8-8-2022

Diseño de un equipo morado para el sector financiero colombiano enfocado en las Sociedades Comisionistas de Bolsa (SCB)

Jeimy J. Cano M.

Omar A. Hernández

Diseño de un equipo morado para el sector financiero colombiano enfocado en las Sociedades Comisionistas de Bolsa (SCB)

Artículo Completo

Jeimy J. Cano M.
Universidad de los Andes
jcano@uniandes.edu.co

Omar A. Hernández A.
Escuela Superior de Guerra
hernandezoa@esdegue.edu.co

Abstract

Currently, private and public sector companies are suffering cyber attacks globally, so the need to invest in cybersecurity has become a priority. In this sense, several supervisors have formulated regulations around cybersecurity, with a particular emphasis on banks and their challenges, but not much on the Stockbrokers (SBK) entities that are the subject of this research work. Although one of the most common methodologies is the simulation of offensive (red team) and defensive (blue team) security, purple teams are emerging as an alternative that enables a broader spectrum of learning and analysis for companies, particularly SBKs This article details a methodological guide for the design and implementation of a purple team in SBKs in order to strengthen cybersecurity governance in the face of contemporary cyber threats.

Keyword

Cybersecurity, purple team, red team, blue team, financial sector, stockbrokers.

Resumen

En la actualidad, las empresas del sector privado y público están sufriendo ataques cibernéticos a nivel global, por lo cual, la necesidad de invertir en ciberseguridad se ha convertido en un aspecto prioritario. En este sentido, varios supervisores han formulado regulaciones entorno a la seguridad cibernética, con un énfasis particular en los bancos y sus retos, pero poco sobre las Sociedades Comisionistas de Bolsa (SCB) entidades objeto de este trabajo de investigación. Si bien, una de las metodologías más frecuentes es la simulación de seguridad ofensiva (equipo rojo) y defensiva (equipo azul), los equipos morados se abren paso como una alternativa que habilita un mayor espectro de aprendizaje y análisis para las empresas particularmente las SCB. Este artículo detalla una guía metodológica para diseño y puesta en operación de un equipo morado en las SCB con el fin de fortalecer el gobierno de ciberseguridad frente a las amenazas cibernéticas contemporáneas.

Palabras Clave

Ciberseguridad, equipo morado, equipo rojo, equipo azul, sector financiero, comisionistas de bolsa.

Introducción

Hace algunos años, internet no estaba disponible y la conexión entre las personas era escasa. Los riesgos por inseguridad en internet no eran comunes en ese entonces, pero hoy en día, a medida que la tecnología ha evolucionado, el panorama de amenazas crece y cambia constantemente. Situaciones asociadas como robo de contraseñas, delitos informáticos, grupos cibercriminales, fallos en los sistemas de información, entre otras, generan desconfianza en el usuario e inestabilidad en los mercados.

Resultado de lo anterior, las instituciones financieras tienen el desafío de evolucionar en sus capacidades de defensa para mantenerse al día en la forma de enfrentar estos ataques y en el mejor de los casos, anticiparlos. A pesar de contar con controles, herramientas y personas entrenadas, no resulta suficiente para hacer frente a las modernas amenazas cibernéticas, razón por la cual, este estudio busca incorporar una metodología distinta para fortalecer la gestión de la ciberseguridad en las Sociedades Comisionistas de Bolsa (SCB), que hacen parte del mercado de valores y, por ende, del sector financiero.

Así las cosas, la propuesta de este trabajo es establecer un marco de implementación de un equipo morado, es decir, un equipo multidisciplinario con capacidades técnicas y tácticas, conocimientos en herramientas y gestión de riesgos cibernéticos, que permita preparar a las Sociedades Comisionistas de Bolsa para enfrentar ataques de grupos avanzados de amenazas persistentes (APT, por sus siglas en inglés) y así superar los retos propios de los equipos ofensivos (equipos rojos) y defensivos (equipos azules) que se usan en la actualidad.

Para desarrollar lo previsto en este artículo, se presenta inicialmente la problemática que enfrentan las instituciones del sector financiero para el aseguramiento de sus activos de información y el valor que representa, lo que conduce a la generación de la pregunta de investigación, el alcance y las limitaciones propias de este estudio. Luego, se detalla el marco teórico, abordando los estudios realizados alrededor de los equipos morados, rojos y azules, así como las diferentes normativas que aplican a las instituciones del sector financiero.

Seguidamente, se introduce la propuesta del marco de trabajo para el diseño e implementación del equipo morado a partir de las revisiones previas realizadas, los mecanismos de integración que se conforman a partir de los roles y responsabilidades, procesos y herramientas, y finalmente, las relaciones y operación que integrará la propuesta, la cual se detallará en un caso de estudio

Finalmente, se presentan las conclusiones de la investigación realizada, las contribuciones al área de estudio y a la práctica y las limitaciones que se presentaron en el desarrollo del proyecto.

Marco Teórico

La revisión de literatura se adelantó a través de la consulta y análisis de diferentes fuentes académicas y de industria alrededor del tema central de este trabajo, con el fin de dar forma al marco teórico, y de esta manera responder a la pregunta de investigación: ¿cuáles son las características del equipo morado para el sector financiero (Sociedades Comisionistas de Bolsa, SCB) de acuerdo con las tácticas, técnicas y procedimientos de los APT (motivados solo al sector financiero), según MITRE ATT&CK, y los controles de NIST Cybersecurity Framework?

Para ello, se explora el concepto del ciberespacio de manera general, para posteriormente explicar la ciberseguridad desde la definición NIST (traducido como Instituto Nacional de Estándares y Tecnología) (2018), y luego particularizar las amenazas o problemáticas en ciberseguridad y ciberdefensa. En línea con lo anterior, se definen diferentes métodos de evaluación para las organizaciones, como: i) pruebas, ii) exámenes y iii) entrevistas, describiendo cada una de estas, para llegar a las definiciones de las pruebas o simulaciones de los equipos rojos y azules.

Se define cada uno de los equipos previamente mencionados desde diferentes perspectivas, a partir de las metodologías, tareas y el recurso humano que utilizan. Considerando lo anterior, se realiza la caracterización de los equipos morados, objeto central de este trabajo, para aplicarla en las SCB, incorporando las normas y documentos de la Superintendencia Financiera de Colombia. Finalmente, se identifican las tácticas, técnicas y procedimientos de los grupos de amenazas persistentes (por sus siglas en inglés, APT) enfocados al sector financiero descritos en MITRE, y a su vez, los controles específicos para mitigarlos bajo el estándar NIST Framework Cibersecurity (NIST, 2018).

Equipos rojos, azules y morados

El acercamiento del equipo rojo y azul se establece como una forma de interacción, en la que al menos una de las partes finge ser el enemigo. Esta idea ha sido adoptada en el campo de la ciberseguridad para realizar pruebas a partir de una mentalidad hostil mediante la replicación de amenazas, y desarrollando contramedidas basadas en los resultados obtenidos (Drinkwater y Zurkus, 2017).

Equipo Rojo: Según las investigaciones realizadas por Cajaraville y García (2016), el equipo rojo se define como:

> El *Red Team* (equipo rojo) consiste, por tanto, en un servicio altamente especializado y llevado a cabo sobre todos los ámbitos posibles, realizando comprobaciones físicas, electrónicas y sobre las personas de la organización. De esta forma, las corporaciones pueden optar por una actitud proactiva a la hora de asegurar sus recursos más valiosos (pp. 30-33).

Equipo Azul: Se describe al equipo azul, como el contrincante o contraparte del equipo rojo, que debe asegurarse de que los activos de información estén asegurados y en caso de una vulnerabilidad encontrada por el equipo rojo, sea remediada lo antes posible y luego documentada como parte de las lecciones aprendidas (Diogenes y Ozkaya, 2018). En otra investigación publicada por UNIR (UNIR, s. f.), se describe este equipo de la siguiente forma:

> Realiza evaluaciones de las distintas amenazas que puedan afectar a las organizaciones, monitoriza (red, sistemas, etc.) y recomienda planes de actuación para mitigar los riesgos. Además, en casos de incidentes, realizan las tareas de respuesta, incluyendo análisis de forense de las máquinas afectadas, trazabilidad de los vectores de ataque, propuesta de soluciones y establecimiento de medidas de detección para futuros casos (párr. 11).

La rivalidad y el secretismo entre los equipos puede afectar las capacidades de seguridad de una organización. Esta hostilidad puede afectar la credibilidad de las evaluaciones, aumentando el riesgo de ciberseguridad. Debido a las limitaciones propias de estos ejercicios, es necesario tomar distancia de los tipos tradicionales de evaluaciones de seguridad (Miessler, 2020). La necesidad de un enfoque dinámico con una relación simbiótica entre los equipos, condujo al concepto de un equipo morado.

Equipos morados: Los equipos morados analizan los principios de seguridad con base en equipos rojos y azules, lo que les da una perspectiva diferente para evaluar la seguridad de una organización (SecureAuth, 2021). Cuando ambos equipos trabajan de manera aislada, los equipos morados podrán adoptar la estrategia de caja blanca para las pruebas, donde obtienen información de cada equipo. De acuerdo con el modelo simulado que los equipos rojos utilizan, los equipos morados también pueden realizar pruebas de penetración con un conocimiento profundo de los activos de los equipos azules, con el fin de evaluar la seguridad desde una perspectiva diferente (Peters, 2016).

La idea de un equipo que combine los principios de los equipos rojo y azul acorta la distancia entre los enfoques ofensivo y defensivo, y se centra en metodologías de pruebas colaborativas. Algunos tipos de actividad realizados por equipos morados se presentan en la Tabla 1.

Tipos	Descripción
Conciencia recíproca	Consiste en que el equipo azul y rojo mantengan el mismo nivel de conocimiento en todas sus capacidades y no se reserven nada en el momento del ejercicio. Es decir, cada equipo conoce los objetivos del otro, proporcionando la información en el momento de la simulación.
Anfitrión involuntario	En este caso, el equipo azul tiene muy poca información de las acciones que realizará el equipo rojo, por lo cual debe concentrar esfuerzos en fortalecer las capacidades de búsqueda, detección o prevención en contra de las acciones que se materialicen.
Atacante involuntario	Aunque es el menos utilizado, el equipo rojo sabe muy poco de las capacidades o actividades del equipo azul, es decir, en todo momento se monitorea el escenario por el equipo azul. Al final se genera un reporte reflexivo de las acciones tomadas por el equipo rojo y cuáles fueron las implicaciones.
Pruebas de mano roja	Abarca el concepto de ser sorprendido con las manos en la masa, es decir, en plena acción, por lo que la prueba consiste en que el equipo rojo sea sorprendido por el equipo azul a partir de las acciones que realiza en la prueba.

Tipos	Descripción
Atrapar y soltar	Es diseñado para poner a prueba la resistencia de las acciones del equipo rojo, así como la identificación y rastreo del equipo azul. Cuando este es atrapado, recibe una información que le informa que ha sido detectado, lo que conlleva a reaccionar en un breve periodo de tiempo antes de que el equipo azul lo saque de la red.
Hacker útil	Esta actividad es la menos conflictiva y fácil de implementar, ya que se realiza después de una evaluación de seguridad ofensiva, al momento de reparar y mitigar los hallazgos presentados. Lo anterior tendrá como propósito mejorar y solucionar los hallazgos encontrados, para así priorizarlos y abordarlos de manera eficaz.

Tabla 1. Tipos de actividad del equipo morado (Basado en: Oakley, 2019)

Sociedades Comisionistas de Bolsa: De acuerdo con la definición establecida en la página web de la Bolsa de Valores de Colombia (BVC), las SCB son sociedades anónimas que tiene como objeto exclusivo el contrato de comisión para la compra y venta de acciones en la Bolsa. Así mismo, se pueden clasificar en bancarizadas, si su dueño es un banco, y tradicionales, si el dueño son personas naturales o un grupo familiar. Es así como los profesionales de estas entidades deben contar con conocimientos especializados en el mercado, que realizan en nombre de sus clientes para las negociaciones de los títulos. Este servicio que se ofrece, se denomina "contrato de comisión".

Es importante destacar que las sociedades están bajo el control y vigilancia de la Superintendencia Financiera de Colombia (SFC) y el Autorregulador del Mercado de Valores (AMV). Adicionalmente, todas las comisionistas son miembros de la BVC y las resguardan principios generales formulados en el Código de Conducta de las Sociedades Comisionistas miembros de la BVC (Bolsa de Valores de Colombia, s. f.).

Luego de caracterizar, las Sociedades Comisionistas de Bolsa (SCB), objeto de la propuesta para la integración de un equipo morado, se hace necesario indagar ahora en los conceptos de las tácticas, técnicas y procedimientos que describe MITRE y los controles del estándar de ciberseguridad NIST (NIST, 2018), para completar la incorporación de estos equipos en dichas sociedades y su forma de operar.

MITRE ATT&CK: Los grupos avanzados de amenazas persistentes., por sus siglas en ingles APT (*Advanced Persistent Threat*), son grupos organizados, causantes de los ataques cibernéticos a ciertas industrias de un país con distintas motivaciones. Este marco es ampliamente utilizado en la industria de la seguridad y las organizaciones pueden utilizarlo para simular equipos rojos basados en los datos de este marco (Strom, 2018). Algunos de estos grupos tienen como motivación vulnerar el sector financiero, que se considera como infraestructura crítica. Según MITRE ATT&CK (s. f.), se han identificado las tácticas, técnicas y procedimientos (TTP) en los siguientes términos: "La base de conocimientos de ATT & CK se utiliza como base para el desarrollo de metodologías y modelos de amenazas específicos en el sector privado, en el gobierno y en la comunidad de productos y servicios de ciberseguridad" (párr. 1).

Adicionalmente, con la ayuda de la herramienta del MITRE, se seleccionaron los grupos de amenazas, consolidando las tácticas, técnicas y procedimientos que tienen en común. En la siguiente sección se retomarán estas características ofensivas como insumo para la propuesta del equipo morado. En cuanto a las características defensivas, los controles NIST serán explicados a continuación, con el motivo de que este último concepto abarque las bases necesarias para poder construir la propuesta de este trabajo.

NIST Cybersecurity Framework: De acuerdo con la normativa de NIST Cybersecurity Framework, este se define como un conjunto de normativas que deben seguir las empresas, organizaciones o entidades del sector privado para estar mejor preparadas al momento de identificar, detectar, proteger, responder y recuperarse de ataques cibernéticos. En resumen, es un conjunto de las mejores prácticas, estándares y recomendaciones que ayudan a una organización a mejorar sus medidas de ciberseguridad (NIST, 2018). Los controles NIST serán parte fundamental para la integración del equipo morado a las SCB, desde el enfoque defensivo.

A continuación, se presenta la propuesta del marco de trabajo para el diseño e implementación del equipo morado a partir de los fundamentos establecidos en las conceptualizaciones previas. Se detallan los mecanismos de integración previstos para las SCB, que incluyen los roles y las responsabilidades, así como los procesos y las herramientas requeridas, y finalmente las relaciones y las operaciones que hacen parte del modelo.

Propuesta

***Fundamentos de la propuesta*:** Se inicia por la ubicación organizacional del equipo morado al interior de la sociedad comisionista. En principio, es bueno centrarse en la regulación que actualmente existe en la Superintendencia Financiera de Colombia. De acuerdo con la Circular básica jurídica C.E.029 de 2014 Circular Básica Jurídica 029 de 2014 (Superintendencia Financiera de Colombia, 2014), en la Parte III, Título III, Capítulo I, "Disposiciones especiales aplicables a las operaciones de las Sociedades Comisionistas de Bolsa de Valores", el numeral 4, titulado "Operaciones de intermediación de bajo monto en el mercado de valores".

Por lo tanto, la Superintendencia también estableció en la misma circular antes mencionada, en la Parte I, Título I, Capítulo III, "Gobierno Corporativo", en el numeral 2, cómo debe ser la estructura organizacional de los intermediarios de valores, y menciona lo siguiente: "En el diseño y adopción de las políticas y procedimientos aplicables a sus organizaciones, los intermediarios de valores deben establecer como mínimo las siguientes funciones a cargo de los órganos de dirección, administración y demás áreas de la entidad" (p. 4). Lo anterior, involucra a la Junta Directiva, el representante legal y los órganos de control. Sin embargo, no está escrito cómo las sociedades comisionistas deben diseñar una estructura organizacional en los niveles inferiores, es decir, las direcciones o áreas de gran responsabilidad, para llevarlas a cabo.

Adicionalmente, la Superintendencia expidió la Circular Externa 007 de 2018, que tiene como obligación general contar con políticas, procedimientos y recursos técnicos y humanos necesarios para gestionar efectivamente el riesgo de ciberseguridad, basándose fundamentalmente en el estándar de NIST (2018) y, 2018) y fuentes de información confiables enfocadas al sector financiero. En el numeral 3.2, la Circular menciona que las entidades deben crear una unidad de seguridad de la información y ciberseguridad.

***Elementos de la propuesta*:** Se caracteriza el equipo morado teniendo en cuentas los roles y responsabilidades particulares. Cabe destacar que dentro de las referencias consultadas se encuentra muy poca información al respecto, pues se especifican más los equipos rojos y azules. Es por esta razón que se proponen cinco roles específicos para la propuesta del equipo morado, y para los casos en que las entidades no cuenten con el personal requerido, estos deberán ser respaldados por personal contratado con un tercero, para completar el equipo de cinco miembros. A continuación, se muestra en la figura cómo estaría conformado el equipo, sus características, funciones generales, estudios y certificaciones:

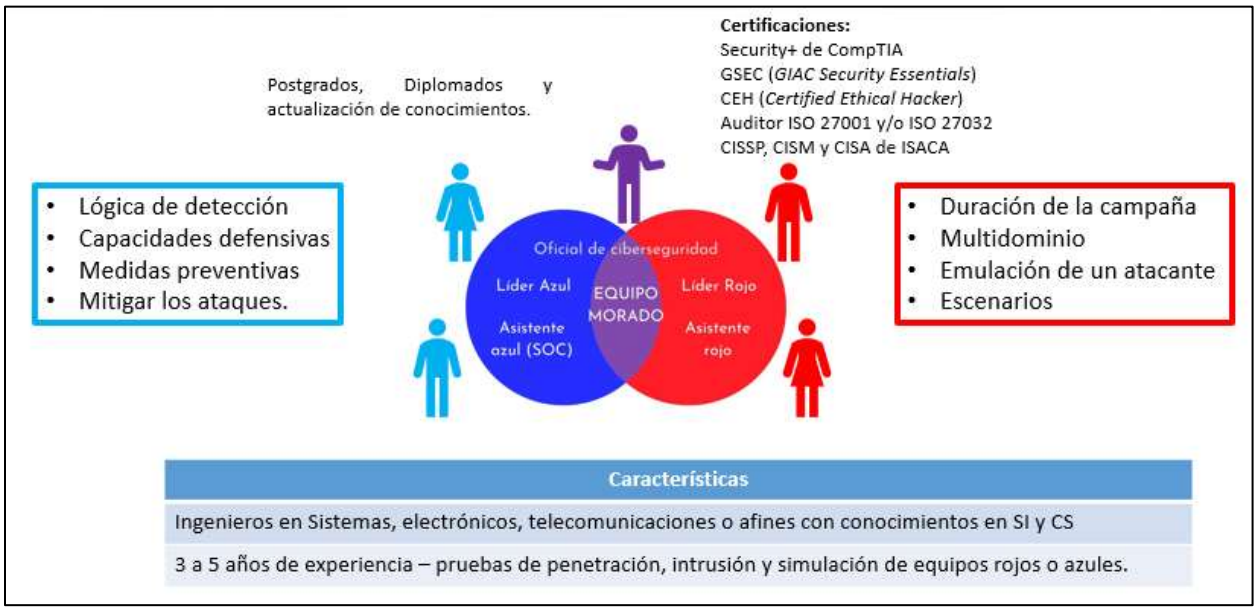

Figura 1. Elementos de la propuesta: Roles y responsabilidades del equipo morado propuesto

***Relaciones de la propuesta*:** Se realizó un derecho de petición[1] a la Superintendencia Financiera de Colombia, donde se preguntó el promedio de personas que trabajan en el área de ciberseguridad, a lo cual la entidad respondió que es de ocho, las cuales fueron discriminadas así: un promedio de tres personas en comisionistas tradicionales y trece para las comisionistas bancarizadas, aclarando que el personal también presta sus servicios a las otras entidades de los grupos financieros a los cuales pertenecen.

En el área de ciberseguridad es donde se pretende incluir los roles del equipo morado, conformada por el oficial de ciberseguridad y los analistas de ciberseguridad, que serán parte fundamental de la caracterización de la propuesta, adicionando las funciones al personal que se encuentra laborando en esta área.

Es de aclarar que esta es la única área que podría integrarse, ya que cumple con las funciones establecidas y los roles correspondientes, o de lo contrario tendría conflictos de interés, en el caso de integrarla en el área del riesgo operativo, donde a la fecha se evalúan los riesgos tecnológicos o cibernéticos.

Adicionalmente, algunas entidades han creado los comités de seguridad de la información o ciberseguridad para escalar los reportes e informes respectivos en caso de que se requiera tomar alguna acción, y asignar presupuesto o metodología propia del área.

Operación de la propuesta:

Para desarrollar la propuesta, es importante tener en cuenta las respuestas a las siguientes preguntas: ¿qué quiero fortalecer, la ofensiva o defensiva?, ¿cuánto tiempo debo dedicar a las pruebas?, ¿límites máximos o plazo establecido?, ¿qué herramienta es la más propia para realizar la simulación?, ¿qué equipos o activos de información debo tener en cuenta?, ¿cuál es el presupuesto asignado y el que será ejecutado?, ¿qué conocimientos tienen los miembros de los equipos?, las cuales establecen el alcance y foco del ejercicio a realizar con el equipo morado, los escenarios dispuestos para efectuar las simulaciones y sobremanera las acciones estratégicas a desarrollar defensa activa, pasiva y colaborativa, además de contar con la identificación de los actores claves, los activos y los procedimientos de preparación esenciales.

[1] Número de trámite 2021256013, según petición realizada a la SFC.

En el siguiente diagrama de flujo se detallan las fases que debe realizar el equipo morado (Figura 2) para desarrollar sus operaciones en el contexto de una SCB.

Figura 2. Diagrama de flujo o proceso para realizar las pruebas de seguridad por parte del equipo morado

Metodología

Considerando que el alcance inicial del trabajo fue la diseñar la propuesta, el ejercicio metodológico que se detalla a continuación se basa en un caso de estudio hipotético (por la sensibilidad del sector) para entender, interiorizar y aplicar la propuesta, siguiendo el paso a paso de cada una de las fases definidas previamente. Para ello, el caso de estudio se presenta desde la perspectiva del oficial de ciberseguridad, que deberá implementar el equipo morado por primera vez para realizar dicha prueba.

La comisionista de bolsa X es una de las más importantes en el sector valores en Colombia, ya que cuenta con una gran cantidad de clientes que ha invertido en acciones o títulos valores a través de los *traders*, personal idóneo o asesor que actúa como intermediario, en el mercado de valores. Así mismo, las líneas de negocio con las que cuenta la entidad, le han permitido posicionarse en otros segmentos del mercado, convirtiéndose en un objetivo muy apetecido por los APT o grupos de ciberdelincuentes, que intentan robar la información, deteriorar la imagen reputacional de la entidad e incluso adquirir recursos monetarios en el mercado de valores de manera fraudulenta.

A pesar de que la entidad invirtió en diferentes estrategias de seguridad de la información y ciberseguridad, como lo son: i) las capacitaciones realizadas a todo el personal, pero en especial al equipo de ciberseguridad; ii) en activos de seguridad avanzados; iii) en aplicación de controles de seguridad como parches y parámetros de seguridad de los usuarios finales, entre otras mejoras, se observa que se han presentado intentos de ciberataques por parte de APT identificados por el SOC (*Security Operation Center*) de la entidad y apoyados por entidades externas, por lo cual la SCB ha tomado la decisión de realizar pruebas o simulaciones a partir de la incorporación de un equipo morado. Seguidamente, la tarea es informada al oficial de ciberseguridad, el cual tendrá como responsabilidad realizar dicha prueba, con

el apoyo de cuatro profesionales que serán divididos entre el equipo rojo y azul, con cada uno de los roles correspondientes y contando con una herramienta para simular los ataques.

A partir de lo anterior, el oficial de ciberseguridad toma el liderazgo del equipo morado, y cuenta con los profesionales idóneos para tomar los roles correspondientes a: líder azul, asistente azul SOC, líder y asistente rojo, es decir, la estructura del recurso humano estaría establecida bajo las responsabilidades en el rol correspondiente, teniendo en cuenta que todos conocen la misma infraestructura y su nivel de conocimientos es el mismo. Es de recordar que, en caso de no contar con un profesional, la entidad deberá apoyarse con un tercero que lo pueda respaldar bajo los acuerdos de confidencialidad, si aplica.

A continuación se detalla el paso a paso del proceso de la Figura 2, a través de las siguientes fases establecidas.

Inicio:

Planificación del ejercicio: el oficial de ciberseguridad debe tener plena claridad sobre las políticas de seguridad de la información y ciberseguridad, el diagrama de red de la entidad y los recursos humanos y tecnológicos con los que cuenta. En primera instancia, las políticas permiten mantener las condiciones actuales con las que cuenta la entidad en temas relacionados con la operación y normativa, sujetos a propender por las mejores prácticas para mantener la seguridad sobre sus activos de información.

Tiempos de ejecución: la prueba se realizará en un mes, para poder realizar diferentes actividades del equipo morado, a lo largo del tiempo laboral y poner a disposición diferentes estrategias que permitan corroborar las debilidades de la entidad.

Restricciones: acceso al servidor que contiene las bases de datos de los clientes de la comisionista por medio de los sistemas de información misionales, los cuales, por política de ciberseguridad, se han identificado como sensibles o joyas de la corona (activos de información críticos). La primera simulación del equipo morado deberá contar con precauciones que permitan identificar solo las vulnerabilidades asociadas a los demás activos de información de la empresa, así como los servidores de aplicaciones o sistemas de información, herramientas, o cualquier otro objeto de riesgo cibernético.

Presupuesto: De acuerdo con los recursos anuales que cuente la entidad, tendrá la posibilidad de invertir en dichas pruebas específicas, bajo el objetivo que se quiere alcanzar.

Escoger APT: Para este caso, será simulado uno de los APT identificados, pero como es el primer ejercicio por parte del equipo de ciberseguridad, se requiere un APT que cuente con un promedio adecuado de técnicas para poder entender la mecánica del grupo morado, por lo cual se opta por la APT FIN4, que cuenta con 12 técnicas identificadas.

Escoger las técnicas: en la anterior fase se optó por el APT FIN 4, de modo que el número de técnicas totales es de 12 técnicas, por lo cual, la entidad puede tomar como base este número y revisar las que más se ajusten para este proceso.

Escoger el tipo de equipo morado: en esta fase se debe elegir uno de los seis tipos de equipos morados que se mencionan en la Tabla 1. Dado el caso, la mejor opción es el tipo: conciencia recíproca, es decir, que los integrantes cuentan con los mismos conocimientos acerca de los activos de información, ya que los profesionales conocen toda la infraestructura tecnológica y así mismo, lo correspondiente a los activos de información. Para ello, se quiere fortalecer la ofensiva y defensiva como primer ejercicio, y revisar fortalezas y debilidades por parte de la entidad.

Escoger rojo y azul: como ya fue mencionado en la estructura del recurso humano, se cuenta con cuatro profesionales para realizar la simulación, por lo cual, cada uno de los equipos debe contar con metodologías que les permitan realizar su correspondiente acción.

Simulación: para este caso, será utilizado un aplicativo gratuito denominado CRIXO, para poder evidenciar la prueba llevada a cabo.

Resultados: La fase final consiste en documentar en un matriz los resultados obtenidos que se han planteado, por lo cual, la matriz registrada quedaría como se observa en la Figura 3.

PLANTILLA				
Autor	Omar Augusto Hernandez			
APT	FIN 4			
Fecha de Inicio	1 de diciembre de 2021			
Tiempo de preparación	1 mes			
Tipo Equipo morado	Conciencia Reciproca			
Herramienta Utilizada	CRIXO			
Caso de estudio (Breve descripcion)	**MITRE ATT&CK Tacticas**	**MITRE ATT&CK Técnicas**	**¿Cómo fue detectado? (Debilidades, Vulnerabilidades o ataques asociadas)**	**Controles NIST aplicados**
Simulación del APT - FIN4	Acceso inicial	T1078 Valid Accounts (Validación de cuentas)	Microsoft Windows SMB Guessable User Credentials	PR.AC-1: Identificar y credencial son permitidas, gestionadas, verificadas, revueltas y auditadas para los dispositivos, usuarios y procesos autorizados.
		T1190 Exploit Public-Facing Application	SMB Signing Required	PR.AT-2: Los privilegios son usados de acuerdo a los roles y responsabilidades.
		T1566 Phishing	SSL RC4 Cipher Suites Supported	DE.AE-2: Los eventos detectados son analizados para entender los objetivos y metodos del ataque.
	Ejecución	T1059 Command and Scripting Interpreter	Microsoft Windows SMB Shares Unprivileged Access	PR.AC-4: Permisos de acceso y autorizaciones son administrados, incorporando los principios del menimo privilegio y separacion de deberes.
		T1204 User Execution	Unencrypted Telnet Server	PR.AC-3: Acceso remoto es administrado.
	Evasión de la defensa	T1564 Hidden Artifacts	SSL Self-Signed Certificate	DE.CM-7: Mejorar el monitoreo sobre la no autorizacion del personal, conexiones, dispositivos y software.
	Acceso con credenciales	T1056 Input Capture	Anonymous FTP Enabled SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	PR.PT-5: Los mecanismos son implementados para documentar los requisitos de resiliencia en situaciones normales y adversas.
	Recaudación	T1114 email collection	SSL Certificate Cannot Be Trusted	DE.CM-8: Escanear las vulnerabilidades son mejoradas.
	Mando y control	T1090 Proxy	SNMP Agent Default Community Name (public)	PR.PT-4: Las redes de comunicaciones y control son protegidas.
		T1071 Application Layer Protocol	Multiple Web Server Encoded Space (%20) Request ASP Source Disclosure	DE.CM-1: La red es monitoreado para detectar los potenciales eventos de ciberseguridad.

Figura 3. Plantilla de aplicación de la propuesta

Es de mencionar que los controles asociados para poder mitigar las vulnerabilidades encontradas se toman a partir del estándar internacional NIST de Ciberseguridad (NIST, 2018), y son parte fundamental para que el equipo azul pueda gestionar las vulnerabilidades, según la clasificación dada.

El marco de controles del NIST (NIST, 2018) se toma como referente de controles habida cuenta que en las regulaciones propias del supervisor del sector financiero colombiano, particularmente la Circular Externa 007 de 2018, sugiere la implementación de este marco de trabajo como base para el desarrollo de las actividades en los temas de ciberseguridad en el sector. Sin perjuicio de lo anterior, las SCB podrán apalancarse en otras buenas prácticas y extender su uso en la dinámica de sus operaciones para darle mayor profundidad a los resultados de las simulaciones realizadas por la implementación de los equipos morados.

Conclusión

En la medida en que el mundo se vuelve más complejo y se requiere estar en constante continuidad y mejoramiento de las prácticas actuales de ciberseguridad, la propuesta de crear los equipos morados en las evaluaciones de ciberseguridad es fundamental para fortalecer los temas asociados con la gestión de los incidentes y vulnerabilidades, y así validar la ofensiva y defensiva de las empresas, en especial de las comisionistas de bolsa.

Por tanto, concretar una cultura en la cual se interiorice que las pruebas o metodologías utilizadas por el equipo morado son beneficiosas para la empresa, en la medida que se pueden aprovechar como programas de evaluación cíclica, el trabajo en conjunto entre los equipos rojos y azules se puede potenciar aumentando las capacidades de los profesionales que participan, así como la conciencia situacional del entorno cibernético (Oakley, 2019) en la SCB.

En línea con lo anterior, el proceso de planeación y ejecución de las evaluaciones del equipo morado, y el apoyo de los roles y responsabilidades de cada uno de los integrantes que lo conforman, debe conocerse, controlarse e implementarse de forma periódica. Estos equipos deben asegurar que las pruebas ser realicen de manera conjunta, definiendo previamente las funciones de cada uno de los roles en los que participan, las habilidades con las que se cuentan y la metodología a utilizar, que deberá ser bien definida, de acuerdo al proceso propuesto y acorde a las necesidades de la empresa.

Con este estudio se busca contribuir a la academia desde el ámbito de ciberseguridad, las buenas prácticas y la metodología planteada, al ser el equipo morado otra de las opciones que pueden utilizar las entidades, con el fin de superar las rivalidades de los equipos rojos y azul, capitalizando el esfuerzo y los resultados del ejercicio.

Así mismo, se da relevancia al sector bursátil y el mercado de valores, al otorgarle participación dentro del sector financiero, con énfasisi en el área específica de la seguridad de la información, tomando en cuenta la importancia sistémica de la realización de las operaciones de acciones y títulos valores. El estudio revela la importancia de la dinámica de las SCB y sus retos en el contexto de la ciberseguridad en el sector financiero.

En este contexto, los trabajos futuros deberán estar orientados a la evaluación de la percepción que se tiene de las comisionistas respecto de la propuesta desarrollada en este trabajo. En este sentido, se sugiere evaluar factores como la madurez de la plataforma e infraestructura tecnológica de la empresa y el presupuesto asignado, para fortalecer algunos de los equipos o las capacidades de los profesionales, así como valorar el impacto de implementación de los equipos morados frente a otras prácticas o metodologías. De igual forma, deberá comparar y contrastar la percepción de los equipos morados con la toma de decisiones de la alta dirección, vinculando a los altos ejecutivos y la junta directiva, para darles una visión situada y aplicada de cómo interactúan estos equipos durante las pruebas de ciberseguridad.

Agradecimientos

Se hace especial agradecimiento a la Escuela Superior de Guerra “Rafael Reyes Prieto” de Colombia, en particular al programa de Maestría en Ciberseguridad y Ciberdefensa, por el apoyo y acompañamiento durante el desarrollo de este trabajo académico.

Referencias

Bolsa de Valores de Colombia. (s. f.). ¿Qué es una sociedad comisionista? https://www.bvc.com.co/pps/tibco/portalbvc/Home/ComisionistasyAfiliados/Afiliados/Acerca_Comisionistas?action=dummy

Cajaraville, P. S., & García, R. (2016). «Red Team», la evolución hacia las auditorías en entornos ciberfísicos. *Seguritecnia*, 434, 30-33.

Diogenes, Y. & Ozkaya, E. (2018). *Cybersecurity, attack and defense strategies: Infrastructure security with Red Team and Blue Team tactics*. Birmingham - Mumbai: Packt Publishing.

Drinkwater, D., & Zurkus, K. (2017, julio 26). Red team versus blue team: How to run an effective simulation. *CSO Online*. https://www.csoonline.com/article/2122440/emergency-preparedness-red-team-versus-blue-team-how-to-run-an-effective-simulation.html

ISO. (2012). ISO/IEC 27032:2012. Information technology—Security techniques—Guidelines for cybersecurity. https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

Miessler, D. (2020). The Difference Between Red, Blue, and Purple Teams. https://danielmiessler.com/study/red-blue-purple-teams/

MITRE ATT&CK. (s. f.). MITRE ATT&CK. https://attack.mitre.org/

National Institute of Standards and Technology - NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (NIST CSWP 04162018; p. NIST CSWP 04162018). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Navarrete Saavedra, F. (2014). El ciberespacio: Nuevo escenario de confrontación. *Anuario mexicano de derecho internacional*, 14, 863-868.

Oakley, J. G. (2019). *Professional Red Teaming: Conducting Successful Cybersecurity Engagements*. Apress. https://doi.org/10.1007/978-1-4842-4309-1

Peters, S. (2016, julio 13). Purple Teaming: Red & Blue Living Together, Mass Hysteria. https://www.darkreading.com/operations/purple-teaming-red-blue-living-together-mass-hysteria

Purple Team Cybersecurity, SANS Institute. (s. f.). SANS Purple Team. https://www.sans.org/purple-team

SANS. (2009, julio 23). Digital Forensics and Incident Response Blog. https://www.sans.org/blog/security-intelligence-introduction-pt-2-/

SANS. (2019, agosto 14). Practical Tips to Build a Successful Purple Team. https://www.sans.org/webcasts/practical-tips-build-successful-purple-team-110445

SecureAuth. (2021). Security in Plain English: What are Red, Blue, and Purple Teams? SecureAuth. https://www.secureauth.com/blog/security-in-plain-english-what-are-red-blue-and-purple-teams-2/

Superintendencia Financiera de Colombia. (2014). Circular Básica Jurídica 029 de 2014. https://www.superfinanciera.gov.co/inicio/normativa/normativa-general/circular-basica-juridica-ce---/parte-iii-mercado-desintermediado-10083481

Superintendencia Financiera de Colombia. (2020a). Circular Externa 025 de 2020 SARO. https://www.superfinanciera.gov.co/inicio/normativa/normativa-general/circulares-externas-cartas-circulares-y-resoluciones-desde-el-ano-/circulares-externas/circulares-externas--10102740

Superintendencia Financiera de Colombia. (2020b). Informe entidades financieras SFC [Fuente derivada de la intranet privada de la Superintendencia Financiera de Colombia]. Bogotá: Superintendencia Financiera de Colombia.

UNIR. (s. f.). Red Team, Blue Team y Purple Team: Funciones y diferencias. https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/