Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Rol del CISO en un Entorno Organizacional

“Retos y Desafíos”

VIEM
Vicerrectoría de Innovación y Emprendimiento

ECBTI
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación
Ceros y Unos

Boletín de Ciberseguridad

Medio de Divulgación del Centro de Respuestas a Incidentes Informáticos: CSIRT Académico UNAD

E-boletín Informativo CSIRT Académico UNAD

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Veinticinco
Julio de 2024

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CSIRT Académico UNAD

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas - Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo – Decano

Especialización en Seguridad Informática (ECBTI)
Ing. Sonia Ximena Moreno Molano – Líder Programa de Especialización en Seguridad Informática

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Líder
CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernandez

Revisó
Ing. Sonia Ximena Moreno Molano
Líder Maestría en Ciberseguridad – UNAD
Líder Esp. Seguridad Informática - UNAD

Estado legal:
Periodicidad: Mensual
ISSN: 2806-0164

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Tabla de Contenido

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín de Ciberseguridad

Boletín informativo Número 25

Julio 2024

Rol del CISO en un Entorno Organizacional "Retos y Desafíos"

Autores:

Luis Fernando Zambrano Hernández
CSIRT Académico UNAD
https://orcid.org/0000-0002-4690-3526

Hernando José Peña Hidalgo
CSIRT Académico UNAD
https://orcid.org/0000-0002-3477-2645

Libardo Cárdenas Corral
CSIRT Académico UNAD
https://orcid.org/0009-0002-6133-5157

Néstor Raúl Cárdenas Corral
CSIRT Académico UNAD
https://orcid.org/0000-0003-3691-0148

Introducción

Ilustración 1; Generada por ChatGPT

(Da Silva et al., 2022) en su publicación indica que el rol del Chief Information Security Officer (CISO) ha evolucionado significativamente en las organizaciones. Inicialmente, este era visto como un experto que interpretaba un sistema de ciberseguridad complejo y temido, actuando como un "adivino" moderno para la alta dirección. Este papel se caracterizaba por la necesidad de gestionar una amenaza ontológica[1], donde la ciberseguridad se percibía como un riesgo desconocido y aterrador para quienes desconocen de esta disciplina del conocimiento. La naturaleza temerosa de la ciberseguridad contribuía a que se considerara una amenaza existencial para la organización, mientras que la respuesta a esta amenaza ayudaba a definir la identidad general de la misma. Con el tiempo, el CISO ha pasado de ser un simple intérprete de riesgos a un líder crítico en la gestión de la ciberseguridad, enfrentando un entorno cada vez más complejo y en evolución.

El siguiente documento plantea 5 capacidades y conocimientos con las que un CISO debe contar para ser factor de orientación en un equipo de trabajo de **Ciberseguridad**.

[1] La ontología es la rama de la filosofía que se dedica a reflexionar sobre los modos esenciales de existencia de las cosas. Por ejemplo, le es esencial a un triángulo para su existencia el estar conformado por tres ángulos (Posada, 2014).

Desarrollo

Cumplimiento y Adaptación en un Entorno Cambiante

De acuerdo con(World Economic Forum, 2024) un CISO puede aportar significativamente al cumplimiento y adaptación en un entorno cambiante al integrar la ciberseguridad en la gestión de riesgos empresariales, alineando las estrategias de seguridad con los objetivos organizacionales y abordando proactivamente los riesgos emergentes. Este rol, puede aportar desde el liderazgo de iniciativas que fomenten una cultura organizacional enfocada en la ciberseguridad, promoviendo la concienciación y buenas prácticas en todos los niveles, contribuyendo al fortalecimiento de la resiliencia interna. La colaboración entre dependencias y la comunicación de información sobre incidentes son esenciales para enfrentar amenazas cada vez más sofisticadas. Es por esto, que, mantenerse actualizado en regulaciones y normativas permite al CISO garantizar el cumplimiento y anticiparse a nuevos requisitos regulatorios, mientras que el desarrollo de estrategias de resiliencia cibernética asegura que la organización pueda detectar y mitigar riesgos rápidamente en un entorno en constante evolución.

En este sentido los aspectos a considerar son:

- Integración de la ciberseguridad con la gestión de riesgos empresariales.
- El fomento de una cultura organizacional.
- La colaboración y comunicación de información.
- En el desarrollo de estrategias de resiliencia cibernética.

El documento **"Global Cybersecurity Outlook 2024[2]"** se centra en el papel y las responsabilidades de los CISOs (Chief Information Security Officers o Directores de Seguridad de la Información) dentro de las organizaciones y cómo estos han evolucionado en los últimos años, destacando otros aspectos a considerar:

Aumento de la Responsabilidad Personal ya que los CISOs ahora enfrentan una mayor presión y responsabilidad.

Los **riesgos legales y regulatorios**, ya que a medida que crece la expectativa sobre la responsabilidad de los CISOs, también se observan casos donde estos ejecutivos son llevados a juicio por negligencia o comportamiento indebido.

Los CISOs deben **equilibrar la presión** para compartir información sobre ciberataques rápidamente, como lo requieren los organismos regulatorios, con el riesgo de ser penalizados si la información inicial resulta inexacta

Lo anterior crea una tensión entre cumplir con las expectativas regulatorias y proteger a la organización

[2] https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

Las Expectativas del rol del CISO

(IANS & ARTICO, 2024), manifiestan que las nuevas reglas cibernéticas respecto a los CISOs, apuntan a una nueva exposición legal y de responsabilidad y que la situación actual exige que estos expertos cumplan con requisitos de informes similares a los de un director financiero (CFO), pero a menudo sin la autoridad para firmar o la influencia general que posee un CFO.

The new expectations: **Arising from SEC rules and CISO accountability**	The current situation: **As reported by 660+ CISOs in the annual Comp and Budget survey**
The CISO to primarily serve as a **business risk function**, prioritizing business acumen over purely technical skills.	76% of CISOs come from a **mostly technical background**, where risk management is often secondary.
The CISO role as a **C-level position**, capable of bringing a clear voice into executive leadership meetings.	In 63% of cases, the **CISO role is a VP- or director-level position**. Just 20% of CISOs, and 15% of $1B+ company CISOs, are at the C-level.
CISOs have a **direct line of communication** with the CEO, C-suite and board, as well as the support of their leadership to get the resources they need.	90% of CISOs are at least two organizational levels removed from the CEO and just **50% of CISOs engage with their board quarterly**.

Recuperado de. https://cdn.iansresearch.com/Files/Marketing/2024/23-24StateoftheCISO_Summary.pdf

El cuadro anterior, compara las expectativas actuales con la situación real según encuestas a CISOs. Aunque la expectativa es que el CISO tenga un rol ejecutivo, la realidad muestra que muchos de estos profesionales aún operan en niveles jerárquicos más bajos y tienen dificultades para influir en las decisiones estratégicas.

En este sentido, el documento destaca cómo las nuevas reglas están cambiando las expectativas hacia el CISO, exigiendo un enfoque más centrado en la gestión de riesgos empresariales en lugar de solo habilidades técnicas y que este tenga un papel más estratégico y una comunicación directa con la alta dirección, similar a la de un CFO.

De la Teoría a la Práctica en la Gestión del Riesgo

Dada la sinergia del rol del CISO entre lo **técnico y lo estratégico**, es importante considerar acciones que permitan trabajar en conjunto en aras al mejoramiento de la postura de ciberseguridad de una organización. En este sentido, El CISO logra obtener victorias tempranas considerando:

El entendimiento del CISO por la comunicación del riesgo a la que está expuesto el negocio ha evolucionado más allá de lo técnico para convertirse en un líder enfocado en el riesgo de negocio. En lugar de centrarse exclusivamente en la tecnología, este rol debe presentar el riesgo cibernético en términos de impacto financiero y operacional.

Esto implica:

La traducción de vulnerabilidades técnicas en riesgos que afecten a la organización: El CISO debe poder explicar cómo las amenazas afectan directamente los objetivos estratégicos de la empresa.

La necesidad de una interacción frecuente entre el CISO y la alta dirección, ya que esto garantiza que las decisiones de seguridad estén alineadas con la tolerancia al riesgo de esta.

El CISO debe posicionarse como un líder estratégico, no solo como un experto técnico y para lograr esto, se deben tomar las siguientes acciones:

- Desarrollar Presencia Ejecutiva y Habilidades de Comunicación
- Alinear la Gestión de Riesgos con las Expectativas Regulatorias
- Adoptar una Visión Proactiva en la Gestión del Riesgo
- Preparar escenarios de Crisis
- Involucrar a lideres de todas las áreas de la organización

La gestión de riesgos no puede ser responsabilidad exclusiva del CISO

El Papel del CISO en el Desarrollo del Talento de CIberseguridad

(SANS, 2024) en su informe titulado *"SANS CISO Primer: 4 Cyber Trends That Will Move the Needle in 2024"*, se centra en las tendencias clave de ciberseguridad para 2024, destacando la influencia de la inteligencia artificial generativa y la importancia de la implementación de estrategias de confianza cero y como el CISO puede aportar en el fortalecimiento de la ciberseguridad en un entorno organizacional

- Los CISOs deben operar desde una perspectiva proactiva y calculada, enfrentando desafíos como el aumento de ataques y vulnerabilidades.
- Los CISOs deben desarrollar capacidades en sus equipos de ciberseguridad, asegurando que cuenten con la densidad de habilidades necesarias para implementar estrategias efectivas, como la confianza cero y la seguridad en la nube[3].
- Los CISOs deben participar en foros, redes y comunidades específicas de ciberseguridad lo cual les permita compartir lecciones aprendidas y mejorar la gestión de riesgos y resultados de seguridad.

Esto implica un enfoque colaborativo y la necesidad de integrar la seguridad en todas las áreas de la organización, promoviendo la capacitación continua y el desarrollo de habilidades específicas.

[3] https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Boletin/Junio_2024.pdf

Navegando en un Entorno de Amenazas en Evolución (Sinergia con los equipos de respuesta)

En el documento "***Developing a Cyber Incident Exercises Model to Educate Security Teams***"(Alothman et al., 2022), plantea un modelo educativo para la enseñanza de la ciberseguridad a través de entrenamiento práctico, utilizando plataformas como Q8CR y herramientas como Kali Linux, describiendo además, las funciones y responsabilidades de tres equipos en un entorno de entrenamiento de ciberseguridad:

Equipo Azul (Blue Team): Es el equipo defensivo que responde a los ataques del equipo rojo, enfocándose en la gestión de incidentes, evaluación de vulnerabilidades y configuración de seguridad.	**Equipo Negro (Black Team):** Se encarga de crear y evaluar escenarios para los equipos rojo y azul, gestionar cuentas de usuario, manejar problemas técnicos y evaluar el rendimiento de sus integrantes.	**Equipo Rojo (Red Team):** Es el equipo ofensivo que realiza ataques cibernéticos y pruebas de penetración contra el equipo azul, utilizando diversas técnicas como phishing y malware.

Así mismo, esta publicación, categoriza los escenarios de ataque cibernético en cuatro dominios (fraudes en línea, desfiguraciones web, ataques a redes y malware) y resalta la importancia de la práctica en la educación en ciberseguridad.

Aunque el documento no menciona específicamente al CISO, este rol, se enfoca en la importancia de la educación y el entrenamiento en ciberseguridad, lo que es relevante la gestión de la ciberseguridad dentro de una organización. Dado que este rol es el responsable de implementar políticas y estrategias de seguridad, lo cual se alinea con la necesidad de contar con equipos bien entrenados y preparados para enfrentar ciberataques, como se describe en el modelo educativo propuesto en el articulo

La siguiente tabla plantea algunas estrategias de educación que un CISO puede desarrollar con sus equipos de trabajo (red, blue, black).

Estrategia de Educación	Descripción	Ejemplo
Entrenamiento Basado en Escenarios Reales	Diseñar y simular ataques cibernéticos realistas en entornos controlados para poner a prueba las habilidades técnicas de los equipos de respuesta.	Simulación de un ataque de phishing dirigido para evaluar la capacidad de respuesta rápida.
Competencias de Ciberseguridad (CTF)	Realizar competencias tipo Capture The Flag (CTF) donde los equipos deben resolver desafíos específicos, fomentando el aprendizaje práctico y la colaboración.	Un desafío de penetración en un entorno aislado donde el equipo debe encontrar vulnerabilidades y explotar fallos.
Juegos de Guerra (Red Team vs. Blue Team)	Organizar ejercicios donde los equipos rojo y azul compiten, permitiendo a los participantes mejorar tanto en defensa como en ofensiva dentro de un entorno seguro.	El equipo azul defiende una red simulada mientras el equipo rojo lanza ataques coordinados.
Plataformas de Simulación de Incidentes	Utilizar plataformas que ofrecen ejercicios continuos de simulación de incidentes para mejorar la gestión de estos y optimizar la toma de decisiones en tiempo real.	Uso de plataformas para simular un incidente de ransomware y practicar la contención y recuperación.
Evaluaciones de Técnicas Cruzadas	Permitir que los equipos cambien temporalmente de rol (equipo rojo a equipo azul y viceversa) para entender las estrategias y desafíos de ambos enfoques.	Un miembro del equipo azul actúa como atacante para comprender mejor las técnicas ofensivas.

Conclusiones

En un entorno organizacional cada vez más complejo y dinámico, el rol del Chief Information Security Officer (CISO) ha evolucionado de manera significativa, pasando de ser un experto técnico en seguridad a un líder estratégico dentro de la alta dirección. La ciberseguridad, antes vista como una disciplina aislada, se ha convertido en un pilar fundamental para la sostenibilidad y éxito de las organizaciones modernas. En este contexto, el CISO es el encargado de integrar la seguridad con la gestión de riesgos empresariales, liderar la formación y desarrollo de equipos especializados y fomentar la resiliencia frente a amenazas cada vez más sofisticadas. A continuación, se presentan cinco conclusiones que resaltan la importancia y el impacto de este rol en la gestión integral de la seguridad y la continuidad del negocio.

- El rol del CISO va más allá de la protección técnica; su función es clave para integrar la ciberseguridad en la gestión de riesgos empresariales, alineando estrategias de seguridad con los objetivos de negocio y fomentando una cultura organizacional enfocada en la resiliencia cibernética.
- A medida que las amenazas se vuelven más complejas, las expectativas sobre el CISO han evolucionado, requiriendo que actúe no solo como un experto técnico, sino también como un líder estratégico con acceso directo a la alta dirección para asegurar la alineación de las decisiones de seguridad con los riesgos y objetivos empresariales.
- El CISO juega un papel crucial en el desarrollo y fortalecimiento de las capacidades de su equipo, asegurando que cuenten con las habilidades necesarias para enfrentar las amenazas emergentes, implementando estrategias como la confianza cero y fomentando un enfoque colaborativo en toda la organización.
- El CISO debe traducir las vulnerabilidades técnicas en términos de impacto financiero y operacional, permitiendo a la alta dirección comprender el riesgo cibernético en su contexto y tomar decisiones informadas. Esto refuerza la posición del CISO como un asesor clave en la toma de decisiones estratégicas.
- La colaboración entre los equipos Red, Blue y Black es esencial para la seguridad de la organización. El CISO tiene la responsabilidad de facilitar entrenamientos y simulaciones que preparen a la organización para enfrentar ataques cibernéticos, promoviendo un enfoque proactivo y fortaleciendo la capacidad de respuesta a incidentes.

Canales de comunicación

El CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:

- Correo: csirt@unad.edu.co
- Página web: https://csirt.unad.edu.co

Referentes Bibliograficos

Alothman, Alhajraf, Alajmi, Al Farraj, & Alshareef. (2022). *Developing a Cyber Incident Exercises Model to Educate Security Teams*. https://doi.org/10.3390/electronics11101575

Da Silva, Jensen, & Claims. (2022). *Cyber security is a dark art": The CISO as Soothsayer*. https://doi.org/10.1145/3555090

IANS, & ARTICO. (2024). *State of the CISO, 2023–2024—Benchmark Summary Report*. https://cdn.iansresearch.com/Files/Marketing/2024/23-24StateoftheCISO_Summary.pdf

Posada, J. (2014). *Ontología y Lenguaje de la Realidad Social*. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0717-554X2014000200003

SANS. (2024). *SANS CISO Primer: 4 Cyber Trends That Will Move the Needle in 2024*. https://www.sans.org/mlp/ciso-primer-2024/

World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf