

Capítulo 4

Articulación de la ciberseguridad y la ciberdefensa en la planeación estratégica de las organizaciones*

DOI: <https://doi.org/10.25062/9786287818002.04>

Lucas Adolfo Giraldo Ríos

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El capítulo aborda la integración estratégica de la ciberseguridad y la ciberdefensa como pilares esenciales para la protección de los activos digitales en un entorno empresarial digitalizado y amenazado. Destaca cómo han evolucionado las ciberamenazas y subraya la necesidad de adoptar medidas proactivas y reactivas para salvaguardar la confidencialidad, la integridad y la disponibilidad de la información. Se hace hincapié en la importancia de incorporar la ciberseguridad a la planificación estratégica, establecer políticas, asignar recursos y fomentar una cultura organizativa orientada a la seguridad. Además, el texto destaca el papel complementario de la ciberdefensa, que no solo responde a los ataques, sino que refuerza la resiliencia de las organizaciones, incorporando tecnologías avanzadas, formación continua y colaboración interinstitucional. Se concluye que la sinergia entre prevención, respuesta eficaz y resiliencia es crucial para hacer frente a las complejas ciberamenazas actuales porque garantiza la continuidad operativa y una ventaja competitiva sostenible.

Palabras clave: amenazas cibernéticas; ciberdefensa; ciberseguridad; confidencialidad; resiliencia organizacional; planeación estratégica.

* Capítulo de libro resultado del proyecto de investigación "Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales" del grupo de investigación "Ciberespacio Tecnología e Innovación", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen al autor y no reflejan necesariamente los de las instituciones participantes.

Lucas Adolfo Giraldo Ríos

Candidato a doctor en Ingeniería, Industria y Organizaciones, Universidad Nacional de Colombia. Magíster en Administración de Empresas de Base Tecnológica, Universidad Antonio de Nebrija, España. Magíster en Innovación, Universidad EAN, Colombia. Especialista en Gestión Financiera Empresarial, Universidad de Medellín, Colombia. Administrador de Empresas, Universidad de Antioquia, Colombia.

<https://orcid.org/0000-0002-9947-7882> - Contacto: lucas.giraldo@esdeg.edu.co

Citación APA: Giraldo Ríos, L. A. (2025). Articulación de la ciberseguridad y la ciberdefensa en la planeación estratégica de las organizaciones. En M. E. Realpe Díaz & G. A. Gómez Rodríguez (Eds.), *Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales* (pp. 119-156). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818002.04>

CIBERSEGURIDAD EN LA FRONTERA DIGITAL: DESAFÍOS Y OPORTUNIDADES EN LOS NUEVOS ECOSISTEMAS TECNOLÓGICOS EMPRESARIALES

ISBN impreso: 978-628-7602-99-1

ISBN digital: 978-628-7818-00-2

DOI: <https://doi.org/10.25062/9786287818002>

Colección Ciberseguridad y Ciberdefensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2025



Introducción

En la última década, el aumento exponencial de las amenazas cibernéticas ha puesto en primer plano la importancia de la ciberseguridad y la ciberdefensa en el ámbito empresarial. Las organizaciones ya no solo se enfrentan a problemas tradicionales de seguridad física, sino que deben adoptar un enfoque integral que aborde también la protección de sus activos digitales. Este enfoque es esencial, ya que un ciberataque puede comprometer no solo la información y los sistemas críticos de una empresa, sino también su reputación y su capacidad para operar de manera continua (Ramírez, 2024). Ante este panorama, las estrategias de ciberseguridad y ciberdefensa se han convertido en herramientas indispensables para garantizar la estabilidad y la protección de las organizaciones en el entorno digital.

La ciberseguridad, en su esencia, se enfoca en prevenir los posibles ataques mediante la implementación de medidas y controles que protejan los sistemas y la información. Estas medidas incluyen la protección de la confidencialidad, la integridad y la disponibilidad de la información, que son los pilares fundamentales de cualquier estrategia de seguridad. Sin embargo, con el aumento de la sofisticación de los ataques cibernéticos, la ciberdefensa ha emergido como un complemento esencial. La ciberdefensa no solo responde a los ataques una vez que han ocurrido, sino que también se encarga de mitigar sus efectos y garantizar la recuperación rápida de las operaciones (Rincón-Gallón, 2022).

En este contexto, la colaboración interna dentro de las organizaciones y la cooperación externa con entidades gubernamentales y organismos internacionales son elementos cruciales para una ciberdefensa eficaz. Las empresas deben trabajar de la mano con el sector público y otros actores clave para intercambiar información sobre amenazas emergentes y aprender de las mejores prácticas en

el campo de la seguridad cibernética. La falta de una estrategia de ciberdefensa coordinada y global puede dejar a las organizaciones vulnerables a ataques devastadores que comprometan no solo sus datos, sino también su capacidad operativa (Guzmán-Pacheco, 2022).

A medida que las organizaciones dependen cada vez más de la tecnología para sus operaciones diarias, la integración de la ciberseguridad y la ciberdefensa en la planeación estratégica se vuelve más importante que nunca. La protección de los activos digitales ya no puede ser vista como una cuestión técnica aislada, sino como un componente clave de la estrategia empresarial general. En este sentido, aquellas organizaciones que logren implementar medidas proactivas y reactivas de ciberdefensa estarán mejor posicionadas para enfrentar los desafíos del entorno cibernético actual y para garantizar la continuidad de sus operaciones en un mundo cada vez más digital (Valderrama, 2024).

Importancia de la ciberseguridad y la ciberdefensa

La ciberseguridad y la ciberdefensa se han convertido en elementos fundamentales para la protección de los activos digitales de las organizaciones debido al crecimiento exponencial de las amenazas cibernéticas en la última década (Ramírez, 2024). Hoy en día, las empresas enfrentan riesgos que van más allá de los problemas tradicionales de seguridad física, lo cual las obliga a adoptar un enfoque proactivo y preventivo frente a posibles ataques. Además, el enfoque estratégico que integra estas disciplinas resulta clave para la continuidad operativa y la protección de los datos tanto propios como de los clientes.

Confidencialidad de la información

La confidencialidad de la información se ha posicionado como uno de los pilares fundamentales dentro de la ciberseguridad, ya que los datos representan activos de gran valor para las organizaciones. En la era digital, la mayor parte de las operaciones de las empresas depende de la recolección, procesamiento y almacenamiento de información sensible. Esta puede abarcar desde datos financieros hasta información personal de los clientes y otros detalles estratégicos relacionados con la operación diaria de la organización (Rincón-Gallón, 2022).

Relevancia de la confidencialidad

La protección de la confidencialidad de la información no solo es esencial para evitar filtraciones, sino que también asegura la integridad de la relación con los clientes, socios comerciales y otros actores involucrados en la cadena de valor de la organización. La pérdida de confidencialidad puede tener efectos devastadores no solo en términos económicos, sino también en la percepción pública y la reputación organizacional. Un fallo en esta área podría generar desconfianza en los servicios de una empresa, lo que a largo plazo afectaría su competitividad en el mercado.

Según Guzmán-Pacheco (2022), cualquier acceso no autorizado a información confidencial puede causar graves daños, tanto financieros como reputacionales. Por ejemplo, una violación de datos podría exponer detalles sensibles, como números de tarjetas de crédito o información de cuentas bancarias, lo que podría llevar a multas regulatorias, acciones legales por parte de los clientes afectados y una pérdida de confianza en la marca.

Ejemplos de violaciones de confidencialidad

Uno de los casos más emblemáticos de violación de confidencialidad ocurrió en Yahoo entre 2013 y 2014, cuando la empresa sufrió una filtración masiva que afectó a más de tres mil millones de cuentas de usuario. Esta violación no solo comprometió la información personal de los usuarios, sino que también impactó negativamente la confianza en los servicios de la empresa. Como resultado, Yahoo se vio forzada a reducir significativamente el precio de su venta a Verizon, con lo cual perdió aproximadamente 350 millones de dólares en valor de la transacción (Guzmán-Pacheco, 2022).

Este caso subraya el impacto de una falla en la protección de la confidencialidad, que no solo afecta las finanzas de la empresa directamente, sino también su valor de mercado y su posición competitiva a largo plazo. Yahoo, una de las compañías pioneras de internet, nunca pudo recuperarse del golpe reputacional causado por este incidente, lo que la debilitó frente a sus competidores.

Otro ejemplo relevante fue la violación de datos que sufrió Equifax en 2017, la cual comprometió la información personal de más de 147 millones de consumidores, incluyendo números de la seguridad social, fechas de nacimiento y direcciones. Este incidente no solo expuso a los consumidores al fraude y robo de identidad, sino que también condujo a sanciones económicas para Equifax y a una demanda colectiva, lo que subraya las posibles consecuencias legales y financieras de la pérdida de confidencialidad (Rutz, 2021).

Implicaciones legales y regulatorias

Las regulaciones sobre protección de datos, como el Reglamento General de Protección de Datos (GDPR) en Europa y la Ley de Privacidad del Consumidor de California (CCPA) en los Estados Unidos, establecen sanciones significativas para las organizaciones que no protejan adecuadamente la confidencialidad de la información de sus usuarios. Estas normativas no solo buscan proteger a los consumidores, sino también garantizar que las empresas adopten las mejores prácticas en cuanto a la ciberseguridad y la gestión de la información (Pereyra, 2021).

El incumplimiento de estas regulaciones puede resultar en multas millonarias y restricciones adicionales sobre las operaciones de la empresa. Por ejemplo, según el GDPR, las multas pueden alcanzar hasta el 4 % de la facturación anual global de la compañía o veinte millones de euros, lo que sea mayor. Esto resalta la importancia de adoptar un enfoque preventivo y garantizar que todas las medidas necesarias estén en su lugar para evitar violaciones de la confidencialidad.

Medidas preventivas para garantizar la confidencialidad

La protección de la confidencialidad de la información no solo depende de la implementación de tecnología avanzada, sino también de un enfoque integral que incluya políticas claras, procedimientos operativos y la capacitación del personal (Sánchez, 2023). Algunas de las principales medidas preventivas incluyen:

1. *Cifrado de datos*: el uso de técnicas avanzadas de cifrado asegura que, incluso si los datos son interceptados, no puedan ser leídos sin la clave adecuada. El cifrado debe aplicarse tanto a los datos en tránsito como a los datos en reposo.
2. *Gestión de accesos*: implementar políticas de control de acceso que limiten quién puede ver o modificar información confidencial es clave para reducir el riesgo de accesos no autorizados. Esto incluye la autenticación multifactor y el uso de privilegios mínimos.
3. *Auditorías de seguridad*: realizar auditorías regulares para identificar posibles vulnerabilidades en los sistemas de seguridad y corregirlas antes de que puedan ser explotadas. Esto también implica pruebas de penetración y simulaciones de ataques.
4. *Capacitación continua*: capacitar al personal sobre las mejores prácticas en el manejo de información confidencial y sensibilizarlo sobre la importancia de la ciberseguridad en su día a día.

5. *Políticas claras de confidencialidad*: desarrollar y comunicar políticas de confidencialidad que definan claramente cómo se maneja y protege la información sensible en la organización.

Integridad de los datos

La integridad de los datos es uno de los pilares fundamentales de la ciberseguridad y está directamente relacionada con la calidad, la precisión y la fiabilidad de la información. Garantizar que los datos no sean manipulados, alterados o destruidos de manera no autorizada es crucial para asegurar que las organizaciones puedan operar con confianza y tomar decisiones informadas basadas en información correcta (Valderrama, 2024). Sin integridad, la información pierde su valor, ya que no se puede confiar en que sea precisa o representativa de la realidad.

Importancia de la integridad de los datos

En el contexto de las operaciones empresariales, la integridad de los datos tiene un impacto directo en la toma de decisiones y en las relaciones con clientes, socios y proveedores. La alteración de datos, ya sea por acción maliciosa o por error humano, puede tener repercusiones significativas en la credibilidad de una organización. Esto se debe a que la información que se utiliza para tomar decisiones estratégicas o para interactuar con terceros debe ser exacta y fiable. Si los datos son manipulados o corrompidos, la empresa corre el riesgo de tomar decisiones equivocadas, lo que podría generar pérdidas económicas o dañar su reputación (Muñoz-Zambrano & Zambrano-Rendón, 2023).

Un ejemplo clásico de la importancia de la integridad de los datos es el uso de bases de datos en el sector financiero. Las transacciones, los balances y la información contable deben ser exactos y no estar sujetos a cambios no autorizados. Cualquier alteración en estos datos podría afectar la credibilidad financiera de la empresa y generar multas regulatorias o pérdidas financieras. En sectores altamente regulados, como la banca, incluso una pequeña alteración de datos puede tener consecuencias legales graves.

Ataques que comprometen la integridad

Uno de los tipos de ataques más dañinos para la integridad de los datos es la manipulación deliberada de la información. Los atacantes pueden infiltrarse en los sistemas para alterar registros críticos, modificar transacciones financieras o incluso alterar datos sensibles relacionados con operaciones o clientes. Estos ataques no solo afectan la precisión de los datos, sino que pueden tener un efecto

dominó en otros aspectos de la ciberseguridad, como la confidencialidad y la disponibilidad de la información.

Un ejemplo significativo de un ataque que comprometió la integridad de los datos fue el incidente de la cadena de suministro de SolarWinds en 2020. Durante este ataque, los hackers lograron insertar código malicioso en las actualizaciones del software de gestión de red de SolarWinds, lo cual permitió a los atacantes obtener acceso no autorizado a redes gubernamentales y corporativas en todo el mundo. Este ataque no solo comprometió la confidencialidad de los datos, sino que también planteó serias preocupaciones sobre la integridad de la información procesada por las entidades afectadas (Muñoz-Zambrano & Zambrano-Rendón, 2023).

El ataque a SolarWinds destacó la vulnerabilidad de los sistemas críticos y la necesidad de implementar medidas de protección robustas para garantizar la integridad de los datos. La manipulación del código fuente de las actualizaciones no solo comprometió a SolarWinds, sino que también afectó a miles de sus clientes, que confiaban en que el software que recibían no había sido alterado. Este tipo de violaciones puede tener efectos catastróficos, ya que los datos corruptos pueden propagarse a través de sistemas interconectados y afectar múltiples capas de una infraestructura tecnológica.

Consecuencias de la pérdida de integridad

La pérdida de integridad de los datos puede tener consecuencias devastadoras para las organizaciones. En primer lugar, los datos alterados pueden llevar a decisiones erróneas que afecten tanto a la estrategia empresarial como a las operaciones diarias. Por ejemplo, en el ámbito de la manufactura, si los datos sobre la producción o los inventarios son manipulados, las empresas podrían enfrentarse a problemas de suministro, interrupciones en la cadena de valor y pérdidas financieras.

En segundo lugar, la manipulación de datos puede erosionar la confianza entre la organización y sus clientes, socios comerciales y reguladores. En sectores como el de la salud, por ejemplo, la alteración de los datos de los pacientes puede tener implicaciones legales y éticas. La falta de integridad en los registros de salud podría poner en riesgo la vida de los pacientes y exponer a las organizaciones a demandas por negligencia (Valderrama, 2024).

Mejores prácticas para garantizar la integridad de los datos

Para evitar la manipulación o alteración no autorizada de los datos, las organizaciones deben implementar una serie de medidas y prácticas de seguridad que protejan la integridad de su información. La tabla 1 presenta un conjunto de prácticas

de seguridad cibernética que son clave para garantizar la integridad de los datos dentro de una organización, las cuales se centran en proteger los datos contra accesos no autorizados, alteraciones y manipulaciones que podrían comprometer la confiabilidad y precisión de la información. Cada una está acompañada de una descripción, los elementos esenciales que la componen, y referencias bibliográficas en formato APA para ofrecer una visión completa y respaldada sobre su implementación. Cabe señalar que estas herramientas son fundamentales para mantener la integridad de los datos y asegurar que la información se mantenga exacta y confiable en todo momento dentro del entorno empresarial.

Tabla 1. Medidas clave para garantizar la integridad de los datos dentro de una organización

| Medida de seguridad | Descripción | Elementos clave | Referencias |
|---|--|---|--|
| Control de acceso basado en roles (RBAC) | Limitar el acceso a los datos a los empleados que lo necesiten para cumplir con sus funciones. De esta manera se previene que personas no autorizadas modifiquen los datos. | Roles bien definidos, autenticación, permisos basados en funciones y gestión de privilegios. | Valderrama (2024). |
| Cifrado de datos | El cifrado asegura que los datos, tanto en tránsito como en reposo, no puedan ser alterados sin la clave adecuada, con lo cual se protege la integridad en caso de interceptación. | Claves de cifrado, algoritmos de cifrado, cifrado de datos en tránsito y en reposo, y gestión de claves. | Sánchez (2023). |
| Registros de auditoría y control | Mantener un registro detallado de todas las interacciones con los datos para detectar intentos de manipulación. Esto permite rastrear accesos y modificaciones realizadas. | Registro de eventos, auditorías de seguridad, control de acceso y rastreo de actividades sospechosas. | Muñoz-Zambrano & Zambrano-Rendón (2023). |
| Integridad de los datos mediante firmas digitales | Las firmas digitales y algoritmos hash verifican que los datos no han sido alterados desde su creación, validando su autenticidad y detectando cualquier modificación. | Firmas digitales, algoritmos hash, verificación de autenticidad y detección de modificaciones no autorizadas. | Valderrama (2024). |
| Pruebas de integridad periódicas | Realizar pruebas periódicas para identificar vulnerabilidades antes de que sean explotadas. Incluye simulaciones de ataques y revisiones de los procedimientos. | Simulacros de ataques, pruebas de penetración, revisiones de políticas y simulaciones de incidentes de seguridad. | Muñoz-Zambrano & Zambrano-Rendón (2023). |

Fuente: Elaboración propia

Disponibilidad de la información

La disponibilidad de la información es un aspecto crítico dentro de la ciberseguridad, ya que asegura que los sistemas y servicios estén accesibles cuando los usuarios los necesiten. En el mundo empresarial moderno, la dependencia de sistemas digitales para gestionar operaciones clave ha crecido exponencialmente, lo que significa que cualquier interrupción puede tener consecuencias devastadoras para la continuidad del negocio. Por lo tanto, garantizar la disponibilidad de la información es tan importante como proteger la confidencialidad e integridad de los datos (Muñoz-Zambrano & Zambrano-Rendón, 2023).

Importancia de la disponibilidad

La disponibilidad de los sistemas es fundamental para el funcionamiento diario de una organización. Un fallo en la disponibilidad de los sistemas críticos puede paralizar operaciones clave, interrumpir servicios, afectar las cadenas de suministro o incluso llevar a la pérdida de clientes y reputación. Las organizaciones deben asegurar que los sistemas estén disponibles 24/7, ya que cualquier tiempo de inactividad puede traducirse en pérdidas financieras significativas, particularmente en sectores como la banca, la salud o el comercio electrónico, donde los servicios en línea son esenciales para la operación.

Un concepto importante vinculado a la disponibilidad es el "tiempo de actividad" (*uptime*), que se refiere a la cantidad de tiempo en que un sistema está operativo y disponible para los usuarios. Las organizaciones buscan mantener el mayor tiempo de actividad posible, y las interrupciones del servicio pueden ser perjudiciales. Por ejemplo, si una tienda en línea experimenta una interrupción durante una gran venta o un evento promocional, puede perder millones en ingresos debido a la imposibilidad que tendrían los clientes de realizar transacciones (Rutz, 2021).

Uno de los mayores desafíos para la disponibilidad de la información son los ataques de Denegación de Servicio (DoS) y Denegación de Servicio Distribuida (DDoS). Estos ataques intentan sobrecargar los servidores de una organización con un volumen masivo de tráfico falso, haciendo que los sistemas no puedan gestionar las solicitudes legítimas de los usuarios. Los ataques DDoS pueden derribar sitios web, interrumpir servicios en línea y afectar la capacidad de una empresa para operar de manera normal.

Un ataque emblemático de DDoS ocurrió en 2016, cuando los hackers afectaron al proveedor de DNS Dyn. Esto perjudicó a empresas importantes como Twitter, Spotify y Reddit, pues interrumpió sus servicios y causó inconvenientes a millones

de usuarios en todo el mundo. Al explotar las vulnerabilidades en la infraestructura de DNS, los hackers demostraron lo fácil que es para un ataque masivo incidir en múltiples empresas dependientes de un mismo servicio (Casale, 2022). Este suceso subraya la importancia de proteger los sistemas críticos de las organizaciones y de diseñar infraestructuras que puedan resistir ataques de este tipo.

Otra amenaza creciente que afecta la disponibilidad es el *ransomware*, donde los hackers cifran los sistemas de la organización para impedir el acceso a los datos y solicitar un rescate para restaurar la funcionalidad. Este tipo de ataque puede ser igualmente destructivo, ya que impide a las empresas operar hasta que se resuelva el problema, lo cual genera tiempos de inactividad prolongados y pérdidas de ingresos.

La ciberdefensa como complemento a la ciberseguridad

La ciberdefensa, a diferencia de la ciberseguridad, se centra principalmente en las estrategias reactivas para mitigar los efectos de un ataque cibernético que ha tenido éxito en superar las barreras preventivas establecidas. Mientras que la ciberseguridad engloba las medidas preventivas que buscan proteger los sistemas informáticos y las redes de posibles intrusiones y vulnerabilidades, la ciberdefensa se activa una vez que las amenazas han logrado penetrar en los sistemas. En este sentido, la ciberdefensa puede considerarse una respuesta complementaria y necesaria a los fallos que puedan producirse en las estrategias de ciberseguridad (Casale, 2022).

Una de las claves de la ciberdefensa es la capacidad de las organizaciones para detectar rápidamente las amenazas y actuar de forma coordinada para contener y mitigar los daños. Esto requiere la implementación de un plan de respuesta a incidentes bien estructurado, que cubra todos los aspectos del ataque, desde la detección temprana hasta la contención, el análisis forense y la recuperación de los sistemas afectados. La preparación de estos planes debe basarse en la evaluación continua de los riesgos y la simulación de ataques potenciales, de modo que las organizaciones puedan reaccionar con rapidez y eficacia cuando ocurra un incidente real (Fernández, 2023).

En la actualidad, la ciberdefensa ha ganado una relevancia crítica, especialmente en un entorno global donde los ataques a infraestructuras críticas y sistemas gubernamentales se han vuelto más frecuentes. Los ataques cibernéticos no solo afectan a las organizaciones privadas, sino que también ponen en riesgo la seguridad nacional de los países, ya que pueden tener como objetivo sectores clave como la energía, las telecomunicaciones o los sistemas financieros. Como

resultado, la ciberdefensa ha dejado de ser un aspecto meramente técnico y se ha convertido en un tema de importancia estratégica para los gobiernos y las empresas a nivel mundial (González, 2020).

Un componente fundamental de la ciberdefensa es la cooperación internacional. Los ciberataques, debido a su naturaleza transnacional, requieren respuestas coordinadas entre diferentes países y organizaciones. Esto ha llevado al establecimiento de redes internacionales de colaboración, donde los Estados comparten información sobre amenazas, vulnerabilidades y soluciones para mitigar los daños de los ataques. Un ejemplo de ello es la creación de equipos de respuesta a incidentes de seguridad informática (CERT, por sus siglas en inglés), que funcionan tanto a nivel nacional como internacional para ofrecer asistencia técnica y coordinar esfuerzos ante ciberataques de gran magnitud (UNIDIR, 2022).

El ataque Stuxnet, ocurrido en 2010, se ha convertido en un caso paradigmático de cómo la ciberdefensa puede tener un papel crucial en la mitigación de los daños causados por un ciberataque. Stuxnet, un gusano informático sofisticado que fue diseñado para sabotear las centrifugadoras de enriquecimiento de uranio en Irán, demostró la vulnerabilidad de las infraestructuras críticas ante ataques cibernéticos avanzados. Sin embargo, la respuesta del gobierno iraní y la comunidad internacional resaltó la importancia de contar con sistemas robustos de ciberdefensa. A pesar de los daños iniciales, las medidas adoptadas para contener el ataque, analizar su origen y fortalecer las defensas fueron clave para prevenir que Stuxnet lograra su objetivo a mayor escala (Sandoval, 2022).

Otro caso notable es el ataque a la infraestructura energética de Ucrania en 2015, donde un grupo de cibercriminales logró penetrar en las redes de distribución eléctrica y provocar un apagón masivo. La respuesta de Ucrania incluyó no solo la restauración de los sistemas afectados, sino también la implementación de nuevas medidas de ciberdefensa que buscaron proteger sus redes eléctricas de futuros ataques similares. Como en el caso anterior, este evento subrayó la importancia de contar con una ciberdefensa resiliente, que no solo se basa en la capacidad de reaccionar ante ataques, sino también en la adaptación y mejora continua de las defensas ante la evolución de las amenazas (Rodríguez, 2021).

La ciberdefensa, por tanto, no es solo un conjunto de acciones reactivas, sino también un proceso continuo de aprendizaje y adaptación. Las organizaciones deben realizar análisis forenses detallados después de cada incidente para comprender cómo los atacantes lograron penetrar en sus sistemas y qué vulnerabilidades fueron explotadas. Estos conocimientos permiten reforzar las barreras de

ciberseguridad existentes y desarrollar nuevas estrategias de ciberdefensa más efectivas para el futuro (Valencia, 2023).

Asimismo, es importante destacar el papel del sector privado en la ciberdefensa. Dado que gran parte de las infraestructuras críticas y los sistemas digitales están gestionados por empresas privadas, estas tienen un papel esencial en la protección del ciberespacio. En este sentido, el apoyo entre el sector público y el privado es fundamental para garantizar una ciberdefensa sólida y coordinada. Las empresas deben colaborar estrechamente con las agencias gubernamentales para compartir información sobre amenazas emergentes y participar en ejercicios de ciberseguridad que simulen ataques reales y mejoren la preparación colectiva (Nolasco-Mamani et al., 2022).

Por lo anterior, la ciberdefensa complementa a la ciberseguridad al proporcionar las herramientas y estrategias necesarias para reaccionar ante los ciberataques que logran superar las barreras preventivas. La cooperación internacional, la participación del sector privado y la mejora continua de las capacidades defensivas son aspectos clave para enfrentar los desafíos que presenta el panorama actual de ciberseguridad (Casale, 2022).

Resiliencia organizacional

En el entorno actual de crecientes amenazas cibernéticas, uno de los conceptos más importantes en la gestión de la seguridad de la información es la *resiliencia organizacional*. La resiliencia se refiere a la capacidad de una organización para no solo prevenir ataques cibernéticos, sino también para recuperarse de ellos de manera rápida y efectiva, de tal manera que se asegure la continuidad operativa. En términos más generales, la resiliencia organizacional implica la preparación y la capacidad de una empresa para adaptarse a las interrupciones, restaurar las funciones críticas y mitigar el impacto de los incidentes en su infraestructura tecnológica y en sus operaciones comerciales (Carreño & López, 2022).

La resiliencia no debe confundirse con la mera reacción ante un ataque. Va más allá, ya que abarca una estrategia integral que incluye la *gestión de riesgos*, el *fortalecimiento de la infraestructura tecnológica* y la *planificación ante desastres*. Las organizaciones resilientes son aquellas que, además de contar con sistemas de defensa robustos, disponen de planes de respuesta y recuperación bien definidos. Estos planes se diseñan con antelación y deben estar sujetos a revisiones periódicas para asegurar que son efectivos ante las amenazas emergentes. En este sentido, la *cultura de la resiliencia* es fundamental para las organizaciones

modernas, ya que les permite anticiparse a posibles interrupciones, recuperarse de manera eficiente y, por lo tanto, minimizar las pérdidas financieras, operativas y reputacionales (Carlini, 2016).

Un aspecto central de la resiliencia organizacional es la implementación de *planes de recuperación ante desastres* (Disaster Recovery Plans [DRP]) y *planes de continuidad del negocio* (Business Continuity Plans [BCP]). Estos planes proporcionan un marco para que las organizaciones puedan operar durante y después de una crisis, de tal manera que permiten restaurar las funciones críticas en el menor tiempo posible. El BCP, por ejemplo, detalla los pasos que debe seguir una empresa para mantener operaciones esenciales en caso de una interrupción, mientras que el DRP se enfoca más específicamente en los procesos de TI, asegurando que los datos y sistemas puedan recuperarse después de un ataque o fallo técnico (Serrano, 2022).

La *resiliencia tecnológica* también desempeña un papel crucial en este proceso. A medida que las organizaciones dependen cada vez más de la tecnología para sus operaciones, garantizar la solidez y flexibilidad de sus infraestructuras tecnológicas es esencial. Esto incluye la adopción de soluciones en la nube, la creación de copias de seguridad automatizadas, la implementación de sistemas redundantes y la utilización de tecnologías avanzadas de *detección y respuesta ante amenazas*. Todo esto, combinado con una capacitación continua del personal, asegura que las organizaciones puedan no solo sobrevivir a los ataques, sino también adaptarse rápidamente a las condiciones cambiantes (Pacheco-Mangas et al., 2021).

Un ejemplo destacado de resiliencia organizacional es la respuesta del Servicio Nacional de Salud (NHS) del Reino Unido al ataque de *ransomware* WannaCry en 2017. Se trató de uno de los incidentes más grandes de *ransomware* hasta la fecha, pues afectó a miles de sistemas en más de 150 países, incluyendo a muchas organizaciones del sector salud. En el caso del NHS, aunque el ataque causó el cierre de varios hospitales y clínicas —lo cual interrumpió los servicios médicos esenciales—, gracias a la implementación de un plan de resiliencia organizacional sólido, que incluía medidas preventivas y de recuperación, el NHS logró restaurar la mayor parte de sus operaciones en un tiempo relativamente corto. Este caso demostró la importancia de estar preparados no solo para defenderse de ataques, sino también para recuperarse de ellos con rapidez (Sánchez, 2023).

La respuesta del NHS incluyó no solo la restauración de los sistemas afectados, sino también un análisis exhaustivo de las vulnerabilidades explotadas por el ataque. Este enfoque le permitió implementar nuevas medidas de seguridad,

como actualizar sistemas obsoletos y mejorar las defensas cibernéticas. Además, el ataque WannaCry subrayó la importancia de la *resiliencia proactiva*, en la cual las organizaciones no solo se centran en recuperarse, sino también en aprender de los incidentes para prevenir futuros ataques. Este enfoque incluye la actualización constante de los sistemas, la realización de simulacros regulares y la capacitación continua de los empleados para identificar y responder a las amenazas de manera más eficaz (Akbanov et al., 2019)

Además, la *resiliencia organizacional* implica una gestión efectiva de la cadena de suministro y las relaciones con terceros. En el caso de muchas organizaciones, una interrupción en los servicios que prestan proveedores externos puede tener un efecto dominó que afecte la capacidad de la empresa para operar de manera efectiva. Por lo tanto, es fundamental que las organizaciones desarrollen relaciones sólidas con sus proveedores, asegurando que también cuenten con estrategias de resiliencia que puedan complementar las propias de la organización (Ruiz, 2022).

Elementos propios de la ciberresiliencia

La ciberresiliencia es un concepto clave en la estrategia de seguridad de las organizaciones modernas, ya que les permite no solo resistir ataques cibernéticos, sino también recuperarse rápidamente y garantizar la continuidad operativa. En este sentido, la implementación de diversas variables es esencial para fortalecer la capacidad de respuesta y minimizar el impacto de incidentes cibernéticos. La tabla 2 desglosa las principales variables que se deben considerar en la ciberresiliencia y describe sus características, elementos esenciales, condiciones de cumplimiento, riesgos asociados a su omisión y las referencias bibliográficas correspondientes. Este enfoque integral proporciona una guía práctica para las empresas que buscan mejorar su preparación ante posibles amenazas cibernéticas.

Tabla 2. Desglose de las principales variables a considerar en la ciberresiliencia

| Variables que se deben tener en cuenta en la ciberresiliencia | Descripción de la variable | Elementos a tener en cuenta | Condiciones de cumplimiento en la empresa | Riesgos de no tenerla en cuenta en una empresa | Referencias |
|---|--|---|---|--|-----------------|
| Plan de continuidad del negocio (BCP) | Proceso que garantiza la continuidad de las operaciones durante y después de un incidente. | Identificación de funciones críticas, responsables y procesos alternativos. | El plan está documentado, probado regularmente y actualizado. | Pérdida de operaciones esenciales y caos organizacional. | Serrano (2022). |

| Variables que se deben tener en cuenta en la ciberresiliencia | Descripción de la variable | Elementos a tener en cuenta | Condiciones de cumplimiento en la empresa | Riesgos de no tenerla en cuenta en una empresa | Referencias |
|--|---|---|--|--|-------------------------------|
| Plan de recuperación ante desastres (DRP) | Estrategia para recuperar sistemas y datos después de un desastre cibernético o físico. | Identificación de tecnologías críticas, plan de copias de seguridad y responsables de tecnologías de la información (TI). | El plan incluye recuperación de datos y redundancia en sistemas clave. | Pérdida de datos críticos e incapacidad de reanudar operaciones. | Carlini (2016). |
| Cultura de ciberseguridad | Nivel de conciencia y responsabilidad cibernética dentro de la organización. | Capacitación continua, políticas claras y comportamiento proactivo en ciberseguridad. | Empleados capacitados en identificar y prevenir amenazas cibernéticas. | Incremento de vulnerabilidades por errores humanos. | Carreño & López (2022). |
| Colaboración con terceros | Coordinación con proveedores y socios externos para garantizar la resiliencia en la cadena de suministro. | Asegurar que los proveedores tengan BCP y DRP adecuados, así como hacer evaluación de riesgos de terceros. | Contratos actualizados y auditorías periódicas a terceros. | Brechas de seguridad en proveedores e interrupciones en la cadena de suministro. | Ruiz (2022). |
| Infraestructura tecnológica redundante | Mecanismos de respaldo para garantizar el funcionamiento continuo de los sistemas críticos. | Implementación de sistemas de respaldo, almacenamiento en la nube, redundancia de servidores. | Sistemas de respaldo disponibles y probados regularmente. | Interrupción prolongada de servicios y pérdida de datos. | Pacheco-Mangas et al. (2021). |
| Evaluación de riesgos cibernéticos | Análisis de las amenazas y vulnerabilidades que pueden afectar a la organización. | Identificación y clasificación de riesgos y medidas de mitigación. | Análisis regular de riesgos y actualización de políticas. | Falta de preparación ante amenazas emergentes. | (Akbanov et al., 2019) |

| Variables que se deben tener en cuenta en la ciberresiliencia | Descripción de la variable | Elementos a tener en cuenta | Condiciones de cumplimiento en la empresa | Riesgos de no tenerla en cuenta en una empresa | Referencias |
|--|---|--|---|--|--------------------|
| Respuesta ante incidentes | Proceso de manejo y mitigación de incidentes cibernéticos para limitar su impacto. | Equipos de respuesta a incidentes, notificación y contención rápida. | Equipos entrenados y protocolos de respuesta establecidos. | Retraso en la respuesta que agrava los daños y las pérdidas. | Sánchez (2023). |
| Simulacros y ejercicios de ciberseguridad | Pruebas periódicas que simulan incidentes cibernéticos para evaluar la preparación. | Simulacros de ataques, revisión de tiempos de respuesta y efectividad. | Realización de simulacros anuales y revisión de resultados. | Falta de preparación ante incidentes reales. | Serrano (2022). |

Fuente: Elaboración propia

El concepto de resiliencia organizacional ha cobrado relevancia a nivel internacional como respuesta al incremento de ciberataques. Por ejemplo, países como Estonia, tras el ataque cibernético masivo en 2007, reformularon su política nacional de seguridad para incluir la ciberdefensa como pilar estratégico, para lo cual establecieron el Centro de Excelencia en Ciberdefensa Cooperativa de la OTAN en Tallin (Organización del Tratado del Atlántico Norte [OTAN], 2021).

En el ámbito nacional, Colombia ha adoptado un enfoque de ciberresiliencia que vincula al sector defensa, al sector productivo y a la ciudadanía, integrando esfuerzos bajo el marco de la Política Nacional de Seguridad Digital. Esta estrategia ha sido clave para fortalecer la protección de infraestructuras críticas, como el sector eléctrico, el bancario y las telecomunicaciones (MinTIC, 2021).

Por su parte, la experiencia del Reino Unido, con su Centro Nacional de Ciberseguridad (NCSC), es otro referente importante. Esta entidad opera con un modelo de colaboración con empresas privadas, universidades y agencias estatales que promueve campañas educativas, análisis de amenazas y mecanismos de respuesta unificados (UK NCSC, 2020).

En el contexto latinoamericano, México ha formulado la Estrategia Nacional de Ciberseguridad, que enfatiza la protección de infraestructuras críticas, la educación en ciberseguridad y el fomento a la cooperación internacional. Uno de sus mayores avances ha sido el desarrollo de capacidades técnicas en las fuerzas armadas para responder ante amenazas de ciberespionaje y sabotaje digital (OCDE, 2020).

Asimismo, Israel considera la ciberseguridad un asunto de seguridad nacional, de manera que ha integrado capacidades ofensivas y defensivas dentro de su doctrina de defensa. De esta manera, combina vigilancia activa, inversión en *start ups* de ciberseguridad y formación intensiva de talento desde edades tempranas. Cabe señalar que esta visión holística lo ha posicionado como un referente mundial en ciberdefensa (Kaplan & Cohen, 2022).

Estos casos permiten observar cómo distintas naciones han articulado institucionalmente la ciberseguridad y la ciberdefensa con su planeación estratégica. En este sentido, su análisis proporciona insumos valiosos para que las organizaciones diseñen sus propios marcos de actuación, alineados con las mejores prácticas internacionales (Sánchez & Morales, 2022).

Integración de la ciberseguridad en la planeación estratégica

Integrar la ciberseguridad en la planificación estratégica es crucial para garantizar que los activos digitales estén protegidos y las operaciones comerciales puedan continuar sin interrupciones. Específicamente, este proceso debe comenzar con una evaluación exhaustiva de los riesgos cibernéticos, lo cual permite a las organizaciones identificar vulnerabilidades y diseñar medidas para mitigarlas (Muñoz-Zambrano & Zambrano-Rendón, 2023).

El primer paso es identificar los activos más críticos para la organización. Estos pueden incluir bases de datos de clientes, sistemas de gestión financiera, infraestructura de TI y cualquier otro recurso digital esencial para las operaciones. Una vez identificados, se deben evaluar los riesgos específicos asociados a cada uno.

Esta evaluación de riesgos implica no solo identificar amenazas, sino también determinar el impacto que un ataque podría tener en la organización. Este proceso debe realizarse de manera periódica, ya que el entorno cibernético es dinámico y las amenazas evolucionan constantemente. Al realizar evaluaciones regulares, las organizaciones pueden ajustar sus estrategias de ciberseguridad para enfrentar nuevas vulnerabilidades (Guzmán-Pacheco, 2022).

Tras evaluar los riesgos, es necesario diseñar e implementar medidas preventivas que garanticen la protección de los activos digitales, las cuales pueden incluir la implementación de *firewalls*, sistemas de detección de intrusiones, cifrado de datos y controles de acceso. Sin embargo, es importante destacar que la tecnología por sí sola no es suficiente, pues también se deben establecer políticas

y procedimientos que regulen el uso seguro de los sistemas de información (Valderrama, 2024).

La creación de políticas de ciberseguridad debe ser un esfuerzo colaborativo entre el departamento de TI y otras áreas de la organización. Las políticas deben abarcar temas como el acceso a sistemas de información, la gestión de contraseñas y la respuesta ante incidentes de seguridad. Además, deben alinearse con las normativas y regulaciones aplicables, garantizando el cumplimiento legal en materia de protección de datos y seguridad cibernética (Rincón-Gallón, 2022).

Es esencial que estas políticas no solo se implementen, sino que también se comuniquen y sean comprendidas por todos los miembros de la organización, pues la falta de concientización sobre ciberseguridad entre los empleados es una de las principales causas de incidentes de seguridad. Por lo tanto, es fundamental desarrollar programas de formación y concientización que capaciten al personal en buenas prácticas de seguridad (Bermúdez et al., 2023).

Asignar adecuadamente los recursos es clave en la integración de la ciberseguridad, pero requiere inversión financiera y humana, de manera que las organizaciones deben estar dispuestas a invertir en tecnología avanzada y en contratar personal capacitado que pueda gestionar las políticas y medidas de seguridad de manera efectiva (Sánchez, 2023).

La ciberseguridad no puede verse como una solución estática. El panorama de amenazas cibernéticas cambia constantemente, por lo que las organizaciones deben estar preparadas para adaptarse a nuevos desafíos, lo cual implica actualizar regularmente las tecnologías de seguridad, revisar las políticas y los procedimientos, así como mejorar continuamente las capacidades del personal (Casale, 2022).

En este contexto, utilizar indicadores y métricas es útil para evaluar la efectividad de las medidas de ciberseguridad, al tiempo que permiten medir el desempeño de las políticas y procedimientos de seguridad, identificar áreas de mejora y tomar decisiones informadas. Algunos indicadores comunes incluyen el número de incidentes de seguridad detectados, el tiempo de respuesta ante incidentes y el costo de las medidas de ciberseguridad implementadas (Valderrama, 2024).

Además, realizar pruebas regulares de las medidas de ciberseguridad, como simulacros de ataques y auditorías de seguridad, ayuda a identificar posibles debilidades en las defensas de la organización y mejora la capacidad de respuesta ante un ataque real. De igual forma, estas prácticas sensibilizan a los empleados sobre la importancia de seguir las políticas de seguridad y fortalecen la cultura organizacional en torno a la ciberseguridad (Muñoz-Zambrano & Zambrano-Rendón, 2023).

Para realizar estas acciones es muy importante la colaboración con otras dependencias de la organización. Por ejemplo, mientras el área legal puede proporcionar orientación sobre el cumplimiento normativo y las implicaciones legales de un incidente de seguridad, por su parte, el área de TI ofrece soporte técnico para implementar medidas preventivas. Así, esta colaboración asegura que la estrategia de ciberseguridad sea coherente y eficaz (Rutz, 2021).

Asimismo, el compromiso de la alta dirección resulta fundamental, pues sin su apoyo es difícil garantizar que se asignen los recursos necesarios y que las políticas de seguridad se implementen de manera efectiva. Además, la alta dirección debe promover una cultura de seguridad en toda la organización, de tal manera que cada empleado entienda su responsabilidad en la protección de los activos digitales (Pereyra, 2021).

La ciberseguridad también debe integrarse en los procesos de gestión de riesgos. Específicamente, las organizaciones deben considerar los riesgos cibernéticos como parte de su análisis general y desarrollar planes de contingencia que permitan minimizar el impacto de un ataque cibernético. Estos planes deben incluir procedimientos para la recuperación ante desastres, la continuidad del negocio y la comunicación con las partes interesadas en caso de un incidente (Guzmán-Pacheco, 2022). La tabla 3 sintetiza los elementos de la estrategia descritos.

Tabla 3. Elementos ciber en la estrategia

| Elemento | Descripción | Prácticas clave | Referencias |
|---|---|---|--|
| Integración en la planificación estratégica | La ciberseguridad debe integrarse en la planificación estratégica de la organización para garantizar la protección de los activos y la continuidad operativa. | Evaluaciones de riesgos periódicas y adaptación continua a nuevas amenazas. | Muñoz-Zambrano & Zambrano-Rendón (2023). |
| Evaluación de riesgos | Identificar y evaluar los riesgos cibernéticos permite a las organizaciones comprender sus vulnerabilidades y diseñar medidas de mitigación. | Identificación de activos críticos (bases de datos y sistemas TI), determinación del impacto de los ciberataques y realización de evaluaciones periódicas de riesgos. | Guzmán-Pacheco (2022). |
| Medidas preventivas | Después de evaluar los riesgos, se deben diseñar e implementar medidas preventivas para garantizar la protección de los activos digitales. | Implementación de <i>firewalls</i> , sistemas de detección de intrusos, cifrado de datos, controles de acceso y políticas que regulen el uso seguro de los sistemas de información. | Valderrama (2024). |

| Elemento | Descripción | Prácticas clave | Referencias |
|---|---|---|--|
| Creación de políticas de ciberseguridad | Las políticas de ciberseguridad deben ser un esfuerzo colaborativo entre TI y otras áreas de la organización. | Políticas que cubran temas como el acceso a sistemas, la gestión de contraseñas y la respuesta a incidentes de seguridad, alineadas con normativas y regulaciones aplicables. | Rincón-Gallón (2022). |
| Concientización y capacitación | La falta de concientización sobre ciberseguridad entre los empleados es una causa común de incidentes. Es vital capacitar al personal en buenas prácticas de seguridad. | Desarrollo de programas de formación y concientización para todo el personal, con el fin de garantizar el cumplimiento de las políticas de seguridad. | Bermúdez et al. (2023). |
| Asignación de recursos | Asignar los recursos adecuados, tanto financieros como humanos, es clave para la integración de la ciberseguridad. | Inversión en tecnología avanzada y contratación de personal capacitado para gestionar las políticas y las medidas de seguridad de forma efectiva. | Sánchez (2023). |
| Actualización continua | La ciberseguridad es dinámica y debe evolucionar con el panorama de las amenazas. | Actualización regular de tecnologías, revisión de políticas y mejora continua de las capacidades del personal. | Casale (2022). |
| Uso de métricas e indicadores | Las métricas son útiles para evaluar la efectividad de las medidas de ciberseguridad. Permiten medir el rendimiento de las políticas y tomar decisiones informadas. | Uso de indicadores, como número de incidentes detectados, tiempo de respuesta y costo de las medidas implementadas. | Valderrama (2024). |
| Pruebas y auditorías | Realizar pruebas regulares de las medidas de ciberseguridad ayuda a identificar debilidades y mejorar la capacidad de respuesta ante ataques. | Simulacros de ataques, auditorías de seguridad y programas de sensibilización para los empleados. | Muñoz-Zambrano & Zambrano-Rendón (2023). |
| Colaboración interdepartamental | Colaborar con áreas como legal y TI asegura que la estrategia de ciberseguridad sea coherente y efectiva. | El área legal puede orientar en el cumplimiento normativo, mientras que el TI puede implementar medidas preventivas. | Rutz (2021). |
| Compromiso de la alta dirección | El apoyo de la alta dirección es esencial para asignar los recursos necesarios y promover una cultura de seguridad en la organización. | Fomentar una cultura de seguridad en la que cada empleado entienda su responsabilidad en la protección de los activos digitales. | Pereyra (2021). |
| Gestión de riesgos | La ciberseguridad debe integrarse en los procesos de gestión de riesgos y en los planes de contingencia para minimizar el impacto de un ataque. | Desarrollar planes de recuperación ante desastres, continuidad del negocio y comunicación efectiva en caso de incidentes. | Guzmán-Pacheco (2022). |

| Elemento | Descripción | Prácticas clave | Referencias |
|---------------------------------|--|--|-----------------|
| Ciberseguridad y competitividad | Integrar la ciberseguridad no solo protege, sino que también mejora la competitividad al generar confianza en clientes y socios comerciales. | Organizaciones comprometidas con la ciberseguridad mejoran su reputación y se diferencian en el mercado. | Sánchez (2023). |

Fuente: Elaboración propia

Por lo tanto, integrar la ciberseguridad en la planificación estratégica no es solo una cuestión de protección, sino también de competitividad. Las organizaciones que demuestran un compromiso sólido con la ciberseguridad ganan la confianza de sus clientes y socios comerciales, lo cual les permite diferenciarse en el mercado y mejorar su reputación (Sánchez, 2023).

No obstante, uno de los principales desafíos en la integración de la ciberseguridad en la planeación estratégica es la ausencia de marcos metodológicos estandarizados dentro de muchas organizaciones. Para superar esta dificultad, es recomendable adoptar marcos como el NIST Cybersecurity Framework (CSF), COBIT o las doctrinas de ciberdefensa de la OTAN, instrumentos que proporcionan directrices estructuradas para gestionar los riesgos cibernéticos de forma proactiva y alineada con los objetivos organizacionales (ISACA, 2019; OTAN, 2021; NIST, 2018).

El marco NIST CSF se compone de cinco funciones esenciales: identificar, proteger, detectar, responder y recuperar. Esta estructura permite a las organizaciones entender su entorno de riesgo y priorizar acciones que aseguren la continuidad del negocio, pues su flexibilidad permite aplicarlas tanto en grandes corporaciones como en pymes, de tal manera que fomentan la resiliencia digital desde un enfoque escalable (NIST, 2018).

Por su parte, COBIT ofrece un enfoque integral para la gobernanza y la gestión de las tecnologías de la información. Con una orientación hacia el cumplimiento, la calidad y la seguridad de los sistemas, COBIT facilita la alineación de las estrategias de TI con los objetivos corporativos. Su enfoque basado en procesos y control permite definir responsabilidades claras, establecer indicadores y gestionar eficazmente la ciberseguridad como un activo estratégico (ISACA, 2019).

En contextos internacionales y de defensa, las doctrinas de la OTAN establecen principios fundamentales para la protección de infraestructuras críticas, la cooperación internacional y la defensa activa ante amenazas persistentes avanzadas (APT). Estas doctrinas integran la ciberdefensa como una dimensión estratégica

de la seguridad nacional y promueven capacidades conjuntas de disuasión, disuasión activa y recuperación operativa (OTAN, 2021).

Es importante tener en cuenta que la implementación de estos marcos debe adaptarse a la cultura organizacional, el nivel de madurez digital y los recursos disponibles. Ahora bien, también es cierto que un enfoque híbrido que combine los lineamientos de NIST con el gobierno estructurado de COBIT puede resultar particularmente eficaz en sectores regulados o críticos como la banca, la salud y las telecomunicaciones. Además de lo anterior, cumplir los estándares internacionales refuerza la reputación institucional ante clientes, socios y entes reguladores (Sánchez, 2023).

Por lo tanto, es recomendable que las organizaciones incluyan en su planeación estratégica no solo políticas generales de ciberseguridad, sino también una hoja de ruta metodológica apoyada en marcos reconocidos. Esto fortalece la capacidad de anticipación, respuesta y recuperación frente a las amenazas del entorno digital, y permite medir el desempeño de las estrategias implementadas con base en prácticas internacionales consolidadas (Muñoz-Zambrano & Zambrano-Rendón, 2023).

Rol de la ciberdefensa en la planeación estratégica

La implementación práctica de estrategias de ciberseguridad y ciberdefensa puede observarse en organizaciones líderes que han logrado integrar estos elementos en su planeación estratégica. Un caso emblemático es el de la NASA, que adoptó el NIST CSF como base para su marco de gestión de riesgos cibernéticos, con lo cual aseguró una protección integral de sus sistemas críticos y datos científicos (NIST, 2018).

En el sector financiero, el banco HSBC ha implementado el marco COBIT para alinear su estrategia de ciberseguridad con sus objetivos corporativos. Esto le ha permitido establecer controles sobre activos digitales, identificar riesgos emergentes y asegurar el cumplimiento normativo en distintas jurisdicciones. En particular, la combinación de marcos técnicos y una cultura organizacional proactiva ha sido clave en su éxito (ISACA, 2019).

Por su parte, en el sector gubernamental, el Departamento de Defensa de los Estados Unidos ha desarrollado una doctrina de ciberdefensa basada en la resiliencia operativa y en compartir inteligencia en tiempo real con agencias aliadas. Además, esta estrategia incluye ejercicios conjuntos con organizaciones civiles

y privadas para simular ciberataques a gran escala, como parte del programa "Cyber Shield" (OTAN, 2021).

En América Latina, Chile ha avanzado en la institucionalización de su ciberdefensa mediante la creación del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT). Esta entidad trabaja en conjunto con empresas públicas y privadas, promoviendo buenas prácticas, alertas tempranas y estándares de seguridad para infraestructuras críticas (Gobierno de Chile, 2022).

Otro caso interesante es el del Centro Nacional de Ciberseguridad de Colombia (CNCS), que ha desarrollado un marco nacional basado en NIST y la ISO/IEC 27001. Este esfuerzo ha permitido coordinar esfuerzos entre entidades públicas, militares y privadas para aumentar la capacidad de respuesta ante incidentes cibernéticos y proteger el ecosistema digital colombiano (MinTIC, 2021).

Estos ejemplos permiten evidenciar que la integración estratégica de la ciberseguridad no es un ideal teórico, sino una práctica creciente en entornos complejos. Asimismo, sirven como referencia para aquellas organizaciones que buscan estructurar sus esfuerzos en torno a modelos probados, adaptándolos a sus necesidades, capacidades y contexto sectorial (Rutz, 2021).

En un mundo donde las amenazas cibernéticas están en constante evolución, la ciberdefensa ha emergido como un pilar fundamental en la planificación estratégica de las organizaciones. La ciberdefensa no se limita a la simple protección de los sistemas internos, sino que va más allá, proporcionando un enfoque integral que permite a las empresas detectar, responder y recuperarse de ataques cibernéticos con rapidez y eficacia. Finalmente, cabe enfatizar que mientras la ciberseguridad se centra en la prevención de incidentes, la ciberdefensa añade una capa de protección al preparar a la organización para enfrentar incidentes cuando ocurren y mitigar su impacto (Casale, 2022).

DetECCIÓN TEMPRANA DE AMENAZAS: EL PRIMER PASO PARA UNA RESPUESTA EFECTIVA

La detección temprana de amenazas es uno de los pilares fundamentales de una estrategia de ciberdefensa efectiva. En un mundo donde las amenazas cibernéticas son cada vez más frecuentes y sofisticadas, la capacidad de identificar y neutralizar ataques en sus primeras etapas es fundamental para mitigar el impacto que pueden causar en una organización.

Por esta razón, como se ha señalado, los ataques cibernéticos, que pueden ocurrir en cualquier momento, exigen una vigilancia constante y el uso de

tecnologías avanzadas para garantizar una respuesta oportuna. Es aquí donde entran en juego herramientas de *monitoreo continuo* y *análisis de tráfico de red*, las cuales desempeñan un papel esencial porque permiten identificar comportamientos sospechosos antes de que los daños sean irreversibles (Muñoz-Zambrano & Zambrano-Rendón, 2023).

Específicamente, el monitoreo continuo es un proceso activo que involucra la supervisión ininterrumpida de los sistemas informáticos y las redes de la organización. A través del uso de tecnologías como los sistemas de detección de intrusiones (IDS) y de herramientas de análisis en tiempo real, es posible obtener una imagen clara de la actividad que se realiza dentro de la red. Estas soluciones no solo detectan actividades inusuales, sino que también alertan de manera inmediata al equipo de seguridad, lo cual permite que se tomen decisiones rápidas para contener y mitigar cualquier ataque en curso. En tal sentido, esta capacidad de respuesta temprana es esencial porque que minimiza el tiempo de exposición a las amenazas y reduce las posibilidades de que estas se conviertan en incidentes cibernéticos graves.

Por su parte, el análisis de tráfico de red es una técnica avanzada que permite identificar patrones anómalos en los flujos de datos que podrían indicar la presencia de un ataque. A través de la correlación de eventos y el análisis de grandes volúmenes de datos, estas herramientas pueden detectar incluso las amenazas más sutiles que podrían pasar desapercibidas para los métodos tradicionales de defensa. Al identificar estos patrones anómalos, las organizaciones pueden activar de inmediato sus *protocolos de respuesta a incidentes*, lo cual les permite contener la amenaza antes de que esta pueda comprometer sistemas críticos.

Este enfoque proactivo es vital porque los atacantes cibernéticos constantemente buscan puntos débiles en las defensas de las organizaciones. Por lo tanto, si se cuenta con sistemas de monitoreo continuo y análisis de tráfico de red, las organizaciones no solo pueden identificar ataques en curso, sino también prevenir los futuros identificando las vulnerabilidades antes de que puedan ser explotadas. De esta forma, la detección temprana contribuye a reducir el impacto inmediato de un ataque y fortalece las defensas a largo plazo, con lo cual ayuda a que las organizaciones se adapten continuamente a las amenazas cambiantes del ciberespacio.

Capacitación continua: la primera línea de defensa

En el contexto de la ciberdefensa, los empleados son un recurso invaluable que, si se capacita adecuadamente, puede convertirse en la primera línea de defensa

frente a los ciberataques. Dado que los ataques cibernéticos no solo se enfocan en vulnerabilidades tecnológicas, sino también en debilidades humanas, es crucial que las organizaciones inviertan en capacitación continua para preparar a su personal contra las amenazas más recientes del ciberespacio. En este sentido, las organizaciones que implementan programas de formación efectivos están mejor posicionadas para enfrentar los desafíos que presenta el panorama actual de ciberseguridad, ya que los empleados desempeñan un papel clave en la prevención de ataques internos y externos (Bermúdez et al., 2023).

La importancia de la capacitación continua

La capacitación del personal debe ser un proceso continuo y dinámico. Sin embargo, no basta con una formación única o esporádica, pues dado que las cibermenazas evolucionan rápidamente, los empleados necesitan estar al día con las últimas tácticas y métodos empleados por los ciberdelincuentes. Esta formación regular cumple un doble propósito: por una parte mejora la capacidad de los empleados para identificar y mitigar posibles ataques, y, por otra, contribuye a crear una cultura de ciberseguridad dentro de la organización, la cual se convierte en una herramienta poderosa para reducir el riesgo de ataques que aprovechan errores humanos, como el *phishing* o la ingeniería social (Jiménez-Almeira & López, 2023).

Específicamente, entre la variedad de temas que debe abordar la formación continua, uno de los más críticos para la ciberseguridad es la identificación y la prevención de ataques de *phishing*, los cuales siguen siendo una de las principales tácticas utilizadas por los ciberdelincuentes para acceder a sistemas sensibles. Frente a este escenario, los empleados deben aprender a detectar correos electrónicos sospechosos, mensajes maliciosos y sitios web falsificados, así como contar con las herramientas necesarias para reportar estas amenazas al equipo de seguridad de la organización (Rueda, 2020).

Además de continua, la capacitación a los empleados también debe incluir simulacros regulares de incidentes cibernéticos que les permitan familiarizarse con los protocolos de respuesta ante un ataque y saber cómo actuar en situaciones reales. De hecho, las organizaciones que realizan simulacros con regularidad pueden evaluar y ajustar sus planes de respuesta a incidentes, de tal manera que garantizan que sus empleados estén preparados para enfrentar cualquier amenaza. Finalmente, cabe señalar que, según Valencia (2023), los simulacros aumentan la capacidad de respuesta organizacional y permiten identificar debilidades en las estrategias de defensa.

Capacitación adaptada a las nuevas amenazas

Como se ha enfatizado en los apartados anteriores, la evolución de las cibermenazas exige que la capacitación en ciberseguridad no sea estática, pues los atacantes innovan constantemente las tácticas y las técnicas que emplean, como *malware* avanzado, *ransomware* o ataques dirigidos. Frente a esta problemática, Nolasco-Mamani et al. (2022) señalan que uno de los errores más comunes en las organizaciones es confiar en programas de capacitación desactualizados, ya que esto deja a los empleados en una condición de vulnerabilidad ante nuevos vectores de ataque.

Además de la capacitación técnica, es crucial que las organizaciones también incluyan formación sobre aspectos éticos y de cumplimiento normativo. En particular, el creciente enfoque en la privacidad de los datos, así como el surgimiento de regulaciones similares al Reglamento General de Protección de Datos (GDPR), hacen necesario que los empleados comprendan las implicaciones legales de un ataque cibernético y cómo proteger adecuadamente la información personal y sensible.

El papel de la alta dirección en la capacitación

Es fundamental que la alta dirección esté comprometida con la implementación de políticas de seguridad cibernética y que los líderes aseguren los recursos necesarios para capacitar de forma continua al personal. Como argumentan García y argumenta Flores-Romero (2023), la importancia de este compromiso radica en que se crea una cultura organizacional donde todos los empleados, independientemente de su rol, comprenden la importancia de la seguridad digital.

Así pues, la creación de una cultura de ciberseguridad robusta depende de que los empleados de todos los niveles estén alineados con los objetivos de seguridad de la organización. De igual forma, la colaboración entre departamentos, la comunicación clara de las políticas de seguridad y la disponibilidad de recursos para el entrenamiento constante son componentes esenciales para lograrlo (tabla 4).

Tabla 4. Proceso de capacitación que vincula estrategia con ciber

| Capacitación en ciberseguridad | Descripción | Roles para su desarrollo |
|--------------------------------|--|--|
| Identificación de phishing | Capacitación para detectar correos electrónicos y mensajes maliciosos. | Equipos de seguridad TI y departamentos de recursos humanos. |
| Respuesta a incidentes | Entrenamiento en protocolos de acción ante un ciberataque. | Equipos de respuesta a incidentes y alta dirección. |

| Capacitación en ciberseguridad | Descripción | Roles para su desarrollo |
|---------------------------------------|---|--|
| Simulacros de ataques | Realización de simulaciones de ataques para evaluar la capacidad de respuesta. | Equipos de seguridad y gerencia de operaciones. |
| Protección de datos personales | Formación en cumplimiento de regulaciones, como GDPR y manejo de datos sensibles. | Equipos legales y departamentos de <i>compliance</i> . |
| Uso seguro de redes sociales | Educación sobre los riesgos asociados con el uso de redes sociales en el trabajo. | Equipos de seguridad y comunicación interna. |
| Manejo de dispositivos móviles | Capacitación en seguridad para el uso de dispositivos móviles y BYOD. | Equipos de TI y recursos humanos. |
| Ingeniería social | Entrenamiento para evitar ser víctima de técnicas de manipulación humana. | Seguridad TI, recursos humanos y equipos de psicología organizacional. |

Fuente: Elaboración propia.

Implementación de tecnologías avanzadas en la ciberdefensa

El uso de tecnologías avanzadas es un elemento esencial para una estrategia de ciberdefensa efectiva. Herramientas como los sistemas de detección y prevención de intrusiones (IDS/IPS), *firewalls* de próxima generación y soluciones basadas en inteligencia artificial ayudan a las organizaciones a detectar y neutralizar amenazas cibernéticas de manera proactiva. Estas tecnologías permiten automatizar muchas de las respuestas a ataques, lo que reduce significativamente el tiempo de reacción y mejora la eficiencia operativa en la protección de los sistemas críticos (Sánchez, 2023).

La inteligencia artificial, en particular, está transformando la ciberdefensa al proporcionar capacidades avanzadas de detección de amenazas. Mediante el uso de algoritmos de aprendizaje automático, es posible identificar patrones de comportamiento anómalos en grandes volúmenes de datos, lo cual facilita la detección de ataques en etapas tempranas. La IA también ayuda a las organizaciones a anticiparse a posibles amenazas, lo cual les permite implementar medidas de defensa antes de que los atacantes puedan explotar vulnerabilidades.

Colaboración interna y externa en la ciberdefensa

En el entorno actual de amenazas cibernéticas crecientes y cada vez más sofisticadas, la colaboración interna y externa se ha convertido en un componente fundamental de una ciberdefensa efectiva. La ciberseguridad ya no puede abordarse

como una responsabilidad exclusiva del departamento de TI o del equipo de seguridad de una organización; requiere un enfoque holístico que implique a todos los niveles y áreas de la empresa, desde la alta dirección hasta los empleados de línea. Asimismo, la colaboración con entidades externas, como agencias gubernamentales y organismos reguladores, es vital para construir una infraestructura de ciberseguridad robusta y resiliente. Este punto subraya la importancia de la cooperación interna y externa para mitigar los riesgos cibernéticos y garantizar una respuesta coordinada ante incidentes de seguridad.

Colaboración interna: un enfoque transversal

Una ciberdefensa efectiva dentro de una organización comienza con la colaboración entre departamentos. La integración de todos los actores internos es clave para que las medidas de seguridad no solo se implementen, sino que también se mantengan de manera coherente y efectiva. Esto implica la cooperación entre el departamento de TI, que es responsable de la infraestructura tecnológica; el equipo de seguridad encargado de la protección y respuesta ante incidentes; y la alta dirección, que proporciona la visión estratégica y los recursos necesarios para implementar una estrategia integral de ciberdefensa (Guzmán-Pacheco, 2022).

Para que esta colaboración sea exitosa, es necesario que cada área comprenda su rol y cómo su trabajo contribuye a la protección de la organización. El departamento de TI, por ejemplo, es el encargado de asegurar que la infraestructura tecnológica esté actualizada y protegida contra las amenazas. No obstante, sin el apoyo de la alta dirección, que debe asignar los recursos financieros y humanos necesarios, y sin la participación activa de todos los empleados, los esfuerzos del departamento de TI serán insuficientes. Por otro lado, el equipo de seguridad debe coordinarse con todas las áreas para que las políticas y los protocolos de seguridad se implementen de manera coherente en toda la organización.

Además, como se ha señalado, es esencial fomentar una cultura organizacional donde todos los empleados sean conscientes de la importancia de la ciberseguridad. Esto implica que las políticas de seguridad no se vean como algo exclusivo del equipo de TI, sino como una responsabilidad compartida por toda la empresa. Los trabajadores deben ser capacitados regularmente para estar preparados ante posibles ataques, lo cual incluye saber cómo responder y reportar incidentes cibernéticos. Según Fernández (2023), una de las mayores fallas en ciberdefensa ocurre cuando los empleados no tienen claros los protocolos de seguridad o no están preparados para actuar rápidamente ante un incidente.

Respuesta coordinada ante incidentes

La respuesta rápida y coordinada ante incidentes de seguridad es otro aspecto crucial de la colaboración interna. Para que la organización pueda minimizar el impacto de un ataque cibernético, es necesario que los protocolos de respuesta estén bien definidos y que todos los departamentos sepan cómo proceder en caso de un incidente. Esto requiere que los planes de contingencia y las respuestas a incidentes no sean responsabilidad exclusiva del equipo de seguridad, sino que involucren a toda la organización. Los departamentos de TI, operaciones, recursos humanos y comunicaciones, así como la alta dirección deben trabajar de manera conjunta para asegurar que la respuesta sea rápida, eficaz y minimice el impacto operativo y reputacional.

Un ejemplo de esta colaboración es la implementación de simulacros regulares de incidentes, en los cuales todos los departamentos participen para evaluar su preparación y coordinar su respuesta ante posibles ciberataques. Estos simulacros ayudan a identificar debilidades en la estrategia de ciberseguridad de la organización y permiten realizar ajustes en los protocolos de respuesta antes de que ocurra un incidente real. Al respecto, Nolasco-Mamani et al. (2022) argumentan que los simulacros no solo mejoran la capacidad de respuesta, sino que también fomentan la colaboración y la comunicación entre los distintos departamentos.

Colaboración externa: aliados estratégicos

La colaboración externa en la ciberdefensa es igual de importante que la interna. Las organizaciones no operan en un vacío, y cuando enfrentan amenazas cibernéticas, muchas veces la mejor defensa es aplicar un enfoque cooperativo que involucre tanto al sector privado como a entidades gubernamentales y otros organismos de seguridad cibernética. La colaboración con el sector externo es especialmente crítica en caso de un ataque de gran escala, donde los recursos internos pueden no ser suficientes para contener y mitigar el impacto del incidente.

El sector privado y las autoridades gubernamentales pueden proporcionar los recursos, la orientación y la asistencia técnica que resultan vitales para mitigar el impacto de un ciberataque. En particular, las agencias de ciberseguridad gubernamentales suelen disponer de recursos especializados que pueden ayudar a las organizaciones a analizar y gestionar incidentes cibernéticos. En muchos países, existen mecanismos de cooperación público-privada que permiten a las empresas compartir información sobre amenazas y acceder a conocimientos técnicos proporcionados por entidades especializadas, lo cual fortalece la ciberdefensa en su conjunto (Carlini, 2016).

Un buen ejemplo de esta colaboración es el trabajo conjunto entre empresas privadas y los CERT (Computer Emergency Response Teams), que proporcionan soporte y orientación en caso de incidentes cibernéticos. Estas organizaciones tienen acceso a información crítica sobre nuevas amenazas y tácticas utilizadas por atacantes, lo cual permite a las empresas ajustar rápidamente sus defensas. Según Alonso y Tejada (2017), la colaboración con los CERT ha sido fundamental para mejorar la respuesta global a ciberataques, lo cual ha proporcionado a las organizaciones el acceso a herramientas y conocimientos especializados que de otro modo no tendrían.

La colaboración entre sectores: el papel del gobierno y las organizaciones internacionales

La colaboración entre sectores va más allá del simple intercambio de información. En muchos casos, la cooperación con organismos internacionales es clave para enfrentar amenazas cibernéticas que traspasan fronteras. Los ciberataques, por su naturaleza, son problemas globales que requieren soluciones globales. Los organismos internacionales como la Interpol, la OTAN y otros grupos de seguridad globales tienen un papel fundamental porque proporcionan recursos y establecen protocolos de respuesta transnacionales. Esta cooperación es crucial, especialmente cuando se trata de ataques dirigidos a infraestructuras críticas que pueden tener consecuencias regionales o mundiales (Ramírez, 2023).

Además, las organizaciones internacionales trabajan en conjunto para crear normas y estándares de ciberseguridad que las empresas deben cumplir. Como se mencionó, un ejemplo de esto es el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, que establece pautas claras para proteger la información personal y obliga a las empresas a garantizar la seguridad de los datos que manejan. El cumplimiento de estas normativas no solo protege a las organizaciones de sanciones legales, sino que también mejora sus capacidades de ciberdefensa al estandarizar las mejores prácticas en el mundo (Sánchez & Morales, 2022).

Beneficios de la colaboración en la ciberdefensa

Los beneficios de la colaboración en la ciberdefensa son numerosos. En el ámbito interno, la colaboración entre departamentos fortalece la capacidad de respuesta de la organización, mejora la comunicación y fomenta una cultura de seguridad. En el ámbito externo, la cooperación con el sector público y las organizaciones internacionales proporciona a las empresas los recursos y conocimientos necesarios para protegerse de amenazas cibernéticas complejas. Según Ramírez (2023),

las organizaciones que colaboran tanto interna como externamente están mejor preparadas para enfrentar los desafíos de la ciberseguridad y mitigar el impacto de los ciberataques.

En conclusión, la colaboración interna y externa es un componente esencial para consolidar una estrategia de ciberdefensa robusta. Las amenazas cibernéticas modernas requieren un enfoque cooperativo, tanto dentro de las organizaciones como en el contexto global. Al fomentar la colaboración entre departamentos y trabajar de la mano con agencias gubernamentales y entidades internacionales, las organizaciones pueden mejorar significativamente su capacidad de protegerse y responder a los ciberataques.

Conclusiones

La creciente complejidad del entorno digital ha subrayado la importancia crítica de la ciberseguridad y la ciberdefensa en la protección de los activos digitales de las organizaciones. Las amenazas cibernéticas, que han evolucionado en alcance y sofisticación, representan riesgos significativos para la confidencialidad, la integridad y la disponibilidad de la información. Ante estos desafíos, la integración de la ciberseguridad y la ciberdefensa en la estrategia organizacional, lejos de ser opcional, es esencial para garantizar la continuidad operativa y la protección de los datos sensibles, tanto de la empresa como de sus clientes. Las organizaciones que fallan en adoptar medidas preventivas y reactivas adecuadas quedan expuestas a un mayor riesgo de sufrir ataques que pueden comprometer no solo su infraestructura tecnológica, sino también su reputación y posición en el mercado (Ramírez, 2024).

El enfoque de ciberseguridad, con su énfasis en la prevención, debe complementarse con estrategias de ciberdefensa que permitan a las organizaciones detectar, responder y recuperarse de manera efectiva ante los incidentes. Las organizaciones que logran establecer un equilibrio entre la prevención y la respuesta están mejor preparadas para mitigar el impacto de los ciberataques. La implementación de medidas como la detección temprana de amenazas, los planes de respuesta a incidentes y la formación continua del personal se vuelven imprescindibles en este contexto. Sin estas acciones, la capacidad de una organización para enfrentar un ciberataque se reduce drásticamente, exponiéndola a mayores pérdidas financieras y reputacionales (Rincón-Gallón, 2022).

Además, la colaboración interna entre los distintos departamentos de la organización, desde el equipo de TI hasta la alta dirección, es fundamental para asegurar una ciberdefensa efectiva. Cada departamento debe estar alineado con los objetivos de seguridad de la empresa y participar activamente en la implementación y el mantenimiento de las medidas de ciberseguridad. Al mismo tiempo, la colaboración externa con entidades gubernamentales, agencias de seguridad y organismos internacionales es vital para compartir información sobre amenazas emergentes y mejorar las capacidades defensivas de la organización. La falta de colaboración, tanto interna como externa, limita la efectividad de cualquier estrategia de ciberseguridad (Guzmán-Pacheco, 2022).

Por otro lado, la ciberseguridad no solo protege los sistemas y datos de una organización, sino que también contribuye a su resiliencia y capacidad de adaptación frente a las nuevas amenazas. Las organizaciones deben estar preparadas no solo para prevenir ataques, sino también para recuperarse rápidamente y garantizar la continuidad de sus operaciones. En este sentido, la creación de una cultura organizacional sólida en torno a la ciberseguridad y la ciberdefensa, junto con la actualización constante de las tecnologías y estrategias de seguridad, es clave para mantener una ventaja competitiva en el mercado actual (Valderrama, 2024).

En conclusión, el camino hacia una ciberdefensa robusta requiere un enfoque integral que combine la prevención con la capacidad de respuesta ante incidentes, junto con una cultura organizacional orientada hacia la seguridad. Las organizaciones que inviertan en tecnología avanzada, formación continua para sus empleados y colaboración efectiva con agentes externos estarán mejor equipadas para enfrentar las amenazas cibernéticas actuales y futuras. En este sentido, la ciberseguridad y la ciberdefensa ya no pueden ser vistas como cuestiones técnicas aisladas, sino como elementos fundamentales en la estrategia general de cualquier organización que aspire a sobrevivir y prosperar en el entorno digital global (Sánchez & Morales, 2022).

Futuros trabajos

Los futuros trabajos en el área de ciberseguridad y ciberdefensa deben enfocarse en varios aspectos clave para continuar fortaleciendo las estrategias organizacionales frente a las amenazas emergentes. En primer lugar, es necesario investigar nuevas tecnologías, como la inteligencia artificial y el aprendizaje automático para la detección predictiva de amenazas. Estas herramientas tienen el potencial

de mejorar significativamente la capacidad de respuesta porque automatizan la identificación de patrones anómalos y reducen el tiempo de detección de ataques.

En segundo lugar, es fundamental explorar las implicaciones de la ciberseguridad en la cadena de suministro. A medida que las organizaciones dependen cada vez más de proveedores externos y sistemas interconectados, los ataques dirigidos a los socios comerciales pueden representar un riesgo importante. La investigación futura debería centrarse en el desarrollo de marcos de colaboración y protocolos de seguridad que fortalezcan la ciberdefensa en toda la cadena de valor.

Otro aspecto importante para el futuro es la creación de normativas y regulaciones internacionales más robustas y coherentes. A medida que las amenazas cibernéticas se globalizan, la capacidad de los marcos regulatorios nacionales es limitada para gestionar adecuadamente los ataques que traspasan fronteras. Por lo tanto, los futuros trabajos deben centrarse en cómo mejorar la cooperación internacional para abordar estas amenazas mediante la creación de acuerdos y estándares que unifiquen las mejores prácticas en el mundo.

También será esencial investigar el impacto de las nuevas tecnologías disruptivas, como la computación cuántica, en la ciberseguridad. Si bien estas tecnologías presentan oportunidades para mejorar las defensas, también plantean desafíos únicos en términos de la capacidad de los sistemas actuales para resistir ataques. El desarrollo de estrategias de defensa cibernética frente a las amenazas cuánticas debe ser una prioridad en la investigación futura.

Pese al creciente reconocimiento de la importancia de integrar la ciberseguridad y la ciberdefensa en la estrategia organizacional, aún son escasas las investigaciones empíricas que documenten casos exitosos y replicables en el contexto latinoamericano. Esta ausencia representa una oportunidad de investigación y desarrollo de capacidades en materia de gobernanza digital (Carreño & López, 2022).

La mayoría de los estudios se centran en propuestas teóricas o marcos de referencia genéricos, sin abordar cómo estos modelos han sido implementados en escenarios específicos. Por ello, resulta necesario desarrollar estudios de caso que documenten experiencias reales de integración en sectores críticos como salud, energía, banca o educación (Carlini, 2016).

Adicionalmente, los marcos metodológicos disponibles, como NIST CSF o COBIT, deben ser contextualizados a las realidades organizacionales locales, pues la transferencia de estos modelos a países en desarrollo enfrenta barreras como limitación de recursos, escasa capacitación o debilidad institucional (Sánchez, 2023).

En este sentido, la generación de conocimiento contextualizado es clave para fortalecer las capacidades locales. Investigaciones futuras podrían centrarse en cómo adaptar buenas prácticas internacionales a entornos con distintos niveles de madurez digital, infraestructura tecnológica y cultura organizacional (Bermúdez et al., 2023).

Otra línea prometedora de trabajo consiste en el análisis comparativo de políticas públicas regionales de ciberseguridad y ciberdefensa, pues esto permitiría identificar brechas, sinergias y oportunidades de cooperación entre países, con miras a construir un ecosistema digital más resiliente en América Latina (OCDE, 2020).

Referencias

- Akbanov, M., Vassilakis, V. G., & Logothetis, M. D. (2019). WannaCry Ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. *JTIT*, 75(1), 113-124. <https://doi.org/10.26636/jtit.2019.130218>
- Alonso, G. M. P., & Tejada, R. R. (2017). La cooperación público-privada en el fomento de la cultura de ciberseguridad. *Cuadernos de Estrategia*, (185), 217-246. <https://tinyurl.com/2z4dbvb6>
- Bermúdez Oviedo, M. Y., Téllez Florián, M. A., & Conde Urrea, C. A. (2023). *Gestión financiera y administrativa de las inversiones digitales en empresas del sector comercial financiero y de economía solidaria* [trabajo de grado, Universidad Cooperativa de Colombia, Bogotá]. Repositorio Institucional UCC. <https://tinyurl.com/65snauk9>
- Carlini, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. *Boletín IEEE*, (2), 950-966. <https://tinyurl.com/yt44u768>
- Carreño, J., & López, A. (2022). *Resiliencia organizacional y ciberseguridad: Estrategias para la continuidad del negocio*. Editorial Cibertec.
- Casale, C. G. (2022). *La ciberdefensa como factor crítico en el desarrollo de operaciones militares en el nivel operacional* [trabajo final, Escuela Superior de Guerra Tte Grl Luis María Campos, Buenos Aires]. CEFADigital. <https://tinyurl.com/22tmc7dm>
- Fernández Delgado, L. (2023). *SIC Revista Ciberseguridad, seguridad de la información y privacidad*, 156. <https://revistasic.es/sic156/revistasic156.pdf>
- Flores-Romero, M. B., & González-Santoyo, F. (2023). *La dirección estratégica y su impacto en el desarrollo de la empresa de clase mundial*. Instituto Iberoamericano de Desarrollo Empresarial. <https://tinyurl.com/ys3dtame>
- González, J. (2020). *La ciberseguridad como eje central en la protección de infraestructuras críticas*. Instituto de Estudios Estratégicos.
- Guzmán-Pacheco, J. A. (2022). Importancia de una Ley de ciberseguridad y ciberdefensa para Colombia. *Revista Ciberespacio Tecnología e Innovación*, 1(1), 67-90. <https://doi.org/10.25062/2955-0270.4766>
- Jiménez-Almeira, G. A., & López, D. E. (2023). Ciberseguridad y seguridad integral: Un análisis reflexivo sobre el avance normativo en Colombia. *Revista Ibérica de Sistemas e Tecnologías de Informação*, (E62), 16-31 .
- Muñoz-Zambrano, C., & Zambrano-Rendón, A. D. (2023). Security Operations Center como modelo de gestión de ciberseguridad para el Hospital Especialidades de Portoviejo, Manabí, Ecuador. *MQRInvestigar*, 7(3), 3220-3236. <https://doi.org/10.56048/MQR20225.7.3.2023.3220-3236>

- Nolasco-Mamani, M. A., Vidaurre, S. M. E., & Choque-Salcedo, R. E. (2022). Innovación y Transformación Digital en la Empresa. ACVENISPROH Académico.
- Pacheco-Mangas, J., Palma-García, M. D. L. O., & Hombrados-Mendieta, I. (2020). Resiliencia y cultura organizacional de los Servicios Sociales en la era de la digitalización. *Prisma Social*, (29), 123–137. <https://tinyurl.com/59zj77ec>
- Pereyra Acosta, M. A. (2021). *La ley de gobierno digital y su implicancia en la ciberdefensa del Estado Peruano* [tesis doctoral, Universidad César Vallejo, Lima]. Repositorio Institucional UCV. <https://hdl.handle.net/20.500.12692/68971>
- Ramírez Acosta, A. J. (2024). Ciberdefensa como estrategia para la seguridad y soberanía digital en Paraguay. *Revista Jurídica. Investigación en Ciencias Jurídicas y Sociales*, 7(14), 16-41. <https://tinyurl.com/29l4uts6>
- Ramírez, P. (2023). La cooperación internacional en la ciberseguridad: Desafíos y oportunidades. *Revista de Seguridad Global*, 11(2), 22-40.
- Rincón-Gallón, M. F. (2022). Los factores armados de inestabilidad frente a la ciberseguridad y la ciberdefensa nacional. *Revista Ciberespacio, Tecnología e Innovación*, 1(1), 7-40. <https://doi.org/10.25062/2955-0270.4768>
- Rodríguez Rodríguez, C. G. (2020). La importancia de un plan de continuidad del negocio. <https://tinyurl.com/yc656434>
- Rueda Quintero, J. A. (2020). *Impacto de las técnicas de phishing en Colombia durante los últimos cinco años* [Trabajo de especialización, UNAD]. Repositorio institucional. <https://tinyurl.com/4427s3yc>
- Ruiz, J. (2022). Gestión de la cadena de suministro y resiliencia ante interrupciones tecnológicas. *International Journal of Supply Chain Resilience*, 6(1), 72-85.
- Rutz, G. (2021). Ciberdefensa como campo intelectual: Aportes y propuestas de investigación en ciberdefensa y ciberseguridad para la realidad argentina. *Revista de Estudios y Pesquisas sobre las Américas*.
- Sánchez, A. (2023). *La ciberdefensa en la Fuerza Terrestre ecuatoriana desde una visión prospectiva al 2033* [Tesis de maestría. Universidad de las Fuerzas Armadas ESPE]. Espositorio ESPE. <https://repositoriobe.espe.edu.ec/server/api/core/bitstreams/242f40a2-af64-45c9-b7c4-048f9895f392/content>
- Sandoval, O. (2022). Using cyber threat intelligence to support adversary understanding applied to the Russia-Ukraine conflict. <https://tinyurl.com/4dd3jzmu>
- UNIDIR (2022). *Cooperación internacional para mitigar las operaciones cibernéticas contra la infraestructura crítica*. Instituto de las Naciones Unidas para la Investigación sobre el Desarme. <https://unidir.org/files/2022-03/https://tinyurl.com/mrc3r6ef>

Valderrama Rojas, C. (2024). *Respuestas ante incidentes cibernéticos: Guía práctica para organizaciones*. Editorial Innovatec.

Valencia Soto, E. O. (2023). *Guía para el diseño de simulacros de incidentes de ciberseguridad a través de la adaptación de estándares y metodologías como ISO/IEC 27035, NIST SP 800-61 y NIST SP 800-84 en el Banco Popular* [Trabajo de grado, Universidad Piloto de Colombia]. Repositorio institucional. <https://tinyurl.com/2mz29xek>