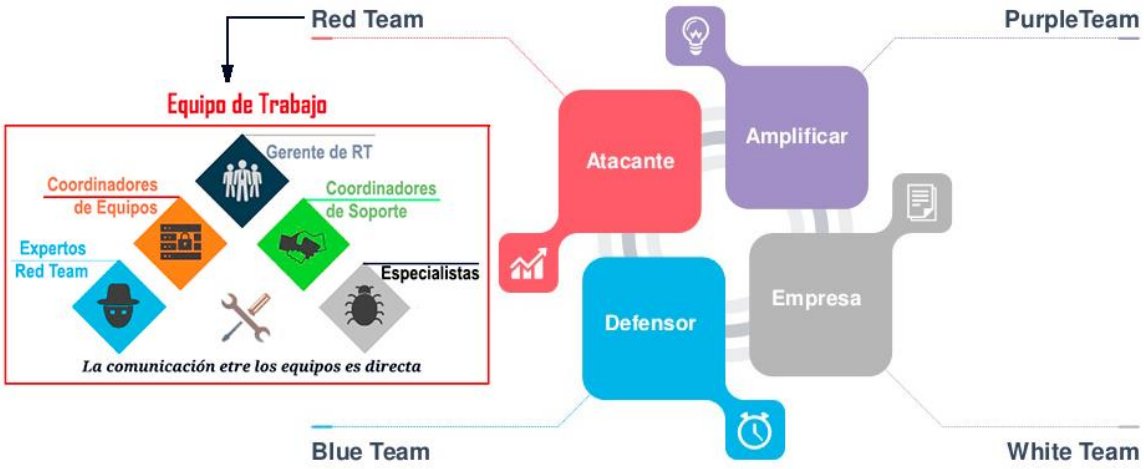
[8] **INTERNEXA,** Las 5 herramientas más poderosas en ciberseguridad, sobre los impacto de los ataque cibernéticos p.7.

- ✓ Construya contraseña fuerte para cada dispositivo y plataforma.
- ✓ Usa antivirus que se actualice constantemente.
- ✓ Analizar los archivos antes de abrir
- ✓ Configura las aplicaciones de tu dispositivo móvil, SMS, micrófono, ubicación, cámara, videos.

Fuente: "https://www.gb-advisors.com/es/vectores-de-ataque-en-ciberseguridad/"[9]

3.3 DEFENSA ESTRATEGICA A EJERCICIOS RED TEAM & BLUE TEAM

Figura 3. Equipos involucrados.[10]



Fuente: Edición propia.

El ataque es el secreto de la defensa, la defensa es la planificación de un ataque, la misión de un equipo **Red Team** es simular ataques reales que sean controladas dentro de una organización, con el fin de lograr un acceso no autorizado. En la estructura se va mostrar la comunicación entre equipos de trabajo, equipos involucrados. cada equipo tiene una función correspondiente. Pero debe estar bajo a un reglamento legal, donde se establezcan roles y responsabilidades, y

[9] **GB-ADVISORS,** ¿Qué debemos hacer para librar nuestras redes de vectores de ataque en ciberseguridad? Mencionamos algunos consejos para mantener a salvo la información.
[10] **MOSCOWCON,** Aspectos técnicos de la realización de ejercicios de Red Team, p.11.

reglamentos éticos dentro de una organización. para el ejercicio se tiene claro que inicia el primer equipo de la primera línea de defensa, dándole la seguridad a **Blue Team**, y la posibilidad de defenderse de forma controlada, es decir el *Red Team es un entrenamiento para el Blue Team.*

El lema de Red Team, Pensando como el enemigo *"Conócete a ti mismo y conoce a tu enemigo".* frases sabias puesta por el filósofo y militar chino, Sun Tzu. Donde se va a evaluar las capacidades reales que tiene una organización para proteger sus activos críticos y sus capacidades de detección y respuesta considerando el ámbito de seguridad **digital, física, humano** que tiene la organización. Rf. (G. Juanes, 2016).

3.3.1 ÁMBITOS DE ACTUACIÓN DE SEGURIDAD EN LA ORGANIZACIÓN

Figura 4. Nivel de seguridad global.

Fuente: Edición propia.

Primero que todo se requiere un equipo de trabajo que debe estar formado por cuatro ámbitos de actuación de seguridad **digital, física, y humano.** Con ellos se va verificar el nivel de protección de la organización, frente a *ataques dirigidos*, ya que esto busca tomar el control de los principales activos de la organización, mediante la *combinación de vectores de ataque* y *amenazas dirigidas*. En este ámbito es fundamental teniéndose en cuenta en todas las acciones y proceso para el ejercicio.

3.3.2 ATAQUES QUE SE ENFRENTA EL EQUIPO RED TEAM

Figura 5. Simulación Real de un Ataque Dirigido.[11]

Fuente: Edición propia**.**

Cuando hablamos de **ataques dirigidos** entendemos que son aquellos **vectores de ataques de acceso.** Es decir que podemos recibir a nuestro nombre un E-mail, o un ataque Phishing en fin. Las empresas de hoy en dia son las mas atacadas a estas ciertas practicas o tecnica cibereneticas, sabemos que para ellos no sigue normas ni reglas.[12]

En este modelo de ataques, el equipo estratégico Red Team, se enfrenta a cinco pasos fundamentales que serán satisfactorio para llevar con éxito la seguridad y la defensa hacia el acceso o activo de la organización en la empresa,

1. Identificación del nivel de seguridad global y riesgo real de la organización
2. Entrenamiento del equipo de seguridad frente a amenazas (APT)
3. Identificación de vectores de acceso críticos (acceso o activos)
4. Comprobaciones de seguridad en los ámbitos digitales, físico, humanos.
5. Impacto real de negocio

[11] **INNOTEC CCN-CERT,** Enfoques y aspectos clave en ejercicios Red Team, evolución y simulación real de un ataque dirigido p.3.
[12] **REDES ZONE,** Gran aumento de ataques dirigidos, son muchos más peligroso y frecuentes en la actualidad.

3.3.3 METODOLOGÍAS PARA EL EJERCICIO RT Y BT

Figura 6. Modelo de amenazas realizado al inicio.

Fuente: Edición propia.

Se da inicio las principales metodologías de este modelo, para el ejercicio de defensa a través de estas cuatro fases, con el fin de obtener y recopilar información para el equipo Red Team, teniendo en cuenta el ámbito de seguridad en que se encuentra **digital, físico, humano.** Así realizar las capacidades de detección y respuesta frente amenaza. Este modelo cuenta con ciertos enfoques que son,

- ✓ **Objetivos:** Que es la simulación de un ataque dirigido o APT sobre una determinada organización.

- ✓ **Alcance:** Identificar **vulnerabilidades** en aquellos activos definidos, demostrar cual sería el **nivel de riesgo** e **impacto** que tendría un ataque dirigido sobre la organización.

- ✓ **Pruebas:** Ámbitos de ataque permitidos, vectores de acceso y ataque identificados.

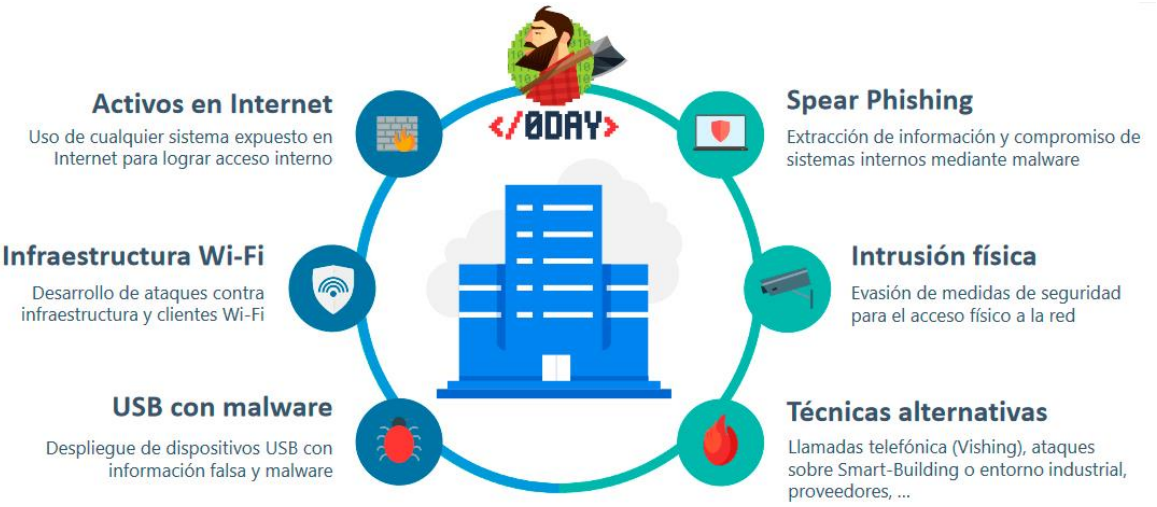
- ✓ **Beneficios:** Identificación de vectores de ataque críticos, evaluación del nivel de exposición y riesgo, capacidad de prevención y detección de amenazas, eficiencia de los procedimientos internos y, por último, la identificación de principales vulnerabilidades y debilidades de la organización.[13]

3.3.3.1 PASO 1 - DEFINICIÓN Y PLANIFICACIÓN

En esta etapa se define qué tipo de **vectores** serán utilizados y de qué manera serán atacados. Después de **definirlos**, se pasa a una etapa de **planificación** en el tiempo de las acciones que apoyan estos ataques.

- ❖ **Vectores de Acceso Red Team**

Figura 7. Vectores de acceso e intrusión Interno.



Fuente: Edición propia.

De esta forma se tiene acceso para pivotear a un atacante, y no dejar que se apodere y tome control de los elementos de información de la organización. cada uno de estos son vectores de ataque más conocidos, son tan peligros por el impacto que genera en la organización, es importante tomar medidas de control a tiempo ante cualquier vulnerabilidad critica que se presente, y sobre todo informar. Así

[13] **HACKBYSECURITY**, cumplimiento de la normativa de seguridad infromatica, en la organización de vulneravilidades e incidentes cibernetico.

evitar ser víctima de un fraude. Cuando se habla de un vector es la ruta o camino que utiliza un atacante para tener acceso al activo u objetivo de ataque.

3.3.3.2 PASO 2 - RECONOCIMIENTO EXTERNO

consiste en desarrollar todas las **acciones** posibles para identificar los activos que están expuestos en el **ámbito** que se vaya a comprobar, para después, empezar a probar cada parte y así identificar las vulnerabilidades para hacer una **intrusión**.

❖ **Vectores de Ataques Externo**

Dependiendo de los ámbitos de actuación **digital, físico, humano** se tendrá en cuenta una lista de vectores más reconocidos en la organización.

Tabla 4. Vectores de Ataques externo.

Intrusión física	Instrucción digital	Ingeniería social
"Cualquier vector que permita acceso a la infraestructura física"	"Cualquier vector que permita acceso a la infraestructura digital"	"Cualquier vector que haga uso de ingeniería social"
✓ Análisis perimetral de seguridad física ✓ Identificación de acceso alternativo ✓ Evasión de controles RFID/NFC ✓ Evasión de controles biométricos ✓ Evaluación de sistemas embebidos ✓ Análisis Wireless ✓ Control remoto de CCTV ✓ Análisis de Smart-building ✓ Análisis físico de entorno industriales	✓ Anonimizarían de las comunicaciones ✓ Análisis de sistemas perimetrales ✓ Análisis de servidores públicos ✓ Intrusión y control de dominios internos ✓ Control a sistemas industriales ✓ Control de sistemas mainframes ✓ Desarrollo de exploits propios ✓ Desarrollo de malware a media ✓ Obtención de información critica	✓ Desarrollo de campaña de phishing ✓ Envió de phishing dirigido ✓ Envió de malware personalizado ✓ Despliegue de dispositivo USB cebo ✓ Acciones de vishing personalizado ✓ Suplantación de identidad ✓ Escenario personal de ingeniería social ✓ Análisis de leaks y datos filtrados ✓ Creación de escenarios a medias

Fuente: Propia**.**

3.3.3.3 PASO 3 - COMPROMISO INICIAL

En este paso se identifica una **vulnerabilidad** lo suficientemente crítica que permita abrir paso a la **intrusión**, puede ser desde hacer ataques de fuerza bruta para obtener usuarios, hasta una subida de ficheros que permita **pivotar** a la red interna.

Nuestro servició **Red Team** realiza ataque real por un equipo de especialista, un grupo que actúa como si fuera atacantes que se enfrentan a **Blue Team** primera línea de defensa en la organización, como lo hacemos creamos un acceso no autorizado pivoteando redes **wifi, correo electrónico, perímetro.** Tratamos no solo de entrar sino a poner a prueba los sistemas de detección y respuesta a incidentes de la organización.

3.3.3.4 PASO 4 - ACCESO A LA RED INTERNA

Una vez se compromete un primer activo, se debe buscar el camino y la forma para acceder a la **red interna**. Este proceso puede variar según la seguridad de la empresa y puede convertirse en un ejercicio de minutos o días.

Así es, los equipos **Red Team** pasan más tiempo planeando un ataque que realizándolos, despliegan una serie de métodos para obtener acceso a una red. Todo con tal de conseguir información de interés, nombre, **horarios, claves, número de tarjeta**, esperamos que nos detecte y así comprobar los mecanismos que tiene la organización para detectar y dar respuesta a un incidente en la organización.

Tabla 5. Formato de asistencia para un servicio de Red Team.

Datos para Ejercicio Red Team			
Alcance:	*Completo*	**Ámbito:**	*Cualquier ámbito*
Detalle:	*Desconocido por la organización*	**Tiempo:**	*Horas, Días, Meses*
Vectores:	*Simulación de amenazas dirigidas*		

Fuente: Investigación propia.

3.3.3.5 PASO 5 - ELEVACIÓN DE PRIVILEGIOS

Esta etapa del ejercicio busca crear vías de acceso secundarias en caso que el **Blue Team** detecte el ataque al **vector principal** y lo detenga. De esta manera se podrá continuar con el ejercicio, incluso sin la detección del equipo de seguridad.

Persistencia: El objetivo es garantizar el acceso a la infraestructura sin ser detectado como lo hacemos.

Instalando puertas traseras en sistemas como:

- ✓ Aplicaciones (tipo RAT) que permiten acceder directamente.
- ✓ Creando usuarios y contraseñas para usar posteriormente.
- ✓ Habilitando accesos remotos (rdp, ssh o similares).
- ✓ Creando nuevos servicios.

Vulnerar el menor número de sistemas posibles:

En este método es generar una clave en el registro para arrancar un meterpreter cada vez que el sistema se reinicie. La **exfiltración** es la fase la que se extrae la información del perímetro de la organización para esto realiza la. Utilización de proxy HTTP/HTTPS, Uso de correo electrónico, Túneles DNS/ICMP.[14]

3.3.3.6 PASO 6 - RECONOCIMIENTO INTERNO

Cuando se tiene acceso pleno a toda la organización, lo primero que se debe hacer es un reconocimiento interno de todos los activos para evaluar cuáles podrían ser los ataques más radicales que se puedan hacer.[15]

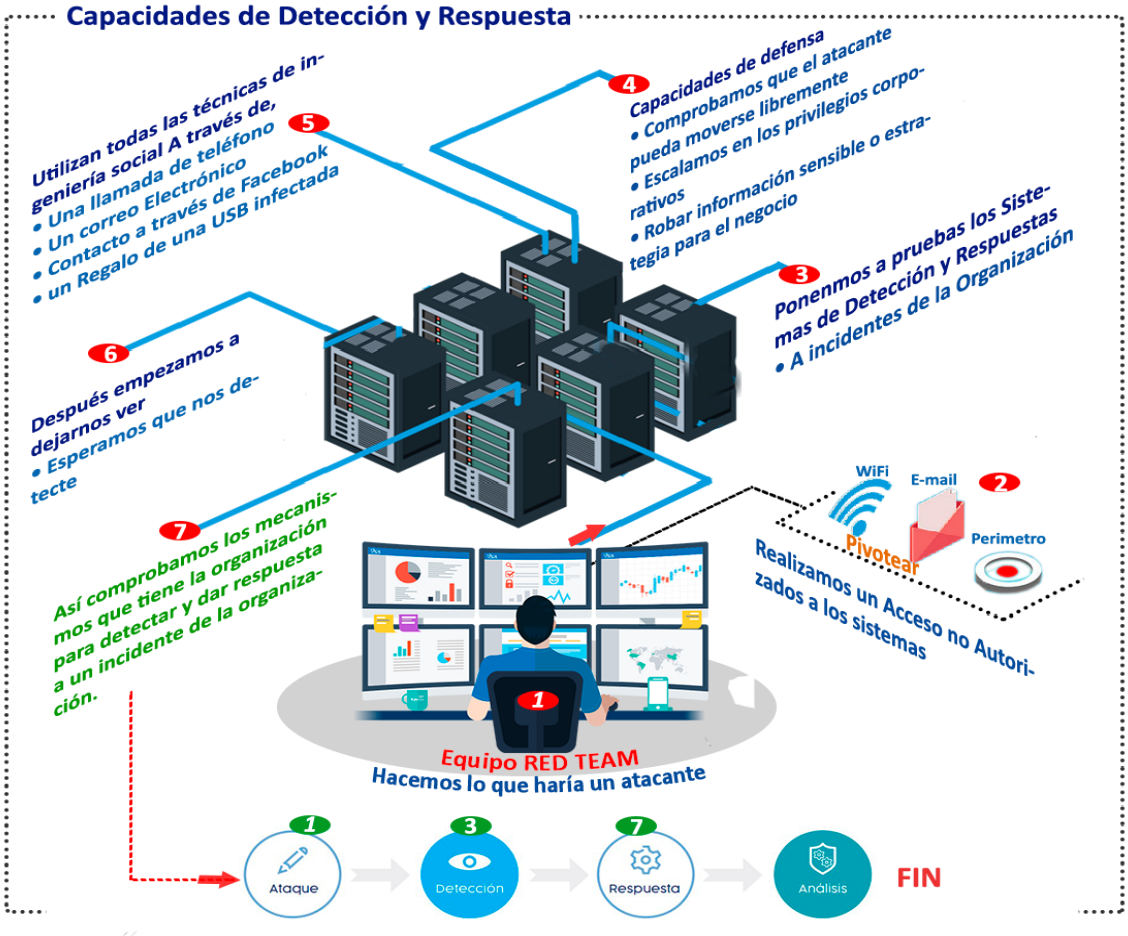
El movimiento lateral: se conoce como **salto de red**, o **pivotar**. consiste en vulnerar otros sistemas para obtener más información o mayores privilegios en la red. Ejemplo Cazar credenciales de un administrador de dominio. Localizar un servidor con acceso a toda la red como rutas, Revisar servidores, sistemas de ficheros, etc.[16] Se realiza mediante:

[14] **CYBERCAMP,** RedTeam, el hacking en otra dimensión 0, movimiento lateral, mantener persistencia p.35 y 40.
[15] **KEEPCODING**, ¿Qué es Red Team en Ciberseguridad? Equipo de primera línea estratégica en la organización.

- ✓ Ataques de red – MiTM
- ✓ Reutilización de contraseñas –PtH
- ✓ Otras vulnerabilidades en otros sistemas
- ✓ Errores de configuración.

3.4 CAPACIDADES TECNICA DEL EQUIPO RED TEAM

Figura 8. Modelo de ejecución de las Capacidades RT y BT.



Fuente: Edición propia.

Así comprobamos las capacidades de **Detección y Respuesta,** con los equipos de seguridad Red Team, dos conceptos claves que se tiene en cuenta porque **Detección,** por la exposición de técnicas y tácticas y procedimientos de ataque habituales en **seguridad en sistemas**, porque **Respuesta,** para llevar a cabo

reuniones entre determinadas personas para el análisis de infraestructura y ataque sobre ella a lo que llamamos un **workshop, En seguridad en redes.**

3.4.1 BENEFICIOS PARA LA ORGANIZACIÓN

En este modelo se centra en la **Preparación y Defensa frente a Ataques Dirigidos y Amenazas Reales,** resumidos en estos cuatro pasos.

Figura 9. Beneficios para la organización.[17]

Fuente: Edición propia.

En este modelo se sigue cuatro pasos, que nos trae como beneficio para la organización global,

1. **Primer paso** identificar el nivel de seguridad real, y exposición de la organización frente a un ataque dirigido.

2. **Segundo paso** identificación e incremento del nivel de detección y respuesta a incidentes.

[17] **MOSCOWCON,** Aspectos técnicos de la realización de ejercicios de Red Team, sobre preparación y defensa frente ataques dirigidos y amenazas reales p.13.

3. **Tercer paso** identificación del tiempo para la recuperación de una amenaza y procedimientos.

4. **Cuarto paso** identificación de vectores de ataques más críticos para la empresa combinados. [18]

3.5 PROPUESTAS PARA MEJORAR LA CIBERSEGURIDAD GLOBAL

3.5.1 Mejorar el uso de las herramientas TIC en las organizaciones

El principal problema es el mal uso que le dan los usuarios a la herramienta TIC, las ventajas de estas herramientas es que nos permite la cercanía con las personas y los clientes, también han transformado la manera de trabajar y gestionar recursos en las grandes, medianas, y pequeñas empresas "PYMES", se ha convertido en un elemento clave para que el trabajo desarrollo sea más productivo. Agiliza la comunicación de la empresa con su entorno, sustenta el trabajo en equipo, y aumenta la productividad de la empresa. *Rf.* (Martín, 2021)

Debido a la **Transformación digital**, permite que las organizaciones compitan a la medida que la tecnología evoluciona, eso es necesario para cualquier empresa. Pero en realidad lo que nos interesa es la **Seguridad TIC, o seguridad de tecnología de información** también conocido como **ciberseguridad**, la importancia de esto es algo que no se puede negar, sabemos que la nueva sociedad cada vez más conectados, más información compartida en la red, tanto particulares como empresas. Hay estaríamos generando una falta de seguridad esto puede llevarle a obtener pérdidas millonarias y sufrir graves perjuicios tanto a nivel económico como a nivel social.

3.5.2 Herramientas TIC más utilizadas en empresas

Tabla 6. Herramientas TIC más usadas en la organizaciónes[19]

Herramientas	Funciones

[18] **X CONAI,** Auditando los procesos de detección y respuesta a incidentes, sobre la identificación de vectores de ataques más críticos en la organización p.20.
[19] **PLINK,** 10 herramientas TIC para empresas.

Redes sociales: Instagram, Facebook, WhatsApp business	Se potencia las ventas de los negocios, las relaciones con los clientes, y proveedores.
Dropbox	Se requiere enviar, documentos, archivos, fotos, o videos, y almacenar información.
Trello	Es un tablero para gestionar tareas, desde las más sencilla hasta grandes proyectos.
Suite de Google	Es una plataforma completa que integra correos electrónico corporativos, almacenamiento de archivos en línea, reuniones virtuales, hoja de cálculo, etc.
Google Analytics	Es utilizada para monitorear el estado de un sitio web.
Hootsuite	Se utiliza para gestionar redes sociales, permite programar y monitorear las publicaciones de cualquiera de las cuentas empresariales.
Slack	Facilita la comunicación entre compañeros de trabajo.
CRM de Hubspot	Facilita realizar la gestión de relaciones con el cliente en cuanto a ventas, marketing.
Wordpress, wix **Plink**	Se ofrece todo para diseñar un sitio web Plataforma que utiliza para entregar datos detallados sobre el perfil de los clientes.

Fuente: "https://vendemas.plink.com.co/herramientas-tic-mas-usadas"

3.5.3 Acciones para mejorar la seguridad informática [20]

Generalizar la autenticación de doble factor. La autenticación de doble factor es una tecnología que verifica dos veces la identidad digital para aumentar la seguridad

[20] **FUNDACIONBANKINTER,** 10 propuestas para mejorar la Seguridad Informática en Colombia.

informática. Es recomendable su implantación para la industria financiera y los pagos digitales.

- ✓ Se debe empezar a implementar las Políticas de seguridad en las empresas

Educar a los ciudadanos en ciberseguridad básica. Podrían organizarse campañas de **concienciación** global para que los ciudadanos estén informados al tanto de las nuevas modalidades. Del uso de las nuevas tecnologías que se tiene en cuenta, así como.

- ✓ Educar – en su uso es el arma principal
- ✓ Ordenador o celular – siempre en zona comunes de la casa
- ✓ Control parental – usar herramientas de control parental
- ✓ Redes sociales – configurar la privacidad
- ✓ Privacidad – no dar datos personales a desconocidos
- ✓ Webcam – si no se usa siempre tapada, o suspendida
- ✓ Chats – no se sabe quién hay realmente al otro lado, solo con amigos
- ✓ Videojuegos – adquirirlo en función de la edad.

Concienciar al consumidor digital en seguridad. Debería existir una 'ciber' entidad para educar a los ciudadanos a tomar precauciones frente a ciertas prácticas de riesgo.com el **Phishing, vishing.**

- ✓ No responda ni de clic a enlaces que reciba de remitentes desconocidos; primero asegúrese de que se trata de una fuente confiable.

- ✓ Cambie sus contraseñas de forma regular, evite usar la misma en todas las cuentas que tenga, así como datos evidentes como su nombre, teléfono o fecha de nacimiento.

3.6 MARCO CONCEPTUAL

AMENAZAS DIRIGIDAS: Son los que se enfocan hacia un objetivo, intentar lograr algo o específicamente a un usuario en particular.

AMENAZAS REALES: son los peligros potenciales de que ocurra algún evento adverso que pueda afectar la prestación de un servicio dentro de la empresa,

valiéndose de los activo o recursos informático. Sin previo conocimiento para ser instalado o ejecutado cualquier tipo de programas maliciosos bien sea un malware o vectores de ataque.

ATAQUE DIRIGIDO: Es un proceso lento que viola la seguridad y permite al ciberdelincuentes evitar los procesos de autorización. Utiliza la ejecución de vulnerabilidades o debilidades en un sistema. Afecta la integridad, disponibilidad o confidencialidad de la información.

- ✓ **Autenticación:** Se refiere a que solo las personas autorizadas tienen acceso a los recursos.

- ✓ **Confidencialidad:** Se refiere a que la información solo debe ser comunicada a las personas, entidades o sistemas autorizados para su acceso.

- ✓ **Disponibilidad:** Se refiere a que la información sea accesible cuando la necesitemos teniendo en cuenta la privacidad.

- ✓ **Integridad:** Se refiere a que la información sea correcta, verificada, garantizada y libre de modificaciones y errores.

CAPACIDADES DE DEFENZAS: Comprobamos que el atacante pueda moverse libremente, permanecer en un largo periodo de tiempo escalando los privilegios corporativos o robando información sensible y estratégicas para el negocio, si algo le falta utilizamos todas las técnicas de ingeniera social que se pueda ocurrir.

CAPACIDADES DE RESPUESTAS: tratamos no solo de entrar sino de poner a pruebas los sistemas de detección y respuestas a incidentes de la organización, esperamos que nos detecte así comprobar los mecanismos que tiene la organización para detectar y dar respuesta a un incidente, se trata de aprender, prevenir, y saber gestionar situaciones de crisis.

CIBERATAQUES: Es un conjunto de Acciones ofensivas producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los sustentan.

INGENIERÍA SOCIAL: Obtención de información confidencial de una persona u organismo para utilizarla con fines maliciosos. Los ejemplos más llamativos son el **phishing** y el **spam**.

PILARES DE LA SEGURIDAD INFORMÁTICA: se articula en cuatro dimensiones que son la *disponibilidad, la integridad, la confidencialidad y la autenticación*, Rf. (Proteccion de la Informacion, p.7. [en Linea] Empresa incibe.: [Consulta: 26 Noviembre 2021])

SIMULACIÓN REAL: Es la necesidad de realizar una intrusión realista, se siguen en todo momento las mismas acciones que realiza el mismo atacante durante un ataque dirigido (APT), Amenaza Avanzada Persistente.

VECTOR DE ATAQUE: Es la ruta o camino que utiliza un atacante para tener acceso al activo objetivo de ataque. Su objetivo es apoderarse de los activos de información

3.7 MARCO HISTÓRICO

El ataque es el secreto de la defensa; la defensa es la planificación de un ataque. Esto lo decía el filósofo y militar chino **sun tzu** en su libro **El arte de las guerras.** El origen del concepto **Red Team** proviene del ámbito militar los, militares se dieron de cuenta que para defender mejor era necesario atacar sus propias defensas con el fin de encontrar sus puntos débiles, así conforme se fue pasando el tiempo se transformó una especie juego de querrá donde los defensores o las fuerza amigas denominaban el Blue Team. La fuerza opuesta o los atacantes eran el Red Team.

Este tipo de ejercicios se ha venido realizando de forma continuada desde hace décadas por los ejércitos desde hace muchísimos años, siempre se ha venido utilizando este mismo concepto. Y suponen uno de los entrenamientos más eficaces para conocer su estado de la seguridad, cuáles son sus puntos débiles y sobre todo sus capacidades defensivas y de reacción ante cualquier intrusión.

Como resultado de los atentados del 11 de septiembre en el año 2001, esta práctica de ataque de la defensa militar, se fue trasladando e intensificando a la comunidad de inteligencia tanto civil como militar, y al ámbito privado. Principalmente al sector de la seguridad de las grandes compañías, contratista del estado o del gobierno, mejor dicho, estadounidenses.

En la actualidad, equipos del Red Team, como el de la empresa de ciberseguridad InnoTec (del Grupo Entelgy), han adaptado estas tácticas militares a entornos de seguridad para dar un paso más en la defensa de los activos críticos de una organización. Se ha demostrado que las medidas tradicionales dirigidas a la protección de sistemas y equipos, el desarrollo de planes y políticas de seguridad o las auditorías que intentan verificar que las acciones realizadas son correctas. Ref. (G. Juanes, 2016).[21]

[21] **CUADERNOSDESEGURIDAD**, Red Team: Pensando como el enemigo, El Arte de la Guerra.

3.8 MARCO LEGAL

Tener ese súper poder de conocer todos los movimientos posibles de un ciberatacante y anticiparse a ellos. Nuestro servicio Red Team realiza intrusiones de ataques reales dirigidos por un equipo de especialista. Un grupo que **actúa como si fueran atacante.** Como lo hacen, realizan un acceso no autorizado a los sistemas corporativos, Utilizan todas las técnicas de ingenia social las que se nos puede ocurrir. Así podemos entrar, romper, restringir, suplantar, robar información.

Un **Hacker ético,** en ciberseguridad en Colombia, es aquel que sigue las reglas de aquellas leyes que lo rigen en su labor de trabajo, para no cometer ninguna pena o sanción según el caso, como lo establece la **ley 1273 del 2009 de los delitos informáticos**, **ley 842 de 2003, del código ético de COPNIA,** que tiene la función de controlar, inspeccionar y vigilar el ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares en general, en el territorio nacional. La **ISO/IEC 27001 y 27032,** normatividad para los estándares de Seguridad y Ciberseguridad.

Tabla 7. Ley 1273 del 2009.

Ley 1273 del 2009 - Articulo 269	
Intrusismo informático	**A -** Acceso abusivo a un sistema informático.
Espionaje informático	**C -** Interceptación de datos informáticos. **F -** Violación de datos personales. **G -** Suplantación de sitios web para capturar datos personales.
Sabotaje informático	**B -** Obstaculización ilegítima de sistema informático o red de telecomunicación. **D -** Daño Informático. **E -** Uso de software malicioso.
Defraudación informática	**H -** Circunstancias de agravación punitiva. **I -** Hurto por medios informáticos y semejantes. **J -** Transferencia no consentida de activos.

Fuente: ("https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf", "https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003")

4 DISEÑO METODOLÓGICO

Figura 10. Modelo general de detección y respuesta.

Fuente: Edición propia.

5 DESARROLLO DE LOS OBJETIVOS

5.1 OBJETIVO 1 - *Ataques e incidentes a los que se ven enfrentadas las organizaciones.*

Este objetivo, está orientado a conocer los problemas de **ciberseguridad**, causados por **ataques principales** e **incidentes, e impactos emergentes** a los que se ven enfrentadas las organizaciones, y que puede ser utilizadas para comprometer los activos o recursos de información hoy en día en Colombia. Para evitar ser sorprendido por un ataque cibernético es fundamental adquirir buenos hábitos de ciberseguridad, tanto con la **información personal** como con la **información corporativa**.

Se plantea 7 fases del ciclo de vida de un **modus operandi cibernético**, como un atacante llega apoderarse del sistema y de los activos de información en la organización. mediante técnicas y tácticas a través de vectores de ataques dirigidos, para llegarle a la víctima. En primer lugar, se tiene **el atacante, las pymes, y la víctima**.

Atacante: es una persona que está clasificada en diferentes perfiles como cibercriminales, ciberataque, cibernético, cibercrimen, ciberdelito, ciberespionaje, ciberdelincuencia y otros. Estos atacantes a nivel global cresen a un ritmo considerable cada vez con nuevas tendencias, utilizan nuevos métodos o modalidades a través de técnicas de ingeniería social, dándole la capacidad de materializar un ataque en cuestión de minutos. Para esto el atacante debe valerse principalmente de las vulnerabilidades existentes de las Pymes. Para esto Se tiene en cuenta **siete faces** de un modus operandi cibernético que son:

1. **Reconocimiento:** El ciberdelincuente recopila información sobre su objetivo. Mediante técnica por correo electrónico, y redes sociales.

2. **Preparación:** Se prepara el ataque de forma específica sobre un objetivo, se crea un correo electrónico que suplante la identidad.

3. **Entrega:** Se produce se envía el paquete armado a la víctima, por medio de un correo electrónico, es decir un phishing.

4. **Explotación:** Implica la detonación del ataque, Se ejecuta el código en el sistema del equipo y la red a la que pertenezca la víctima.

5. **Instalación:** El atacante instala el malware en la víctima. También puede darse de que no se requiera instalación, como en el robo de credenciales.

6. **Comando y control:** El atacante cuenta con el control del sistema de la víctima de forma remota.

7. **Acciones:** El atacante logra sus objetivos de forma remota. Y puede volver a ejecutar todas y cada una de sus fases e infectar a más víctimas.

Pymes: son las grande, mediana y pequeñas empresas. Donde se maneja todos los activos o datos de información financiera, empleados, clientes, proveedores etc. Y se divide en Entorno de la información personal. Entorno de la Información corporativa,

Víctima: Es quien recibe el fraude, estafa, hurto por aquellos cibercriminales, sin importar que sea cualquier usuario de la empresa, para un atacante la primera presa es su víctima. Por medio de víctima el atacante logra materializar las 7 faces cibernética. Por esta razón mantenerse al día y formar y concienciar a tus empleados y aprender a identificarlos, será la principal barrera o línea de defensa para frenar el ataque de esta fase. Así evitamos el número de impacto emergente en la productividad y daños reputacionales por la pérdida de sus activos financieros.

Muchos descuidamos el potencial valor del correo electrónico, sabemos que es una herramienta primordial más usada en las empresas al igual que el numero telefónico, los correos no fraudulentos llevan un certificado de seguridad como (https://), los correos fraudulentos vienen enlazados identificándose cualquier entidad, hay que revisar si la URL coincide con el sitio oficial, para verificar pulsamos un segundo sobre la URL y copiamos el enlace, luego lo verificamos en la plataforma virus total https://www.virustotal.com/gui/home/upload pegamos el enlace, esta web realizara un análisis y nos indicara si el enlace está libre de malware.

5.2 OBJETIVO 2 - *Metodologías, técnicas y tácticas utilizadas existentes por los equipos de seguridad RT y BT.*

En este objetivo se da inicio la identificación de las técnicas y metodologías para los ejercicios de los equipos de seguridad **Red Team y Blue Team**, en primera medida se evalúa el ámbito de actuación **digital, físico, y humano** de la empresa, para identificar el nivel de seguridad real, y exposición de la organización frente a un **ataque dirigido**. Una vez que se tenga el nivel de seguridad, se llevara a cabo la ejecución de las cuatro fases y pasos para la recolección de la información.

fase 1. Intrusión externa

- *Definición y planificación,* se define qué tipo de vectores serán utilizados y de qué manera serán atacados, de esta forma se hará uso de la inteligencia ofensiva.

- *Reconocimiento externo,* se desarrolla todas las acciones posibles para la identificación de vectores de acceso, y así identificar vulnerabilidades para hacer una intrusión.

- *Compromiso inicial,* se va a identificar una vulnerabilidad critica, que permita abrir paso a la intrusión, puede ser desde ataques de fuerza bruta, o pivotear a la red interna, con esto daríamos el primer acceso o activo de la empresa.

fase 2. Intrusión interna

- *Acceso a la red interna*, se debe buscar el camino y la forma para acceder a la red interna, cuando se compromete un primer activo, es decir el acceso privilegiado al sistema y visibilidad a la red interna.

- *Elevación de privilegios,* se busca crear vías de acceso segundarias en caso que el Blue Team detecte el ataque al vector principal y lo detenga, es decir la obtención de privilegios elevados en la infraestructura interna.

- *Reconocimiento interno,* se debe hacer un reconocimiento interno de todos los activos para evaluar cuáles podrían ser los ataques más radicales que se puedan hacer, es decir el acceso a activo críticos e información sensible.

fase 3. Prueba de ataque

Análisis de capacidades, aquí se emplean todas la técnicas y tácticas necesarias de ingeniería social, así comprobamos los mecanismos que tiene la organización detectar y dar respuesta a un incidente en la organización.

fase 4. Formación

Entrenamiento Blue Team, La primera línea de defensa en la organización, aquí se evalúa la capacidad real que tiene una organización para proteger sus activos críticos y sus capacidades de detección y respuesta frente amenaza. Gracias al equipo Red Team que se enfrenta al Blue Team para brindarle la seguridad y posibilidad de defenderse de forma controlada.

La ejecución de estas cuatro fases de la metodología, se centra en los **Objetivos, Alcance, Pruebas, y Beneficios.**

5.3 **OBJETIVO 3 - *Estrategia para el mejoramiento de ciberseguridad en la organizaciónes.***

Este objetivo, está orientado a establecer una estrategia para mejorar los niveles de seguridad en las organizaciones en Colombia, debido al mal uso que le dan los usuarios a las herramientas TIC. Teniendo en cuenta estas dos acciones de estar **concienciados,** y **educado** sería el punto clave para mejorar la **ciberseguridad**, el mejor mecanismo para frenar cualquier vector de ataque dirigido.

En primer lugar, la ciberseguridad está en relación con las herramientas TIC, nos ofrece un conjunto de herramientas interna para la empresa, a nivel global tenemos las herramientas TIC, estas nos permite utilizar para proteger los activos de una organización y se ocupa de analizar los riesgos y vulnerabilidades, que integra los entornos para determinar acciones que se van a implementar, unas de esas acciones son las **Políticas de seguridad,** esta es una buena estrategia que puede tomar la empresa para evitar ciertas prácticas de riesgo.

El principal problema al que vamos a enfrentar es como regular y a mejorar nuestra ciberseguridad de los vectores de ataques presentes, esto resulta un poco indispensable. Mas cuando se tiene que enfrentarse con la ciberdelincuencia, Ciberataques, Ciberguerras, Ciberespionaje, Cibercrimen, etc. Hoy en día con la

nueva Hera de la tecnología los dispositivos móviles han logrado un cambio drástico en la seguridad del mal uso y manejo de estos dispositivos en manos de los ciudadanos. Veamos las siguientes acciones.

- ✓ **Generalizar la autenticación de doble factor.** La autenticación de doble factor es una tecnología que verifica dos veces la identidad digital para aumentar la seguridad informática. Es recomendable su implantación para las organizaciones financiera y los pagos digitales. Para esto hay que empezar a implementar las Políticas de seguridad

- ✓ **Educar a los ciudadanos en ciberseguridad básica:** Se debe realizar campañas de concienciación global para que los ciudadanos estén informados de la nueva modalidad. Se debe educar a niños jóvenes, y adultos sobre el uso de las herramientas TIC.

- ✓ **Concienciar al consumidor digital en seguridad:** Se debe educar a los ciudadanos a tomar precauciones frente a ciertas prácticas de riesgo. Como el phishing, vhising.

6 CONCLUSIÓN

El presente trabajo se identificó los problemas de ciberseguridad causados por **ataques principales** e **incidentes,** e **impactos emergentes** a los que se ven enfrentadas las organizaciones hoy en día, como se ha visto nada es seguro cuando se navega en internet en primera instancia es proteger la información y la privacidad que ya es una responsabilidad de todos. A través de los equipos RT y BT se logra mantener esa seguridad y confianza con la sociedad y empresas. De acuerdo a la evaluación de técnicas, tácticas y metodologías que realizan estos equipos, se busca establecer estrategia que permita mejorar los niveles de seguridad y defensa en las organizaciones. Por medio de una simulación de un ataque dirigido o APT sobre una determinada organización, donde se Identifica vulnerabilidades en aquellos activos definidos, así logramos demostrar cual sería el nivel de riesgo e impacto que tendría un ataque dirigido sobre una organización, de esta forma se reforzara la seguridad y defensa con herramientas de contención y detención, teniendo en cuenta las cuatro fases de ejecución del diseño metodológicos.

7 RECOMENDACIONES

- ✓ Reforzar las políticas de seguridad en la empresa, para evitar cualquier impacto emergente que comprometa con los activos de información, que evidencian de vulnerabilidades, ataques e incidentes a los que se ven afrentadas las organizaciones hoy en día, para mejorar los niveles de riegos informático.

- ✓ Realizar pruebas de detección y respuesta con los equipos de seguridad RT y BT, para evaluar el nivel de seguridad de la empresa, por medio de la ejecución de faces metodológicas, para mantener la seguridad a la defensiva con informes detallados de las vulnerabilidades existentes en la organización.

- ✓ Implementar estrategias para el mejoramiento de ciberseguridad en las organizaciones, debido a la Transformación digital, al ciberespacio, o internet de las cosas que han cambiado constantemente, mediante acciones se permitirá regular la diversidad de ataques reales en Colombia.

BIBLIOGRAFÍA

ADRIANA C, L., LORENA M, G., & CARLOS A, Q. [Sitio web]. Bogota D.C, Tendencia Cibercrimen en Colombia 2019 - 2020, p.4. [Consulta: 26 Noviembre 2021]. Obtenido de: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

CAIVIRTUAL. [Sitio web]. Bogota D.C, Balance Cibercrimen 2020, P.2. [Consulta: 26 Noviembre 2021]. Obtenido de: : https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

CAIVIRTUAL. [Sitio web]. Bogota D.C, Reporte Centro Cibernetico Policial. [Consulta: 26 Noviembre 2021]. Obtenido de: https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico

CORPORATION, Z. (S.F.). [Sitio web]. La evolución de los Ciberataques - Empresa manageengine. [Consulta: 26 Noviembre 2021]. Obtenido de: https://www.manageengine.com/latam/log-management/infografia-evolucion-ciberataques.html

DATACREDITOEMPRESAS. [Sitio web]. Bogota D.C, Situación del Cibercrimen en Colombia primer trimestre del 2021. [Consulta: 26 Noviembre 2021]. Obtenido de: https://www.datacreditoempresas.com.co/blog-datacredito-empresas/situacion-del-cibercrimen-en-colombia-primer-trimestre-del-2021/

G. JUANES, G. [Sitio web]. Red Team Pensando como el enemigo. [Consulta: 26 Noviembre 2021]. Obtenido de https://cuadernosdeseguridad.com/2016/06/red-team-pensando-enemigo/

GB-ADVISOR. [Sitio web]. ¿Qué debemos hacer para librar nuestras redes de vectores de ataque en ciberseguridad? - Empresa Tech-Blog. [Consulta: 26 Noviembre 2021]. Obtenido de: https://www.gb-advisors.com/es/vectores-de-ataque-en-ciberseguridad/

HACKBYSECURITY. (S.F.). [Sitio web]. Ejercicio de Red Team - Empresa Hack by Securty. [Consulta: 26 Noviembre 2021]. Obtenido de: https://www.hackbysecurity.com/servicios-empresas/auditoria-informatica/ejercicio-de-red-team

INCIBE. (S.F.). [Sitio web]. Proteccion de la Informacion, p.7. - Empresa incibe. [Consulta: 26 Noviembre 2021]. Obtenido de: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

INTELEQUIA. [Sitio web]. Red Team y Blue Team - funciones y diferencias en ciberseguridad. [Consulta: 26 Noviembre 2021]. Obtenido de: https://intelequia.com/blog/post/2088/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

INTERNEXA. (S.F.). [Sitio web]. Las 5 herrsamientas mas poderosas en ciberseguridad de esteaño p.7. - Empresa ISA. [Consulta: 26 Noviembre 2021]. Obtenido de: https://www.internexa.com/wp-content/uploads/2020/03/Las-5-herramientas-ma%CC%81s-poderosas-en-ciberseguridad-de-este-an%CC%83o.pdf

J, J. (06 DE ABRIL DE 2020). [Sitio web]. Los ataques dirigidos son mucho más peligrosos y frecuentes. - Empresa Redes Zone.[Consulta: 26 Noviembre 2021]. Obtenido de https://www.redeszone.net/noticias/seguridad/gran-aumento-ataques-dirigidos/

MALWAREBYTES. (S.F.). [Sitio web]. ¿Que es el Cryptojacking?. - Enpresa Malwarebytes. [Consulta: 26 Noviembre 2021]. Obtenido de: https://es.malwarebytes.com/cryptojacking/

MARTÍN, J. [Sitio web]. Con las Tecnologías de Información en las - Empresas diarium. [Consulta: 26 Noviembre 2021]. Obtenido de: https://diarium.usal.es/i_jmartin/importancia-de-las-tic-en-las-empresas/

NUÑEZ, E. A. [Sitio web]. Technical Approach to Red Team Operations, p.11. congreso MoscowCON (Moscu). [Consulta: 26 Noviembre 2021]. Obtenido de: https://www.slideshare.net/eduan796/technical-approach-to-red-team-operations-moscow-c0n

PLINK. (S.F.). [Sitio web].10 herramientas TIC para empresas: cuáles son las más usadas y para qué sirven. - Empresa Plink - TIC. [Consulta: 26 Noviembre 2021]. Obtenido de: https://vendemas.plink.com.co/herramientas-tic-mas-usadas

RAMOS, A. (s.f.). [Sitio web]. Red Team, el hacking en otra dimension 0, p.40. [en Linea] Servicio CyberCamp incibe.: [Consulta: 26 Noviembre 2021]. Obtenido de https://cybercamp.es/sites/default/files/contenidos/videos/adjuntos/cybercamp2017-redteam_el_hacking_en_otra_dimension_alejandro_ramos.pdf

REDSEGURIDAD. [Sitio web]. ¿Qué es el cryptojacking y cómo evitar este ‘malware’ que mina criptomonedas? - Informacion Red Seguridad. [Consulta: 26 Noviembre 2021]. Obtenido de: https://www.redseguridad.com/actualidad/que-es-el-cryptojacking-y-como-evitar-este-malware-criptomonedas_20210421.html

SECURITY, I. (S.F.). [Sitio web]. Enfoques y aspectos Clave en ejercicios Red Team, p.3-9. [Consulta: 26 Noviembre 2021]. Obtenido de: https://www.ccn-cert.cni.es/pdf/documentos-publicos/xii-jornadas-stic-ccn-cert/3449-fp1-02-stic-aspectos-clave-red-team-innotec-eduardo-arriols/file.html