Gestión de la exposición en ciberseguridad

Federico Pacheco[1], Diego Staino[2]

[1] Universidad Tecnológica Nacional, Buenos Aires, Argentina
[2] Instituto Universitario de la Policía Federal, Buenos Aires, Argentina
federico.pacheco@gmail.com
diegostaino@hotmail.com

Abstract. La gestión de la exposición en ciberseguridad es una nueva área de estudio considerada dentro de la Ciberdefensa Activa, centrada en la aplicación del concepto de exposición proveniente de la gestión de riesgos organizacionales. La misma extiende las ideas y prácticas de la gestión de vulnerabilidades y amenazas, para darle un enfoque generalizado y abarcativo, que permite interpretar el conjunto integral a través de la lente de los riesgos. En este trabajo se analiza el estado del arte de los conceptos y aplicaciones de la gestión de la exposición en ciberseguridad, y se presenta un enfoque para su aplicabilidad en organizaciones. La contribución propuesta está relacionada con la inexistencia previa de contenidos académicos sobre la temática, dada su reciente aparición.

Keywords: Gestión de la Exposición, Gestión de Riesgos de Seguridad.

1 Introducción

En ciberseguridad es común adaptar conceptos y modelos de otras disciplinas. Como ejemplos, del sector militar provienen la defensa en profundidad y seguridad perimetral, y de la gestión de riesgos operacionales y financieros, proviene la gestión de riesgos de ciberseguridad. El abordaje del malware se basa en las estrategias contra virus biológicos, con analogías como la cuarentena y la inoculación. De la ingeniería se toma la tolerancia, resiliencia y fallo seguro, del urbanismo la zonificación y segmentación, de la industria automotriz las capas de seguridad, de la aeronáutica los sistemas redundantes, y de la ciencia forense la informática forense.

El concepto de "gestión de la exposición en ciberseguridad" (en adelante GEC) sigue esta lógica, ya que fuera del ámbito de la ciberseguridad se refiere al proceso de identificar, analizar y gestionar los diversos tipos de riesgos a los que una organización puede estar expuesta. Áreas clave en las que el concepto es fundamental son las transacciones financieras, los seguros y ciencias actuariales, la cadena de suministro y riesgos operacionales, el medioambiente y sistemas sanitarios, la gestión de proyectos, y el cumplimiento legal y normativo.

Este trabajo se centra en la GEC, una nueva área de estudio dentro de la Ciberdefensa Activa como evolución del enfoque de protección de la seguridad basada en la premisa de que el uso de tácticas ofensivas para ralentizar a un atacante hace que los ciberataques sean más difíciles lograr y más fáciles de detectar[1]. La Ciberdefensa Activa implica estrategias y tecnologías para orquestar el movimiento o cambios en

varios componentes y capas de entorno de TI, a través de la superficie de ataque, para aumentar la incertidumbre y la complejidad dentro de un sistema objetivo.

La obvia diferencia entre exposición y vulnerabilidades radica en la naturaleza del acceso que brindan a los actores de amenazas. Mientras una vulnerabilidad es una debilidad que se explota activamente para obtener acceso directo no autorizado a un sistema o red, la exposición se refiere a las condiciones que permiten a los actores de amenazas obtener acceso indirecto, generalmente a través de ataques dirigidos en capas. La exposición entonces puede definir como las condiciones que, aunque no son explotables por sí solas, crean un entorno propicio para que un atacante pueda obtener acceso. Estas pueden incluir configuraciones incorrectas, falta de cifrado, políticas de seguridad inadecuada. Comprender esta distinción es clave para desarrollar estrategias de seguridad específicas y mantener una postura de defensa sólida.

Considerando una amenaza como acción que puede causar daño si se manifiesta, sabemos que para que se convierta en un ataque se requiere intención, capacidad y oportunidad. Dado que no se pueden controlar las intenciones ni las capacidades, solo se pueden controlar sus oportunidades, que dependen de cuán expuesta y vulnerable esté una organización a las acciones previstas. Esto lleva a que la gestión derive en requerir el manejo de la exposición a amenazas, tomando el control de la reducción de las oportunidades que los actores podrían tener al manifestar su intención y capacidades en un ataque. Esta situación de incertidumbre en el resultado del enfrentamiento con el adversario se refleja en el concepto de “niebla de guerra” (fog of war) de Clausewitz.

Dada su reciente aparición, el término y el concepto de GEC no son universalmente reconocidos en la literatura estándar de ciberseguridad, por lo que este estudio busca presentarlo de forma sistematizada y estructurada, a fin de que pueda servir como punto de partida para el estudio del tema. No existiendo aún investigaciones formales al respecto, este trabajo tratará el tema desde una perspectiva crítica, sin asumir que el concepto pueda funcionar como mejor enfoque que los ya existentes. Sin embargo, vale destacar los aportes de investigadores de empresas de ciberseguridad reconocidas, que permitieron allanar el camino para su comprensión desde la perspectiva de la industria.

2 Problemática

Las organizaciones experimentan un volumen creciente de vulnerabilidades descubiertas y exposiciones a amenazas priorizadas debido a la complejidad de los entornos, la mayor cantidad de aplicaciones utilizadas, y el mayor uso de servicios en la nube. La abrumadora cantidad de vulnerabilidades que aparecen a diario requiere a las organizaciones no solo reconocerlas, sino concentrarse en aquellas que las afectan, lo que lleva a determinar qué sistemas están potencialmente amenazados por los fenómenos conocidos[4]. Junto a esta situación, el tiempo promedio que lleva explotar las vulnerabilidades ha disminuido significativamente en los últimos años.

El aumento de la complejidad es generado por entornos ampliados y diversificados, donde aumenta naturalmente la superficie de ataque, haciendo más difícil identificar y proteger los activos críticos. Esto dificulta sostener en el tiempo una clasificación y comprensión de los riesgos, junto con los numerosos hallazgos, dejan a las organizaciones con demasiado por hacer respecto a su exposición y poca orientación sobre qué hacer primero, paralizando a menudo las acciones realizables.

Las interrelaciones entre la gestión de vulnerabilidades, riesgos y resiliencia, fue largamente tratada en la literatura especializada, concluyendo que reducir las vulnerabilidades reduce los riesgos, aunque no necesariamente a gestionarlos con eficacia, no está orientada a potenciar la capacidad para hacer frente a eventos disruptivos[5]. Además, se considera que el foco para la mitigación debe estar en vulnerabilidades que tienen un potencial real de generar impacto, esto es posible mediante un acercamiento basado en riesgo[9]. Por otro lado, aunque la evaluación de los riesgos de seguridad es algo que se realiza periódicamente, un panorama de superficie de ataque que evoluciona al ritmo actual deriva en una gestión reactiva que no reduce adecuadamente la exposición. Recientemente, algunos autores comenzaron a recomendar abandonar los modelos de gestión de riesgos en favor de la gestión de la exposición a las amenazas[2] lo cual puede interpretarse como un primer movimiento hacia la necesidad de este nuevo enfoque.

Uno de los grandes inconvenientes de la gestión de vulnerabilidades es que se basa en su mayor medida gran medida en que los parches existen, y los equipos de seguridad se han vuelto dependientes de estos hasta el punto de que los controles y los procesos de gestión de riesgos técnicos han pasado a un segundo plano en algunas de estas discusiones. Esto dio origen a la gestión holística de las vulnerabilidades[9]. El hecho de que exista una vulnerabilidad no significa que aplicar parches sea la respuesta. A veces, son los cambios de configuración, actualizaciones, o controles compensatorios.

Finalmente, es bien sabido que el volumen de esfuerzo requerido y la diversidad de problemas potenciales conducen a prioridades conflictivas y una "fatiga de información" (*dashboard fatigue*) que complica la interpretación adecuada de los indicadores, limitando su utilidad.

3 Un abordaje integral

La GEC puede parecer un concepto forzado por el mercado y por la necesidad de mantener siempre activo el negocio de la ciberseguridad. Sin embargo, al profundizar en su enfoque, se entiende que podría tratarse de una forma más eficiente de encarar la problemática moderna de la ciberseguridad en entornos organizacionales, con el objetivo de abordar la complejidad mediante una visibilidad completa y la gestión proactiva de los riesgos asociados a cada elemento de manera integral.

Podemos definirla como un conjunto de procesos y tecnologías que permiten a las organizaciones evaluar continuamente la visibilidad (qué activos tenemos y cuánto son visibles para un atacante) y validar la accesibilidad, entendida como evaluar qué tan accesibles son los activos para usuarios no autorizados, y sus vulnerabilidades[3]. Como tal conjunto de procesos, se debe regir por un programa mayor de gestión continua de la exposición a amenazas (CTEM, Continuous Threat Exposure Management) y en principio cuenta con cinco etapas: alcance, descubrimiento, priorización, validación y movilización. Esta mirada deriva en que las organizaciones deban usar nuevas herramientas para por ejemplo inventariar activos digitales, identificar exposiciones, simular o probar ataques y movilizar una respuesta.

La GEC se propone como opción para reducir los desafíos de inventariar, priorizar y validar la exposición a amenazas que existen debido a una superficie de ataque en expansión donde la gestión de vulnerabilidades tradicional no es suficiente. Algunos

resultados que se esperan de la GEC son el registro y la presentación de informes del impacto potencial en la reducción de riesgos y la justificación del valor organizacional. En este sentido, se busca prioriza la reducción de riesgos, dejando usualmente algunas brechas donde tienen menos control, como las plataformas SaaS o las redes sociales.

La GEC propone un enfoque sistémico para mejorar las prioridades y moverse entre dos realidades de la seguridad: que no es posible solucionar todo, y que no se puede confiar en corregir una vulnerabilidad puede posponerse si es de bajo riesgo. Si bien GEC no es una tecnología, implica una combinación de procesos y tecnologías, lo que significa usar métodos, protocolos y herramientas para gestionar el grado de exposición de los activos. El aspecto continuo de la evaluación lo hace diferente a enfoques tradicionales que podrían evaluar los riesgos periódicamente, y se requiere una revisión constante para comprender y gestionar la relación entre la naturaleza evolutiva de las amenazas y la maduración de las organizaciones para actuar en consecuencia. GEC sugiere que exista un programa estructurado para gestionar y mitigar los riesgos asociados a la exposición. El enfoque proactivo y continuo busca mantener la integridad de los sistemas, que los activos críticos estén protegidos y que los recursos se asignen de forma óptima, para abordar las vulnerabilidades antes de que puedan ser explotadas, minimizar los riesgos, salvaguardar los datos y garantizar la continuidad operativa.

El foco se sitúa en las amenazas, no en las vulnerabilidades, se derivan de estas en combinación con el impacto potencial, a través de un cálculo probabilístico. En efecto, la forma tradicional de gestionar las vulnerabilidades puede verse como un enfoque reactivo, mientras esta nueva perspectiva, se busca aplicar remediciones después de haber encontrado una amenaza, y no ante la eventual aparición de una vulnerabilidad.

Desde dicha proactividad, la GEC busca realizar monitoreo, evaluación, priorización y resolución continua de problemas de seguridad, tratando la explotabilidad de las amenazas. Como objetivo, se espera obtener un plan de mejora y remediación de la postura de seguridad dinámica, consistente y viable, que los tomadores de decisiones de negocios puedan comprender y sobre el que equipos de arquitectura puedan actuar.

La GEC tiene como requisito la gestión de la superficie de ataque, referida a la exposición general de todos los activos digitales, físicos, externos, redes compartidas y otros puntos de entrada a ciberataques. Además, abarca aspectos técnicos, legales, éticos y de gestión, lo que produce una necesidad de convergencia, y crea nuevos desafíos para las organizaciones más allá de los propios de la ciberseguridad.

Bajo la consideración de que, fuera de la ciberseguridad, la gestión de la exposición fue largamente estudiada en ámbitos como el de los mercados y los negocios, a través del estudio sobre el riesgo, se propone una tabla en la que se presentan analogías posibles entre su campo de acción tradicional, y la ciberseguridad, para permitir una comprensión más cabal.

Tabla 1. Analogías de gestión de la exposición

Aspecto	Gestión de Exposición en Negocios	Gestión de Exposición en Ciberseguridad	Gestión de Exposición en la Inmunología
Foco	Identificar, evaluar y gestionar riesgos que podrían impactar financieramente, en las operaciones o la reputación.	Identificar, evaluar y mitigar riesgos para los sistemas de información y datos.	Identificar, evaluar y responder a agentes patógenos que puedan impactar en la salud.

Riesgos Clave	Riesgos financieros, interrupciones operativas, desalineaciones estratégicas, volatilidad del mercado.	Malware, phishing, brechas de datos, acceso no autorizado, vulnerabilidades de sistema.	Infecciones, enfermedades autoinmunes, reacciones alérgicas.
Enfoque de Gestión	Gestión de riesgo integrada, cobertura financiera, planificación de resiliencia operacional.	Implementación de controles de seguridad, evaluaciones regulares de vulnerabilidad, planificación de respuesta a incidentes.	Prevención de enfermedades, fortalecimiento del sistema inmune.
Herramientas y Técnicas	Evaluaciones de riesgo, instrumentos financieros (p. ej., seguros, derivados), planificación de continuidad de negocio.	Software de seguridad (p. ej., firewalls, antivirus), pruebas de penetración, cifrado, controles de acceso.	Vacunas, terapias inmunológicas, medicamentos preventivos.
Resultado	Estabilización de ganancias, mejora de confianza de inversores, cumplimiento de regulaciones.	Protección de activos de información, cumplimiento con leyes de protección de datos, mantenimiento de la confianza.	Protección contra enfermedades, mejora de la respuesta inmunológica.
Desafíos	Imprevisibilidad del mercado, cambios regulatorios, factores económicos globales.	Amenazas en evolución, vulnerabilidades tecnológicas, error humano.	Variabilidad genética de los patógenos, resistencia a los medicamentos.
Objetivos	Estabilizar las ganancias corporativas contra riesgos más allá del control de la gestión.	Salvaguardar la integridad, confidencialidad y disponibilidad de los activos de información.	Mantener la salud y prevenir enfermedades.
Dificultades	Complejidad de los mercados y los contextos económicos. Continuo desarrollo de nuevos participantes.	Complejidad y dinamismo de los entornos tecnológicos. Continuo desarrollo de amenazas.	Adaptación a la evolución rápida de los patógenos, manejo de las reacciones adversas a tratamientos inmunológicos.

3.1 Requerimientos y aspectos clave

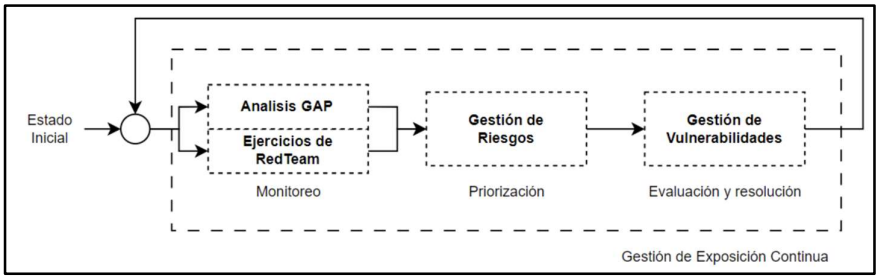
La existencia de un enfoque conceptual para la gestión de la ciberseguridad se basa en muchos de los mismos aspectos que producen un sistema de gestión efectivo, por lo que sus elementos y aspectos clave no son nuevos, pero sí hay algunos que emergen con mayor relevancia. A continuación, se mencionan algunos de estos elementos en base a su importancia en el contexto de la GEC, en torno a algunos ejes centrales.

Primero, la visibilidad integral emerge como un requisito crítico, facilitando el entendimiento exhaustivo de los activos de TI, incluyendo sistemas en la nube, redes, aplicaciones y endpoints, lo que a su vez permite una apreciación completa de la superficie de ataque. La Evaluación de Riesgos complementa este panorama con análisis continuos que no solo identifican vulnerabilidades técnicas, sino que también las contextualizan dentro del entorno empresarial, evaluando su impacto potencial en los procesos de negocio y la continuidad operativa.

En segundo lugar, la Priorización basada en el riesgo y la Automatización y orquestación constituyen pilares para la eficiencia en la gestión de la ciberseguridad.

La priorización permite focalizar esfuerzos en mitigaciones críticas, mientras que la automatización y orquestación de procesos facilitan respuestas rápidas y eficientes ante incidentes. La colaboración entre los departamentos de IT y negocios se presenta como esencial para alinear las estrategias de seguridad con los objetivos corporativos.

Finalmente, se subraya la importancia del monitoreo continuo, la mejora continua, la mitigación de vulnerabilidades, la inteligencia de ciber amenazas, la planificación de respuesta a incidentes, el establecimiento de políticas y procedimientos de seguridad, el cumplimiento y requisitos regulatorios, y la seguridad de la identidad. Estos aspectos, interconectados, son fundamentales para una gestión proactiva y adaptativa frente a las dinámicas amenazas cibernéticas, asegurando no solo la detección y respuesta efectivas, sino también la evolución constante de las prácticas de seguridad para enfrentar el cambiante panorama de amenazas y los avances tecnológicos.



Esquema de interrelación de funciones conocidas

3.2 **Tecnologías relacionadas**

Existe una serie de tecnologías relacionadas, que toman forma de herramientas creadas para encarar diferentes aspectos de la ciberseguridad, y conforman el conjunto de tecnologías en las que puede apoyarse la GEC. Analizando la naturaleza de estas herramientas, podemos agruparlas en dos subcategorías, una relacionada con la gestión de la superficie de ataque y otra relacionada con las evaluaciones de seguridad. De hecho, ambas categorías han presentado con el tiempo una clara convergencia, comenzando algunas a incluir funciones de las otras. Incluso han aparecido convergencias entre herramientas en apariencia opuestas, como ser las de equipo azul (Blue Team) y de equipo rojo (Red Team).

- Herramientas de Gestión de Superficie de ataque

Servicios de protección de riesgos digitales (DRPS, Digital Risk Protection Services). Conjunto de soluciones enfocadas en la identificación, el monitoreo y la gestión de la presencia digital de las organizaciones. Abordan ciberataques, filtraciones de datos y fraudes, extendiendo su cobertura más allá de la infraestructura TI para incluir el ecosistema digital, como redes sociales y dominios web. Ofrecen inteligencia contextual sobre amenazas, permitiendo adoptar medidas proactivas para mitigar riesgos, proteger activos digitales.

Gestión de superficie de ataque externo (EASM, External Attack Surface Management). Conjunto de procesos y tecnologías dedicados a identificar, catalogar,

y analizar los activos digitales expuestos en el entorno digital externo, con el objetivo de evaluar y mitigar vulnerabilidades antes de que sean explotadas por actores maliciosos. Se centra en el reconocimiento y la gestión proactiva de los componentes accesibles públicamente de la infraestructura tecnológica, incluidos servidores, aplicaciones web, y servicios en la nube, entre otros. Esto permite obtener una visión integral de su presencia digital desde la perspectiva de un potencial atacante externo,

Gestión de la superficie de ataque de ciberactivos (CAASM, Cyber Asset Attack Surface Management). Si bien en principio es similar a la anterior, tiene un aspecto diferente en cuanto a su alcance, abarcando todos los componentes susceptibles dentro del entorno digital de la entidad, incluyendo dispositivos, redes, aplicaciones y servicios en la nube. Su objetivo es fortalecer la seguridad mediante vigilancia continua y gestión de las vulnerabilidades, facilitando la protección y mejora en la postura de seguridad.

- Herramientas de Evaluaciones de seguridad

Simulación de brechas y ataques (BAS, por su sigla en inglés de Breach and Attack Simulation). Permite evaluar la resistencia a las ciber amenazas mediante la ejecución de simulaciones controladas de ciber ataques reales. Implica el uso de estrategias que imitan las tácticas, técnicas y procedimientos (TTP) de los adversarios. Ofrece una visión práctica del nivel de preparación frente a incidentes de seguridad, permitiendo la identificación de áreas de mejora y la implementación de medidas correctivas para reforzar las defensas antes de que ocurran ataques reales.

Pruebas de penetración como servicio (PTaaS, Penetration Testing as a Service). Modelo de entrega de servicios en el que las pruebas de penetración son realizadas de manera periódica o continua. Permite realizar pruebas sobre sistemas, redes y aplicaciones, y se distingue por su flexibilidad, permitiendo ajustar la frecuencia y el alcance de las pruebas según sus necesidades dinámicas, lo que resulta en una visión más consistente y actualizada de la postura de seguridad. Además, facilita una implementación más oportuna de medidas correctivas.

Pruebas de penetración automatizadas y herramientas de equipo rojo (Automated Penetration Testing and Red Teaming Tools (también CART, por Continuous Automated Red Teaming). Integran tecnologías para simular de manera continua y automatizada ataques contra sistemas, redes y aplicaciones. Combina la automatización de las pruebas de penetración con las estrategias de equipos rojos, que emplean tácticas ofensivas para evaluar la eficacia de las defensas desde la perspectiva de un adversario. Busca identificar vulnerabilidades y brechas de forma persistente, proporcionando información de interés para el fortalecimiento de las medidas de seguridad.

Evaluación de vulnerabilidades (VA, por Vulnerability Assessment) y tecnología de priorización de vulnerabilidad (VPT, por Vulnerability Prioritization Technology). Son procesos acotados y complementarios que se enfocan en la identificación sistemática. La VA implica el escaneo de redes, sistemas y aplicaciones para detectar fallos de seguridad, y deficiencias técnicas conocidas. Las VPT permiten analizar y ordenar estas vulnerabilidades basándose en su criticidad, el contexto

operativo y el potencial impacto, permitiendo una asignación eficaz de recursos hacia la mitigación de los riesgos más significativos.

Estas tecnologías se centran en identificar, evaluar y mitigar las vulnerabilidades de los activos digitales y sistemas de información, en algunos casos en relación a las ciber amenazas, y se entrecruzan de diversas formas. Varias de ellas implican mapear y comprender la superficie de ataque, que refleja la suma de diferentes puntos donde un usuario no autorizado puede introducir o extraer datos desde y hacia un entorno.
El objetivo general de estos servicios y herramientas es mejorar la postura global de seguridad, mejorar las defensas, prepararse para posibles ciberataques. Más allá de esto, estas tecnologías abogan por un enfoque dinámico y continuo, reconociendo que el panorama de amenazas está en constante evolución y requiere una vigilancia y adaptación constantes. Cada una desempeña un papel en la estrategia, y se complementan entre sí, dando un enfoque integral para la gestión de riesgos digitales.

El impacto de la GEC en las tecnologías existentes radica principalmente en la consolidación de sus capacidades individuales. Las tecnologías que respaldan los procesos de la GEC permiten escalar mejor la capacidad para identificar la probabilidad de explotación en función de la visibilidad en la superficie de ataque, validar si los ataques tendrán éxito y si los controles de seguridad pueden ayudar a prevenirlos. El nivel de automatización e integración que brindan las tecnologías de gestión de exposición transforma la forma en que las organizaciones realizan actividades de exposición aisladas, que incluyen pruebas de penetración y escaneo de vulnerabilidades, que en general se realizan principalmente con fines de cumplimiento y sin integrar los hallazgos para una gestión de exposición más eficaz.

Si bien muchas de las actividades relacionadas con la GEC pueden realizarse aisladas, la integración estrecha y la consolidación de soluciones que la respaldan impulsan la adopción por parte del usuario final.

3.3 Beneficios

Como se mencionó, la GEC es un enfoque proactivo que se centra en identificar, evaluar y abordar posibles vulnerabilidades y riesgos antes de que puedan ser explotados por adversarios. En lugar de reaccionar a amenazas después de actuar sobre ellas, la GEC tiene como objetivo reducir la superficie de ataque comprendiendo y minimizando los puntos débiles de un sistema, red u organización, para identificar y priorizar sistemáticamente las vulnerabilidades. Esto ofrece múltiples ventajas de cara a reforzar la postura de ciberseguridad de una organización. Estos beneficios incluyen:

- **Facilitación de la TDIR (Detección de amenazas y respuesta a incidentes) y GRC (Gobernanza, riesgo y cumplimiento):** así como seguridad se percibió históricamente como ralentizador de TI, GRC suele verse como ralentizador de la seguridad. Mientras que TDIR requiere respuestas rápidas, GRC busca el juego a largo plazo, y a veces están en desacuerdo. Para encontrar el punto medio entre, GEC toma resultados técnicos de TDIR y lo traduce en un análisis mensurable, priorizado y más fácil de entender para que GRC lo interprete y concuerde desde una posición estratégica. Al priorizar las vulnerabilidades por proximidad a la amenaza, se facilita la comprensión y urgencia de los informes estratégicos. Con

acuerdo interno, el frente unificado ayuda a comunicar a equipos de infraestructura y arquitectura la importancia de la remediación y cronogramas asociados.

- **Identificación proactiva y comprensión temprana de vulnerabilidades**: al anticipar áreas de debilidad antes de que sean explotadas, se pueden implementar medidas preventivas para salvaguardar activos críticos, lo que reduce el riesgo de incidentes y posibilita una gestión más eficaz del perfil de riesgo global.
- **Mejora en la toma de decisiones de ciberseguridad**: al tener una comprensión clara del perfil de riesgo, se pueden distribuir recursos de manera más estratégica, enfocándose en áreas que requieren atención prioritaria, lo que conduce a una asignación de recursos más eficiente, maximizando la inversión en seguridad.
- **Optimización de las prioridades de ciberseguridad**: esto se traduce en concentrar los esfuerzos en áreas con mayor riesgo y potencial de daño, garantizando que los recursos se utilicen donde más se necesitan.
- **Mejora de la prevención y respuesta a ataques**: significa que las organizaciones no solo están mejor preparadas para prevenir ataques, sino que también están equipadas para responder de manera más efectiva y rápida en caso de que ocurra un incidente.
- **Reducción de la superficie de ataque**: esto limita las oportunidades de los atacantes para explotar los sistemas y reduce la probabilidad de que los ataques tengan éxito (a menor superficie de ataque, menor exposición a riesgos).

3.4 Ciclo de vida

La GEC es un proceso continuo, ya que el entorno de amenazas cibernéticas está en constante cambio y evolución, y las organizaciones deben ser diligentes. El ciclo de vida de la GEC abarca una serie de pasos destinados a fortalecer la postura de seguridad de una organización, y se estructura en cuatro etapas fundamentales:

1) Comprender la exposición: implica la identificación de la superficie de ataque y puntos de entrada explotables. Se analizan los activos digitales y físicos, reconociendo la importancia de un inventario actualizado y la gestión de riesgos asociados, no solo dispositivos y servidores, sino también la seguridad física de los espacios y el manejo de datos. Esto se complementa con el alcance de lo más importante (las llamadas "Joyas de la Corona") que se refiere a la identificación y clasificación de datos y procesos según su valor y sensibilidad, incluyendo propiedad intelectual, datos de clientes, registros financieros y otros elementos críticos para el negocio.

2) Comprender a los adversarios: se enfoca en la visibilidad sobre los objetivos del adversario y TTPs, e implica el análisis de las tácticas, técnicas y procedimientos de potenciales atacantes, utilizando marcos como MITRE ATT&CK para estructurar esta información. También incluye la inteligencia de ciber amenazas (CTI) que consiste en mantenerse informado sobre las últimas amenazas y vulnerabilidades, para adaptar la estrategia de seguridad. Esto sustenta el posicionamiento de CTI como el principal respaldo para la toma de decisiones sobre ciberseguridad en organizaciones[6].

3) Evaluar las defensas: esto incluye la validación de la eficacia de los controles, testeándolos contra amenazas actuales, utilizando herramientas como plataformas de validación de seguridad para simular ataques y evaluar la respuesta de los sistemas de seguridad. Además, implica la cuantificación del valor y la eficacia de los controles y equipos con métricas como los resultados de prevención y detección, comparándolos con estándares de la industria para determinar la efectividad y áreas de mejora.

4) Mejorar la preparación: se centra en fortalecer la preparación ante amenazas conocidas y emergentes, lo que puede implicar la implementación de nuevas tecnologías, la optimización de procesos y la capacitación del personal. Se usan herramientas que ofrecen sugerencias de mitigación y reglas de detección para garantizar defensas efectivas y alineadas con las amenazas y prácticas actuales.

Cada etapas contribuye significativamente a construir una defensa robusta y adaptable. La proactividad y la evaluación continua permiten protegerse contra amenazas actuales, y prepararse para responder a desafíos futuros.

Un punto fuerte de la GEC es su capacidad para anticipar y mitigar las amenazas antes de que se materialicen en ataques efectivos, evitando gestionar episodios independientes, en pos de darles un tratamiento sistemático. Esto representa una evolución en la gestión de la seguridad, alejándose de tácticas reactivas y enfocándose en estrategias proactivas y preventivas, y de ahí su vinculación directa con la ciberdefensa activa. La complejidad creciente de las infraestructuras de TI, exacerbada por tendencias como el trabajo remoto y la política dispositivos propios, amplía la superficie de ataque, haciendo que la gestión proactiva sea más relevante.

Dado que la GEC implica un análisis exhaustivo de las vulnerabilidades potenciales en un entorno de TI, abarca las debilidades técnicas, humanas y organizacionales. Al identificarlas se pueden crear estrategias para mitigarlas antes ser explotadas. El impacto de adoptar GEC se extiende a varios niveles, ya que para los responsables de ciberseguridad implica un cambio en la forma de aborda la seguridad que va más allá de la implementación de nuevas herramientas o tecnologías, y requiere una reevaluación de la estrategia en su conjunto, reforzando el aspecto preventivo.

3.5 Dificultades y desafíos

Los primeros movimientos hacia la introducción de GEC en organizaciones conllevan dificultades en su implementación práctica, reflejadas en ciertas brechas:

Enfoque Limitado: la más importante es la visión aislada de las vulnerabilidades y la exposición. El descubrimiento y la remediación se dan en silos que dificultan comprender el panorama del riesgo. Los límites artificiales para la red o las áreas solo inhiben la capacidad de reducir el riesgo adecuado en el momento adecuado.

El escaneo de objetivos para gestión de vulnerabilidades, pruebas de penetración y otras actividades de evaluación a menudo comienza con un rango de IP o subred, o a veces un área de la empresa, que se percibe como la más riesgosa. Sin embargo, este enfoque tradicional no logra identificar dónde está el foco del negocio y, en cambio, crea barreras arbitrarias. El objetivo principal de la gestión de exposición actual es el escaneo de vulnerabilidades, lo que fomenta el descubrimiento de la criticidad de la vulnerabilidad por activo a través de su implementación. La mayoría de los escáneres

de vulnerabilidades siguen una secuencia de técnicas para recopilar datos para analizar y presentar resultados, que incluyen escaneo de descubrimiento, de puertos, y de aplicaciones. Estos métodos no consideran brechas como las introducidas por partes de la empresa, que no se basan en activos externos, como aplicaciones SaaS, activos relacionados con la marca, como cuentas de redes sociales, o activos de desarrollo, como repositorios de códigos.

Estos elementos de exposición adyacentes introducen oportunidades de compromiso que no se consideran parte del escaneo tradicional. Además, el alcance de dichos análisis se limita a la infraestructura que se puede descubrir en un entorno cerrado o administrado por empresas específicas y no a los servicios más amplios o plataformas de terceros que utilizan las organizaciones[7].

Otra brecha transformada en desafío está en el hecho de priorizar basándose solo la amenaza y gravedad, e ignorar el impacto potencial. El uso de frameworks como MITRE ATT&CK y sistemas de puntuación de vulnerabilidades como CVSS son útiles, pero si se consideran de forma aislada, limitan la relevancia del impacto potencial de una exposición. Por esto es necesario ir más allá de la puntuación para introducir contexto y relatividad a las exposiciones descubiertas, usando por ejemplo elementos de inteligencia de amenazas, o comparaciones con referencias (benchmarks) de la industria y estadísticas sobre compromisos históricos. Esto permite dirigir la inversión de tiempo y recursos a lo que más contribuya al negocio. Evaluar y priorizar las vulnerabilidades requiere un conjunto de medidas para obtener una visión más precisa de cuán explotable, visible, accesible y probable es que se manifieste un ataque.

Enfoque Reactivo: Una dificultad adicional la conforma el enfoque mayormente reactivo a las exposiciones, con participación ad hoc de las partes interesadas, impulsada por eventos. La mayoría de las organizaciones admitiría centrarse en procedimientos de planificación de respuesta para escenarios que se comprenden bien, en lugar de introducir una validación efectiva en cuanto a la probabilidad del evento. El volumen de problemas potenciales significa que es esencial identificar claramente objetivos para la prevención e invertir esfuerzos en reducir el riesgo de que ocurran esos eventos. Sin embargo, también debe invertir en reducir el impacto de eventos que quedan fuera de esa lista de objetivos inicial. La planificación de eventos de respuesta a incidentes suele contener algunos temas importantes: planificación de comunicaciones para limitar o reparar el daño reputacional del negocio, recuperación ante desastres para permitir que el negocio continúe funcionando durante un evento de crisis, y aprender lecciones de las actividades identificadas para garantizar que el trabajo de reparación prevenga o reduzca el impacto de cualquier suceso futuro.

3.6 **Implementación**

La implementación de un programa de GEC es un proceso complejo que requiere un enfoque estratégico. A continuación, se detallan los pasos de este proceso de forma simplificada, cada uno de los pasos tiene su propio cuerpo de conocimientos.

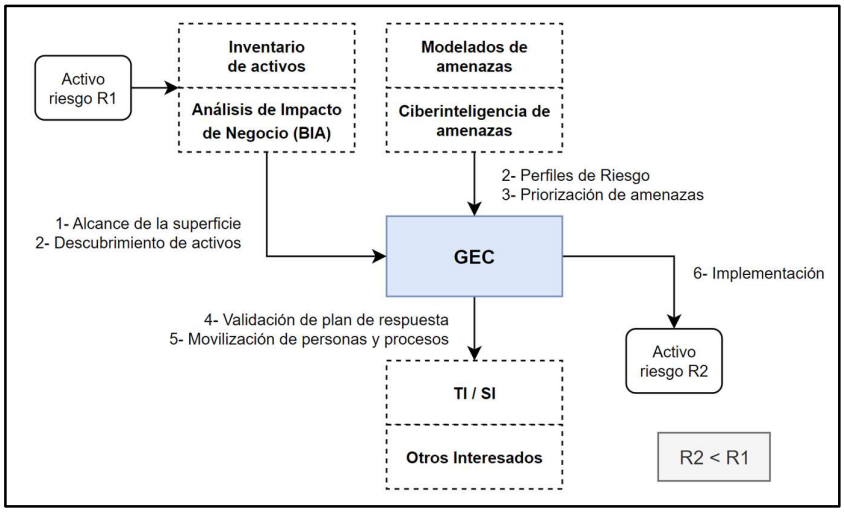
Fase de diagnóstico:

1. Determinación del alcance de la superficie de ataque: implica una evaluación exhaustiva de los activos vulnerables de una organización, que abarca desde

dispositivos y aplicaciones tradicionales hasta elementos menos tangibles como cuentas corporativas en redes sociales y sistemas integrados de cadena de suministro. Para las organizaciones que se inician en GEC, enfocarse en la superficie de ataque externa y la postura de seguridad de SaaS resulta un punto de partida efectivo.
2. Desarrollo de un proceso de descubrimiento de activos y perfiles de riesgo: implica identificar activos, vulnerabilidades, configuraciones incorrectas y otros riesgos, tanto visibles como ocultos, considerando que un volumen elevado de activos y vulnerabilidades identificados no garantiza por sí mismo un programa exitoso, sino que el alcance debe ser preciso, basado en el riesgo empresarial y el impacto potencial.
3. Priorización de amenazas: ponderación según la probabilidad de explotación, considerando factores como urgencia, seguridad, controles compensatorios, tolerancia a la superficie de ataque residual y el nivel de riesgo aceptable. El enfoque debe estar en los activos de alto valor, desarrollando un plan de tratamiento específico para ellos.

Fase accionable:

4. Validación de ataques y reacciones del sistema: implica confirmar la viabilidad de que los atacantes exploten una vulnerabilidad, analizando posibles rutas de ataque y evaluando si el plan de respuesta actual es adecuado. Requiere un consenso entre las partes interesadas sobre los factores desencadenantes que conducen a la remediación.
5. Movilización de personas y procesos: más allá de las soluciones automatizadas, se debe comunicar y comprender el plan GEC entre el equipo de seguridad y las partes interesadas. El esfuerzo de movilización debe asegurar que los equipos implementen los hallazgos eficazmente, documentando flujos de trabajo de aprobación entre equipos.
6. Implementación y herramientas: implica usar herramientas como escáneres de vulnerabilidades hasta plataformas de simulación de amenazas avanzadas, para inventariar activos, identificar exposiciones, simular ataques y movilizar respuestas.



Ciclo de implementación del modelo integrando funciones conocidas

Existen algunos puntos de inflexión que se pueden aprovechar para reducir el riesgo de exposición a amenazas y crear mejores relaciones entre equipos para una respuesta más rápida a las situaciones más relevantes y amenazas de mayor impacto potencial. Esto requiere crear alcances de evaluación de exposición basados en prioridades y riesgos organizacionales claves, teniendo en cuenta el posible impacto comercial de un compromiso en lugar de centrarse en la gravedad de la amenaza únicamente. Además, requiere incorporar técnicas de validación de ciberseguridad mediante simulación de ataques, rutas de ataque, y pruebas de penetración automatizadas. La validación de las amenazas, con mecanismos como simulación, evaluación de configuración o pruebas formales, es una forma de reducir la carga de respuesta al descubrir exposiciones.

Más allá de esto, es importante la colaboración con la alta dirección para comprender cómo informar la exposición de manera significativa usando las evaluaciones de riesgos existentes, y creando una categorización consistente para los descubrimientos, acordadas con otras áreas. También conviene acordar rutas para la resolución y priorización antes de comenzar a informar nuevas exposiciones descubiertas, con líderes de departamentos, en áreas como gestión de TI, operaciones de red, desarrollo de aplicaciones, y recursos humanos. Sin participación generalizada en la organización, la mayoría de los procesos de GEC no pueden funcionar con eficacia, por lo que la colaboración temprana con equipos de resolución y procesos son clave.

3.7 Perspectivas en desarrollo

En términos de las perspectivas futuras, la GEC está preparada para ofrecer una mayor automatización y sofisticación en la identificación y mitigación de riesgos, lo que incluirá la integración de “sistemas inmunes digitales” que se anticipan y adaptan a las amenazas de manera similar al ser humano[8]. La validación de la ciberseguridad, hacia el futuro la GEC implica probar y verificar cómo los sistemas de una organización responderían ante un ataque real, permitiendo mejoras continuas en las estrategias.

La tendencia sugiere un crecimiento de la dependencia de plataformas para evaluaciones de validación de ciberseguridad, que también se integrarán con EASM y DRPS para recopilar información adicional e identificar rutas de ataque vulnerables. Esta convergencia potenciará los productos aislados que respaldan la GEC. El curso de acción más viable pareciera ser aprovechar las oportunidades para incluir características de tecnologías adyacentes para alinearse con la creación de programas de GEC y respaldar la consolidación de soluciones. Además, será necesario mejorar el soporte para organizaciones que buscan madurar su enfoque general hacia estrategias de GEC mejorando sus integraciones tecnológicas y su estrategia de ecosistema de asociación.

4 Limitaciones

La novedad de la temática implica la falta de bibliografía y fuentes académicas de referencia para el tratamiento de este estudio, lo que limita la profundidad de cada tópico, y su aproximación mediante diferentes miradas temáticas. Asimismo, las propuestas realizadas quedan delimitadas a la experiencia de los autores en la industria, pudiendo considerarse otras propuestas más abarcativas y diferentes si se incluyen recomendaciones desde otros saberes.

5 Trabajo futuro

Las investigaciones por venir podrían tomar al menos dos líneas. Una referida al contexto general y el rol de la GEC en la ciberseguridad, y su vinculación con otros elementos de la gestión general de organizaciones, a fin de comprender si es posible legitimarla como nuevo campo. Otra línea es la profundización en la GEC, para crear nuevos constructos conceptuales que potencien su desarrollo. Pueden estudiarse metodologías, herramientas, y tecnologías, que permitan un tratamiento específico, que incluye la aplicación e integración de la inteligencia artificial y aprendizaje automático para automatizar y mejorar la detección de amenazas.

6 Conclusiones

En base a lo expuesto, y esperando dejar abierto el debate de la necesidad de nuevas aproximaciones a las problemáticas de la ciberseguridad, concluimos que la gestión de la exposición es un enfoque válido para abordar los desafíos actuales, que implican entornos complejos donde los enfoques tradicionales tienden a fallar debido a la falta de determinismo natural que presenta la dinámica de la seguridad, y de acuerdos sobre cómo conseguir los mejores resultados. No obstante, dado que los aspectos subyacentes de la GEC se están presentes en las estrategias modernas de ciberseguridad, es menester evitar la creencia de que la novedad requiere nuevos productos y tecnologías. Finalmente, huelga aclarar que, tratándose de una temática novedosa y de desarrollo reciente, esta contribución requiere complementos con otras perspectivas de conocimiento, y no debe entenderse como una simplificación de conceptos, sino como una respuesta inicial desde los conocimientos previos y la experiencia en la industria.

Referencias

1. F. Pacheco, “Ciberdefensa Activa: modelo de trabajo para estrategias defensivas basadas en el error del adversario”.
2. V. Markkanen and T. Frantti, “Patch management planning - towards one-to-one policy,” in *2023 10th International Conference on Dependable Systems and Their Applications (DSA)*, Tokyo, Japan: IEEE, Aug. 2023, pp. 60–69. doi: 10.1109/DSA59317.2023.00018.
3. J. Nunez and A. Davies, “Hype Cycle for Security Operations,” Gartner Inc., Jul. 2023.
4. V. Smyth, “Software vulnerability management: how intelligence helps reduce the risk,” *Network Security*, vol. 2017, no. 3, pp. 10–12, Mar. 2017.
5. K. Rahi, M. Bourgault, and C. Preece, “Risk and vulnerability management, project agility and resilience: a comparative analysis,” *IJISPM*, vol. 9, no. 4, pp. 5–21, Jan. 2022.
6. S. Ainslie, D. Thompson, S. Maynard, and A. Ahmad, “Cyber-threat intelligence for security decision-making: A review and research agenda for practice,” *Computers & Security*, vol. 132, p. 103352, Sep. 2023, doi: 10.1016/j.cose.2023.103352.
7. P. Shoard,“Strategic Roadmap for Managing Threat Exposure” Gartner Inc., Nov. 2023.
8. Dr. A. S. George, A.S.Hovan George, and Dr.T.Baskar, “Digitally Immune Systems: Building Robust Defences in the Age of Cyber Threats,” Aug. 2023.
9. H. Koskenkorva, “The role of security patch management in vulnerability management”.