Evaluación y propuesta de acciones de mejora para el funcionamiento de los data center

Andres Zapata Gomez

Asesor

MSc. Ing. Iván Camilo Nieto Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Ingeniería de Telecomunicaciones

2025

Agradecimientos

Para alcanzar los logros que he conseguido, formarme como la persona que soy actualmente, Aquella persona que siempre creyó en mí; tanto en los buenos y malos momentos, que su amor y su incondicionalidad fue inimaginable, que me brindo toda su sabiduría y su conocimiento de la vida para poder afrontar todo lo que conlleva, aquella vida que no se detiene, que no tiene contemplaciones y siempre te pone a prueba, aquella persona que siempre tuvo una palabra para guiarme a ser una mejor persona, a no desfallecer, a no caer de rodillas antes las dificultades, agradecer lo que no pude agradecer en aquellos últimos momentos de vida, quien ya no me acompaña en este plano, pero me acompaña desde aquel punto en el que no conocemos hasta no cumplir con nuestra misión en la tierra. A mi querida y amada Madre MARIA EUGENIA GOMEZ ESPINOSA, a quien le debo todo y a quien le agradezco infinitamente su incondicional amor, su paciencia, y su forma de ser templada para no dejarme salir al mal camino y su esfuerzo a pesar de su salud en los últimos años. A ti te debo todo para brindarte este paso adelante para ser ejemplo de lo que me queda de familia.

Ahora el agradecimiento a amada mi Hija VICTORIA ZAPATA PARDO, quien con su corta edad me ha demostrado que hay mucho por aprender en la vida, que con su paciencia y entendimiento me ha demostrado que día a día se logra avanzar. Cada momento que he podido compartir con Ella pese a las dificultades y con enormes alegrías; ha sido el pilar para no detenerme, seguir avanzando y ser ejemplo de lograr los objetivos. Es ella quien me da un nuevo rumbo, un nuevo horizonte para crecer y acompañarla para siempre.

ANDRES ZAPATA GOMEZ

Resumen

El mundo evoluciona aceleradamente, y los sistemas de información en línea cada vez tienen mayor impacto para la sociedad, la forma de interacción se ha trasladado a entornos digitales, razón por la cual personas, empresas e incluso gobiernos han decidido adaptar mecanismos de comunicación en línea, siendo este espacio virtual, el escenario principal para salvaguardar información de todo tipo, desde registros de clientes, hasta grandes bases de información financiera, datos confidenciales e incluso decisiones gubernamentales. En ese sentido, los Data Centers se han convertido en sistemas de almacenamiento en línea fundamentales durante el proceso, los que permiten la operabilidad de empresas y gobiernos al proteger y organizar toda la información que estos depositas, hablando de datos masivos que demandan instalaciones físicas apropiadas para el desarrollo. El problema de esta situación es que la seguridad es uno de los desafíos más complejos de afrontar, ya que por el tipo de información que guardan, deben tener un esquema estructurado para garantizar protección de información, y aun así, son propensos a hackeos, acceso no autorizados y corrupción a sistemas. Aún con las mejores adaptaciones, los Data Centers son vulnerables a múltiples amenazas cibernéticas, como ataques de denegación de servicio (DDoS), Ransomware, phishing e inyecciones SQL, lo que pone en riesgo la confidencialidad y la operatividad de las organizaciones que dependen de ellos.

Para abordar esta problemática, se piensa en la IA como alternativa de protección, pero tras una exhaustiva investigación, se descubrió que esta no puede actuar por sí sola, sino que debe estar adaptada con múltiples mecanismos de protección que van desde adaptaciones al espacio físico, hasta estrategias puntuales para garantizar la protección de la información.

***Palabras clave*:** Ciberataque, Data Center, Seguridad.

Abstract

The world is evolving rapidly, and online information systems are increasingly impacting society. The way we interact has shifted to digital environments, which is why individuals, companies, and even governments have decided to adapt online communication mechanisms. This virtual space is the primary setting for safeguarding all types of information, from customer records to large financial databases, confidential data, and even government decisions. In this sense, data centers have become fundamental online storage systems in the process, enabling the operation of companies and governments by protecting and organizing all the information they store. This massive amount of data requires appropriate physical facilities for development. The problem with this situation is that security is one of the most complex challenges to face. Due to the type of information, they store, they must have a structured framework to guarantee data protection. Even so, they are prone to hacking, unauthorized access, and system corruption. Even with the best adaptations, data centers are vulnerable to multiple cyber threats, such as distributed denial-of-service (DDoS) attacks, ransomware, phishing, and SQL injections, which put the confidentiality and operational capabilities of the organizations that rely on them at risk.

To address this problem, AI is considered as a protection alternative, but after extensive research, it was discovered that AI cannot act alone but must be adapted with multiple protection mechanisms, ranging from adaptations to the physical space to specific strategies to ensure information protection.

Keywords**:** Cyberattack, Data Center, Security.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

El mundo evoluciona aceleradamente, y los cambios que se generan van en todos los ámbitos, desde las relaciones personales hasta las formas de trabajo y educación. De acuerdo con Velazco (2025), los avances tecnológicos y digitales han llevado a que todas las comunidades del mundo se adapten a nuevos mecanismos de interacción, dónde las Tecnologías de la Información y la Comunicación (TIC por sus siglas), son el eje primario que sostiene todo ese proceso comunicativo.

Por esta razón, el siglo XXI se enmarca en una revolución tecnológica en la que todo se basa en Internet, comunicaciones en línea, páginas web y redes sociales, lo que permite que ya no sea necesaria solo la presencialidad para interactuar con otra persona, para comunicarse con una empresa o para adquirir un producto. De acuerdo con Polo (2020), este es un efecto derivado de la sociedad digital, y es la nueva realidad, donde toda la humanidad se adapta.

En ese sentido, para las empresas innovar ya no es un valor agregado, es una obligación que demanda acciones para adaptarse a este nuevo contexto, y atender las demandas de los clientes en los nuevos esquemas de comunicación e interacción (Goerlich, 2019), dónde las redes digitales, como una página web o redes sociales, ya no son solo canales alternativos de comunicación, sino son la fuente principal de contacto con clientes, y el esquema que puede representar oportunidades de venta y negocios.

En ese sentido, hay un problema en toda esta situación, y es que, de acuerdo con Anžel et al. (2021), para que una empresa pueda tener un esquema digital y pueda gestionar bases de sus clientes y otra información relevante al negocio, debe tener dónde almacenar dicha información, y la nube es el lugar adecuado para ello, sin embargo, Swatisipra et al. (2024) afirman que uno de los retos más grandes de este modelo moderno de interacción, es la seguridad de la

información, porque muchas veces este tipo de mecanismos pueden representan un riesgo para esta.

En entornos digitales, es sencillo quebrantar el esquema de seguridad de la información, si bien existen cada vez más técnicas de cifrado y protección de datos, la seguirdad sigue siendo un tema preocupante, porque información delicada y confidencial puede ser violentada muy fácilmente con el conocimiento adecuado en redes digitales y programas de hackeo (Prakash et al., 2025), y para responder esta problemática, se crean infraestructuras apoyadas en tecnología, como los Data Center, para almacenar de forma segura, eficiente y funcional toda la información.

De acuerdo con Li et al. (2024), un Data Center es una infraestructura tecnológica que se crea con el fin de almacenar, procesar y gestionar grandes volúmenes de información de manera segura y funcional, de modo que una empresa pueda contratar este servicio, y albergar allí información sobre sus clientes, que para el caso de grandes empresas como bancos, es información delicada, confidencial y masiva, superando más de 10 millones de clientes, cada uno con datos importantes como información personal, certificados, actividades, movimientos, etc.

Por esta razón, los Data Center son tan importantes, y para garantizar su seguridad y funcionamiento, hacen uso de servidores, sistemas de almacenamiento, redes y otros componentes que permiten disponibilidad total de la información, es decir, que tienen un funcionamiento ininterrumpido las 24 horas, con servicios digitales para ofrecer disponibilidad y seguridad (Liu et al., 2024), pero aún con tantas implementaciones, no están exentos de sufrir algún tipo de ataque cibernético.

Las causas que motivan ataques a la seguridad informática de los Data Centers son por la información que albergan, ya que “son el núcleo operativo de organizaciones, tanto públicas

como privadas, con información importante y confidencial" (Helali & Nazih, 2021, pág. 91), y para garantizar las operaciones, se debe tener disponibilidad de la información. En ese sentido amplio, la seguridad va más allá que solo proteger de ataques cibernéticos, también para evitar pérdidas de la información o fallos que no permitan acceder a la misma.

La divulgación o transgresión de la información alojada en un Data Center puede generar daños de gran magnitud a la organización que los requiere, desde pérdida de información hasta un uso indebido de datos confidenciales, lo que se traduce en pérdidas económicas grandes y problemas legales, ligado a daños a la reputación de la organización por el incumplimiento de normativas de protección de datos (Cardenas, 2023).

Por todo esto, es fundamental contar con estrategias efectivas para proteger y garantizar la seguridad de la información de un Data Center, y el presente documento tiene por objetivo realizar una propuesta de mejoramiento de este esquema a partir de una revisión de literatura disponible del tema, identificando por ejemplo, los impactos que tienen nuevas tecnologías como la Inteligencia Artificial para proteger y garantizar la seguridad de la información.

Para alcanzar dicho objetivo, se sigue una metodología de trabajo no experimental, bajo la ruta cualitativa con un enfoque de revisión documental, para identificar, desde la literatura disponible, los mejores mecanismos de protección de información en Data Centers, y estructurar un esquema estratégico para prevenir cualquier problema derivado a esta situación.

Descripción del Problema

En el contexto moderno, los Data Centers son infraestructuras elementales para el almacenamiento, procesamiento y gestión de datos en línea para múltiples sectores, sin embargo, Vinoth et al. (2022) explican que debido a una creciente digitalización y la modernización de las amenazas cibernéticas, en la actualidad se han incrementado los riesgos de vulneraciones de seguridad, lo que compromete la confidencialidad, integridad y disponibilidad de la información, lo que se puede resumir en impactos como:

Corrupción de Sistemas en Línea: Dañar un sistema de información para quebrantar la estructura o alterar el funcionamiento de una empresa o gobierno debido a la corrupción en la información, lo que, al frenar las operaciones, puede ocasionar distintos impactos sociales según el tipo de información que se reposara en él, como sistemas financieros, administrativos, de salud o simplemente negocios comerciales que no puede continuar con sus operaciones.

Pérdida de Información Importante. Según Kim et al. (2025), cuando un Data Center es atacado, muchas veces se realiza por competidores o entidades inescrupulosas cuyo objetivo no es robar información, únicamente eliminarla para que se afecten las operaciones, transparencia, credibilidad o funcionamiento de una empresa o entidad que alberga información en estos sistemas.

Filtración de Datos Importantes. Vinoth et al. (2022) explican que los Data Center son los nuevos esquemas de almacenamiento de datos importantes como la banca, por lo que en la actualidad, la mayoría de empresas, personas y bancos los utilizan con medio principal, y esto implica guardar información sensible como estados de cuenta o información personal de cada personal, lo que, tras su filtración, puede comprometer su seguridad y generar impactos negativos, incumpliendo principios de seguridad.

Existen muchos más impactos negativos tras quebrantar la seguridad de un Data Center, sin embargo, estos trabajan activamente para preservar la seguridad y evitar que estos se materialicen, razón por la cual, Marwan et al. (2024) explica que constantemente hay actualizaciones de seguridad como nuevos cifrados de información, firewalls, protocolos de seguridad, contraseñas fuertes, e incluso estrategia físicas como sistemas de alarmas, control climático para evitar recalentamiento y fallos, alimentación ininterrumpida, etc., pero más allá de tantos esfuerzos, los riesgos cada vez son más grandes.

Según Özkan et al. (2022) la evolución tecnológica y digital también beneficia a personas inescrupulosas que quieran quebrantar sistemas de almacenamiento, como Data Centers, porque en muchos casos esto puede representar un beneficio grande por el tipo de información que contiene y puede ser corrompida, razón por la cual, independiente a nuevas adaptaciones de seguridad, las amenazas también son más fuertes con el tiempo.

El problema frente a esto es que cuando un Data Center presenta problemas en la seguridad, de modo que la información que alberga se ve amenazada, para ser eliminada, divulgada o modificada, se hacen evidentes muchos problemas derivados, desde sanciones legales, hasta sanciones económicas que pueden afectar el funcionamiento de todo este ecosistema. Esta es una realidad, que con el desarrollo informático demanda cada vez nuevas y mejores estrategias para garantizar la seguridad de la información en un Data Center.

Todo lo anterior lleva a formular la siguiente pregunta de investigación que pretende ser resuelta con el desarrollo de este documento.

¿De qué manera se puede fortalecer el esquema de seguridad de la información en un Data Center para garantizar continuidad operativa?

Justificación

La digitalización es una realidad del mundo moderno, y por este auge donde todas las comunicaciones ya sea entre personas, empresas e incluso gobiernos, se dan por entornos digitales, hace de los Data Centers la columna vertebral de este sector informático, siendo la infraestructura necesaria para almacenar y garantizar el procesamiento y transmisión de información que puede ser determinante para cualquier comunicación o gestión con datos en línea (Townend et al., 2019).

A partir de esta situación, esta investigación propone un mecanismo de seguridad para un Data Center considerando que la información que alberga suele ser importante, confidencial y de ser publicada o expuesta, puede generar impactos muy negativos para la organización, y es que, según Thapa & Camtepe (2021) el desarrollo tecnológico y digital, ha traído consigo un incremento en las amenazas cibernéticas y riesgos a la seguridad de la información, por lo que es indispensable contar con esquemas de seguridad completos, y es ahí, donde se justifica la importancia de esta investigación.

Por otro lado, más allá de la imagen o los costos que pueden ahorrar las empresas, uno de los principales motivos para llevar a cabo este proyecto es la necesidad de proteger la información crítica contra accesos no autorizados, ataques cibernéticos y pérdidas accidentales, especialmente en Data Centers que manejan información delicada como cuentas médicas, datos bancarios o gestiones financieras, porque las organizaciones que dependen de un Data Center que procede todos esos datos sensibles, y si su seguridad se quebranta, el impacto social puede ser muy negativo.

En ese sentido, una brecha de seguridad tiene el potencial de generar pérdidas económicas grandes o afectar la reputación de la organización (Thapa & Camtepe, 2021), pero

peor aún, poner en riesgo la integridad de las personas afectadas con una pérdida de información delicada que deba ser confidencial y protegida, por lo que el impacto social que motiva esta investigación es igual de importante.

Esta investigación permite que un Data Center que aplique las estrategias, sea más eficiente, operativamente hablando, garantizando la continuidad de su proceso, sin afectar la integridad de la información, evitando sanciones legales, problemas civiles e incluso fallos en sus operaciones que se podrían traducir en sobrecostos.

Finalmente, este documento tiene un alcance netamente teórico, puesto que llega hasta la propuesta teórica de las estrategias, que se generan a partir de una exhaustiva revisión documental, de artículos especializados en temáticas relacionadas con los Data Center, que abordan el tema a profundidad, definen y han comprobado los mejores mecanismos para responder las demandas de seguridad de este modelo de almacenamiento de información. En ese sentido, no hay implementaciones o evaluaciones posteriores.

Comprendido esto, la motivación para desarrollar esta propuesta investigativa se basa en la tasa incremental de cibercrímenes, ya que de acuerdo con Fox (2024) los costos asociados a responder actividades cibercriminales, en 2025 se proyecta que superen los 10,5 billones de dólares en todo el mundo, con un crecimiento estimado del 15% con respecto a 2024 que fue de más de 9.13 billones de dólares, cifra preocupante que está en aumento ya que está directamente relacionada con el número de ciberataques, que cada año siguen incrementando -ver Figura 2-.

Entonces, es claro que el gasto mundial que se genera por respuesta (no prevención, solo respuesta) a ciberataques es muy alto y este dinero puede destinarse a otros fines porque de acuerdo con Bonnie & Fitzgerald (2025), estos ataques siempre son prevenibles con los

protocolos adecuados, ya que con un esquema de seguridad realmente estructurado que evita filtraciones y el hurto de información.

Ahora bien, más allá de los costos que genera la respuesta a un ataque cibernético, la moticaicón a este proyecto se genera en que los Data Centers se han convertido en objetivos críticos dado su rol estratégico como custodios de información sensible, de modo que no solo albergan datos pasivos en Internet, también información de alto impacto para sitio de gobierno y grandes multinacionales (Canchig & Patricio, 2022).

De hecho, según el informe de IBM y Ponemon Institute, el costo promedio global de una brecha de datos en 2024 alcanzó los 4,88 millones de dólares, un aumento del 10% respecto al año anterior y el nivel más alto registrado hasta la fecha (Vijayakumar & Duraimutharasan, 2024), y en este sentido, más del 46 % de las brechas involucran información personal identificable como números fiscales, direcciones o correos electrónicos, lo cual incrementa los riesgos reputacionales y legales para las organizaciones sin mecnionar el gasto económico por números de tarjeta o extractos bancarios.

Además, se entiende que los data centers cumplen con los estadandes de protección de datos; sin embargo, se pueden realizar optimizaciones de dichos estandares mejorando y enfocando a nuevas brechas de seguridad que se están dando en apertura con el uso de nuevas y mejores tecnologias implementadas para servicios mostrando la fragilidad del modelo operativo si no se aplican estrategias integrales de seguridad, porque en particular, Data Centers que manejan información altamente sensible enfrentan impactos devastadores en caso de exposición, y esto motiva su fortalecimiento en seguridad, aspecto que esta monografia propone.

Objetivos

Objetivo General

Proponer estrategias de mejoramiento que fortalezcan el esquema de seguridad de la información en un Data Center aportando a la continuidad operativa.

Objetivos Específicos

Relacionar soluciones de inteligencia artificial y aprendizaje automático para la detección y respuesta en tiempo real a amenazas cibernéticas, asegurando una protección proactiva y adaptativa contra ciberataques a partir de la literatura disponible.

Identificar los riesgos asociados a la información que albergan los Data Center definiendo mecanismos de acción que permitan la prevención de posibles vulnerabilidades

Desarrollar un esquema metodológico de capacitación al usuario con las mejores estrategias de seguridad de la información, complementando los procesos existentes.

Metodología

En este capítulo se presenta la metodología de trabajo que seguirá el desarrollo de esta investigación, siendo definida por tres fases secuenciales que den respuesta a los objetivos de esta monografía. En ese sentido, se sigue la ruta cualitativa, la cual Hernández & Mendoza (2019) definen como "aquella investigación que permite conocer el trasfondo detrás de un determinado fenómeno social, cultural, ambiental o económico" (pág. 44) de forma que no involucra cuantías o análisis de datos numéricos, únicamente rasgos, hechos, y análisis teóricos, que, en este caso, todo estará enfocado a la seguridad informática de un Data Center.

El primer mecanismo es caracterizar la situación de seguridad en los Data Center, para lo cual es necesario aplicar un enfoque descriptivo, qué, según Vasilachis (2020) se basa en caracterizar algún contexto específico, y conocer la forma en que se desarrolla, identificando el trasfondo de sus atributos y variables, como es la sociedad digital, el desarrollo informático y las causas que motivan a proteger la información en línea.

Finalmente, para el desarrollo de las estrategias, se realizará una revisión documental que permita analizar posturas de otros autores con literatura académica y científica que ha estudiado el tema a profundidad (Casasempere, 2020), buscando conocer la eficiencia de estrategias de protección de la información en Data Centers, resultados y otros factores asociados a esta situación, con los hallazgos de otras investigaciones.

Fases de Investigación

Para seguir estos dos componentes, se plantea una metodología de trabajo dada por tres etapas secuenciales, empezando por dar contexto al proyecto, explicando los avances en materia tecnológica, la sociedad digital y la importancia de las Tecnologías de la Información y la

Comunicación (TIC), de modo que se permita comprender el impacto que tienen los Data Center en esos esquemas de información en línea.

Con esto, se busca abordar como la inteligencia artificial y el aprendizaje automático son herramientas para la detección y respuesta en tiempo real a amenazas cibernéticas, asegurando una protección proactiva y adaptativa contra ciberataques, identificando luego los riesgos que puedan corromper la seguridad de la información en un Data Center, definiendo sus respectivos mecanismos de acción para prevenir esas posibles vulneraciones.

Finalmente, se busca desarrollar un esquema metodológico de capacitación al usuario con las mejores estrategias de seguridad de la información, complementando los procesos existentes para un Data Center, todo desde la literatura disponible, con un enfoque netamente investigativo y sin un componente práctico debido a las limitaciones temporales.

Criterios de Inclusión y Exclusión de Documentos

Para esta investigación serán incluidos únicamente documentos, artículos científicos y académicos, así como tesis de grado que sean publicados en fuentes confiables como revistas indexadas y bases de datos como Web Of Science, Google Académico, Scielo, Redalyc, Scopus, etc. Los criterios de exclusión de presentan a continuación en la Tabla 1.

Tabla 1

Criterios de Exclusión para la Investigación Documental

Criterio	Exclusión
Validez Científica	Documentos sin una validez clara en materia científica, académica o gubernamental.
Fecha de Publicación	Para la revisión documental, artículos publicados con más de 6 años de antigüedad, solo se permiten del rango 2019-2025. Este criterio no aplica para material gubernamental, histórico o noticas.
Idioma de Publicación	Se excluyen artículos o documentos en idiomas que no sean inglés, español y portugués, se permite su versión traducida.
Generalidad	Se excluyen trabajos o artículos duplicados, y todos deben tener acceso gratuito al resumen cuando menos.
Publicación	Para la revisión documental, solo se permiten utilizar artículos de validez científico publicado en base de datos de Web of Science.

Nota. Son criterios establecidos con percepción individual frente a la pertinencia de la investigación. *Fuente*: Autoría Propia

Marco Referencial

En este capítulo se presentan todos los referentes teóricos que soportan la investigación para comprender conceptos y elementos previos que fundamentan el desarrollo, desde teorías, hasta otros artículos que han estudiado el tema a profundidad.

Marco Conceptual

Un Data Center es definido por Long et al. (2022) como una instalación física que almacena y gestiona los datos de una empresa o entidad que es depositada por medios digitales, por lo que, para su funcionamiento, requiere un Hardware grande, con servidores y unidades de almacenaje, así como sistemas TI. Para que un Data Center garantice su seguridad, debe existir un proceso de autenticación y control de Accesos, de modo que la información esté protegida ante entidades no autorizadas.

La autenticación es el proceso que verifica la identidad de un usuario o sistema antes de permitir el acceso (Patel, 2021), y puede realizarse mediante credenciales como contraseñas, biometría, tokens o autenticación de múltiple factor. El control de acceso es el mecanismo que determina qué recursos puede utilizar un usuario autenticado, basado en reglas y permisos, como basado en roles, según tributos, dispositivos o archivos y red.

Por otro lado, Canchig & Patricio (2022) explican que hay múltiples esquemas de seguridad en un Data Center, empezando por el acceso, donde los datos son cifrados, que este corresponde al proceso en el que se transforma la información en un formato ilegible para protegerla contra accesos no autorizados, es decir, una primera capa de seguridad, considerando que hay cifrados como claves, par de claves, durante la transmisión, en tránsito o reposo (AES, SSL, etc.).

Los Firewalls filtran el tráfico de red según reglas de seguridad, y pueden ser de hardware, software o basados en la nube. El IDS (Intrusion Detection System por sus siglas en inglés) es otro concepto fundamental, siendo el sistema que monitorea y alerta sobre actividades sospechosas, pero no interviene ya que su diseño es para aplicar otros mecanismos como el IPS, que por sus siglas es Intrusion Prevention System, y este bloquea amenazas en tiempo real (IBM, 2024).

El trabajo en la nube es básicamente el uso de plataformas como AWS, Azure o Google Cloud para almacenar y procesar datos sin requerir un espacio físico en el lugar de trabajo en red, y para ello, se realizan copias de seguridad automáticas para recuperación en caso de fallos. La redundancia de datos es la replicación de información en múltiples ubicaciones para garantizar disponibilidad (Alouffi et al., 2021).

Otro concepto es el Plan de Recuperación ante Desastres, siendo una estrategia para restaurar operaciones en caso de incidentes como fallos técnicos, ataques cibernéticos o desastres naturales, esto relaciona respaldos y pruebas constantes a sistema de almacenamiento. La Ciberseguridad es el esquema estratégico que se desarrolla con el fin de proteger sistemas y datos contra ataques cibernéticos (AlDaajeh et al., 2022), e incluye medidas como Firewalls, VPNs y segmentación de red, autenticación avanzada con MFA y certificados digitales.

Un ataque DDoS (Distributed Denial of Service por sus siglas) sobrecarga servidores con tráfico malicioso para dejarlos inoperativos. Las infraestructuras Híbridas con On-Premise son un modelo que combina recursos locales con la nube, que es la forma de funcionamiento de un Data Center, un espacio físico para almacenar contenido digital.

Marco Teórico

Ciberseguridad y Protección de Información en Data Centers

La revolución digital ha llevado a darle cada vez mayor importancia a la información en línea, razón por la que los data centers son infraestructuras críticas que almacenan, procesan y gestionan grandes volúmenes de información (Cardenas, 2023), y su rol es muy importante porque de ello dependen factores como la continuidad de operaciones en una organización o el acceso a datos confidenciales en entornos digitales.

Esta innovación es debida al aumento sobre la dependencia de la tecnología en el contexto moderno, razón por la cual la ciberseguridad y la protección de la información en estos centros se han convertido en un parámetro fundamental para garantizar la confidencialidad, continuidad operativa, privacidad de los datos y la resistencia ante amenazas cibernéticas que son cada vez mayores debido al atractivo de la información en la red (Helali & Nazih, 2021).

De acuerdo con Anžel et al. (2021) la red pasó de ser una pequeña innovación para contar con juegos o ligera información en red para interactuar con amigos, a un ecosistema completo en el cual Bancos, Empresas, Gobiernos e Instituciones Internacionales albergan su información para optimizar procesos de comunicación y desarrollo, y en ese proceso, son los data centers quienes albergan toda esa información sensible, lo que los convierte en objetivos atractivos para ciberdelincuentes (Paredes, 2024).

Los ataques pueden incluir malware, ransomware, denegación de servicio (DDoS) y accesos no autorizados, lo que puede provocar pérdidas económicas para las empresas que albergan su información, así como múltiples impactos como un gran daño reputacional y compromisos en la seguridad de los datos, considerando que la información que alberga suele ser confidencial de clientes, que en casos, pueden ser datos sensibles que comprometan su seguridad e incluso desarrollo de una empresa en la economía (Patel, 2021).

Por esta razón, es fundamental implementar estrategias de seguridad como firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS), cifrado de datos y autenticación multifactor, porque de la seguridad y la mitigación de riesgos sobre el robo de datos es lo que define el funcionamiento de este esquema de red, o el fracaso absoluto en línea.

la protección de la información en data centers no solo depende de herramientas tecnológicas, sino también de políticas y procedimientos adecuados, por ejemplo, l implementación de normas como ISO 27001 y marcos de seguridad como NIST que ayudan a establecer buenas prácticas para mitigar riesgos sobre el acceso a esta información (Pesantez et al., 2022).

En Colombia no existe puntualmente una Ley única o específica para esquemas de seguridad en Data Centers, sin embargo, si hay diversas normativas encaminadas a garantizar una protección de información y seguridad informática, que es aplicables a estos centros de datos. La entidad que se encarga de regular esto, es el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), con las siguientes normativas:

Ley 1581 de 2012. Es también conocida como “Ley de Protección de Datos Personales”, y esta establece los principios y reglas para el tratamiento de datos personales en materia tecnológica, de modo que todas las organizaciones están en la obligación de contar con un esquema fuerte de seguridad para garantizar una protección de uno de los derechos fundamentales de las personas, que es proteger su información personal, y permitir conocer, actualizar y rectificar la información que se encuentra en bases de datos o archivos.

Ley 1273 de 2009. Esta es la Ley de Delitos Informáticos en Colombia, fue creada para modificar el Código Penal y establecer un nuevo marco legal para proteger la información y los

datos, garantizando una protección de información en línea mediante penalizaciones a conductas ilegales en el ámbito de las tecnologías de la información y las comunicaciones.

Resolución 746 de 2022. Esta resolución busca fortalecer los esquemas de seguridad informática en centros de datos en Colombia, esta obliga a los administradores de todos espacios destinados al almacenamiento de información en línea a implementar y fortalecer sistemas de seguridad para garantizar que la información esté segura en la red.

Existen otras normativas para la seguridad de información en Data Centers en Colombia, pero que son aplicables en todo el mundo, como la ISO 27001, aspectos que Colombia acoge con el fin de garantizar que la seguridad de la información sea preservada correctamente en línea.

Casos de Éxito en Data Center

Existen múltiples casos de éxito de empresas, iniciativas o proyectos que han empleado diferentes mecanismos para fortalecer sus esquemas de seguridad en los Data Center, un ejemplo de ello es presentado por AWS Amazon (2020) con el caso de Capital One, cuando realizó la Migración a Amazon Web Service (AWS) y seguridad integral, pues el sistema de almacenamiento de datos en línea de Capital One completó la migración de ocho centros de datos locales a AWS, convirtiéndose en el primer banco de EE UU “all-in” en la nube .

La forma en la cual este Data Center operó esta optimización en seguridad, se basó en mecanismos de seguridad dados por la arquitectura de red, ya que de acuerdo con Engström et al. (2023) Amazon VPC es una implementación del AWS con subredes públicas y privadas y gateways NAT, aislando servicios internos de la Internet pública, de modo que se conseguía adoptar mecanismos con un cifrado TLS para datos en tránsito y AWS KMS para cifrado en reposo, garantizando confidencialidad y cumplimiento de PCI DSS.

En esto, Amazon GuardDuty y Amazon CloudWatch son otras adaptaciones de seguridad para alertas en tiempo real, análisis forense y responder a incidentes rápidamente frente a alguna posible vulneración que quebrantarían al sistema de seguridad de datos, y con AWS IAM con políticas granulares y rotación automática de credenciales, minimizando privilegios excesivos (Engström et al., 2023).

En los resultados, la migración permitió provisión instantánea de infraestructura, aceleró la innovación con machine learning y aseguró conformidad con marcos como ISO 27001 gracias al modelo compartido de responsabilidad de AWS, garantizando no solo seguridad, sino también trazabilidad y mayor eficiencia al sistema de gestión de la información de Capital One, como banco con información en la red.

Como estos, hay más cosas, Time Inc., es otro ejemplo sobre el cual se hizo un refuerzo de controles en transición a la nube, pues la organización aprovechó su migración a AWS también, con el fin de reinventar y reforzar sus controles de seguridad en un entorno DevOps distribuido (Naseer, 2023), y para conseguirlo, implemento mecanismos de seguridad basados en la integración DevOps y seguridad, con evaluación en cada despliegue con pipelines de CI/CD.

En el proceso, el esquema de seguridad se fortaleció también para Time Inc., gracias a la automatización de auditorías con AWS Config, para evaluar configuraciones y AWS Security Hub para centralizar hallazgos de seguridad, de modo que se adaptaron microservicios aislados en contenedores, reduciendo la superficie de ataque y alertando en tiempo real cualquier posible vulneración a los datos para tomar medidas preventivas de forma automática.

Otro ejemplo es presentado por Gautam et al. (2020) siendo el de SKIDATA para mejorar su seguridad y cumplimiento global de actividades, esto a partir de los servicios de AWS

también como sistema Data Center más eficientes, gracias a la seguridad y certificaciones (PCI DSS) para su solución de control de acceso y pagos en infraestructuras distribuidas.

Los mecanismos de seguridad que permitieron este éxito en la operación de seguridad en la información se basan en redundancia geográfica, con una replicación de datos en varias regiones para alta disponibilidad y DR. Además, Amazon VPC permite crear redes virtuales aisladas con ACLs y security groups, garantizando estricta segmentación de tráfico, de modo que sea posible evitar cualquier filtración de datos o problemas de seguridad. Con esto, SKIDATA redujo latencias, mejoró rendimiento de sus terminales de pago y mantuvo alta disponibilidad en el servicio en línea.

En este escenario, Amazon no podía faltar, siendo un caso de éxito claro gracias a su propia innovación de AWS, ya que, con ello, cumplía con sus estrictos requisitos de seguridad física para fortalecer la protección a la información de los datos, al tiempo con procesos de cifrado para respaldos de bases de datos (Cárdenas & Olarte, 2022).

Para funcionar, en Amazon se implementaron controles físicos para el acceso biométrico y videovigilancia 24/7 en centros de datos AWS, así como un cifrado de backups, con la integración de Amazon S3 con Oracle RMAN, con llaves gestionadas en AWS KMS. Para conseguirlo también se dio uso de algoritmos certificados para datos en tránsito y en reposo.

Este caso también se replicó a Siemens, empresa que migró a AWS Security Hub en 2018 para unificar alertas y hallazgos de servicios como GuardDuty e Inspector, mejorando respuesta ante posibles vulneraciones de seguridad que podrían atentar contra la información de sus bases de datos (Engström et al., 2023).

Con AWS Security Hub, se agrupan todos los hallazgos de múltiples para identificar amenazas, y este modelo también se replicó al caso de Southwest Airlines, empresa que apostó

por la automatización y visibilidad en tiempo real de amenazas gracias a mejorar su seguridad en Data Center con AWS usando Security Hub, GuardDuty, Config e Inspector, reduciendo tiempo de implementación de controles de seis semanas a solamente una (AWS Amazon, 2020).

En este caso, se implementó GuardDuty & Inspector para la detección de amenazas y análisis de vulnerabilidades continuo, apoyado en un AWS Config que define las reglas personalizadas de la misma empresa, de modo que validan configuraciones y políticas corporativas para dar acceso a la información sin riesgos a la vulneración o robo de datos. Con esto, la empresa tuvo un desempeño mejor, con un escaneo mensual de más de 600,000 recursos con 98 % de conformidad, mayor agilidad y eficiencia en respuesta a posibles vulneraciones.

Otro caso es UK Data Service, en el cual, en 2021 se combina infraestructura híbrida con AWS EC2, S3 y RDS para ofrecer acceso controlado a datos sociopolíticos manteniendo ISO 27001, todo gracias a una arquitectura híbrida con integración de on-premise y cloud para cumplir requisitos de acceso según clasificación de datos (Engström et al., 2023).

Para funcionar, en UK Data Service se adoptó el enrutamiento dinámico con políticas de seguridad que dirigen solicitudes según nivel de sensibilidad, y gracias a la certificación ISO 27001, el uso de servicios AWS generó más confianza para implementar.

Otro caso de éxito de migración a nuevos sistemas de seguridad es en Arvato Systems, con nueva defensa DDoS con Equinix y Link11, pues la empresa mitigó ataques DDoS mediante Link11 Cloud Security sobre Platform Equinix, eliminando el 90 % de llamadas de servicio relacionadas y duplicando su ancho de banda disponible (McIntosh et al., 2024).

Para funcionar esta mitigación, la implementación del sistema de seguridad con servidores externos permitió un filtrado automático en la capa de red para bloquear tráfico malicioso antes de alcanzar la infraestructura interna, y con un despliegue en múltiples IBX para

balanceo de carga y alta disponibilidad, se permitió garantizar disponibilidad, pero también mayor protección ante posibles amenazas.

El noveno caso de éxito es ClusterPower, con la innovación sostenible y seguridad con Cisco ACI, de modo que se levantó el primer centro de datos Tier III de Europa del Este, integrando Cisco UCS X-Series y ACI para ofrecer escalabilidad, eficiencia y protección en entornos multicliente, y según Prieto (2025), los mecanismos de seguridad se basaron en:

Microsegmentación. Cisco ACI desarrolla políticas de seguridad por microflujo, aislando todos los entornos de cliente y previniendo movimientos laterales de riesgo.

Control de acceso físico. Jaulas dedicadas y autenticación en hardware Cisco UCS para acceso restringido a servidores.

Orquestación. Cisco Intersight permite recopilar la información y tiene una automatización de políticas de seguridad, reduciendo errores manuales, donde todo lo hace la misma programación.

El caso de Green Mountain es otro caso de seguridad física de máxima confianza, en este caso, un DATA Center fue aislado, llevado a la en montaña con múltiples capas de seguridad física, como biometría, mantraps, CCTV continuo y personal 24/7, todo certificado Tier III por Uptime Institute, de modo que esta seguridad se basó en redundancia de perímetro y seguridad física, como cercas, control de acceso por tarjeta y detección perimetral (Green Mountain, 2025).

Resultados

La seguridad en los Data Centers es un tema cada vez de mayor impacto tanto en función de estudio como de desarrollo, es fundamental contar con constantes desarrollos que permitan optimizar este proceso de seguridad, considerando que la evolución digital ha llevado a que cada vez sea más común trabajar y conservar información en línea, y en muchos casos, información confidencial que de cierto modo, de ser quebrantada puede suponer un riesgo para la estabilidad social, las personas, empresas e incluso los gobiernos.

Entonces, el Data Center es visto como esquema central de almacenamiento que por su misma naturaleza se vuelve foco de inseguridad y posibles ataques, lo que motiva a evaluar estrategias de desarrollo en términos de seguridad y protección de información, más allá de su espacio físico. En cualquier caso, autores como AlDaajeh et al. (2022) afirman que la innovación se basa en aprovechar ese desarrollo tecnológico para garantizar protección de datos, proyectando entonces la Inteligencia Artificial como un mecanismo de seguridad en línea.

Inteligencia Artificial como Mecanismo de Ciberseguridad

El mundo evoluciona aceleradamente, y la Inteligencia Artificial (IA) evoluciona cada vez más, siendo una rama de la informática evolutiva que busca desarrollar sistemas capaces de realizar tareas que tradicionalmente requieren inteligencia humana, como el aprendizaje, tomar decisiones y el reconocimiento de patrones (Lundvall & Rikap, 2022), y estos sistemas operan con análisis de mucha información para aumentar su precisión.

Su evolución ha sido notoria, en los últimos años ha pasado de simples sistemas basados en reglas para tomar pequeñas decisiones de sugerencia, hasta un contexto moderno, donde existen modelos avanzados de aprendizaje profundo y redes neuronales, razón por la que incluso, esta innovación tecnología se ha incorporado en diferentes sectores importantes, como la salud,

la ciberseguridad y la industria, siendo motivada esta adaptación por el crecimiento del Big Data y el aumento en la capacidad de procesamiento de información en la red, permitiendo soluciones que tienen mayor enfoque y funcionalidad.

En ese sentido, Kaur et al. (2023) afirman que la Inteligencia Artificial cada vez resalta más en el ámbito de la seguridad en la red, porque tiene una capacidad fuerte de automatizar tareas repetitivas, lo que permite una mejora en la detección y respuesta ante amenazas gracias a la naturaleza del proceso, siendo esta una forma de aumentar la precisión en la seguridad de los sistemas digitales.

En términos de aplicación, los autores también afirman que las funciones de la IA están segmentadas en cinco categorías fundamentales:

La primera es la función de identificación, donde la IA optimiza el proceso de la gestión de activos, de modo que, tras una categorización, es posible evaluar riesgos que se presenten de acuerdo con la naturaleza de la información, contrastando datos históricos, posibles ataques, vulneraciones, y demás, y con todo esto, la forma de operar esta primera etapa es con un análisis predictivo para anticipar amenaza y vulnerabilidades posibles.

La segunda función es la de protección de información, como un esquema secuencial que se realiza a partir de la primera etapa, se abarca la autenticación de usuarios y dispositivos, y complementado por Cordova (2024) permite optimizar el control de acceso basado en inteligencia artificial, de modo que exista una prevención de fugas de datos y la detección de amenazas persistentes avanzadas durante el acceso.

La tercera función es la de detección, que se centra en el uso de análisis de registros, detección de anomalías y herramientas de IA para la identificación de ciberataques en tiempo

real, siendo esta una ventaja para no limitarse a lo estático, sino que dinámicamente, en función de la posible amenaza, se detecta el impacto y la forma que está operando.

En la cuarta función, la de respuesta, se desarrollan los métodos para implementar respuestas automáticas ante incidentes, sin una evaluación externa, ya que como complementan Espinoza & Quevedo (2025), la IA no tiene autonomía total, pero si tiene la potestad de actuar en automático según las condiciones de seguridad que se demande, activando protocolos preestablecidos y mecanismos utilizados en el pasado para garantizar la protección de datos e información.

Finalmente, la quinta función corresponde a la recuperación, donde la IA se utiliza para generar planes de continuidad y desarrollar estrategias de recuperación ante desastres cibernéticos, es decir, acoplar el BackUp más reciente sin una previa autorización, sino que, en automático, poder recuperar la información.

En ese sentido, esto es un modelo de desarrollo que aún tiene la necesidad de ser optimizado, principalmente en la representación de datos para la detección y análisis de amenazas, porque muchas veces los patrones no coinciden, y constantemente hay nuevos fallos que alteran la seguridad informática por los mismos avances que tienen los atacantes cibernéticos en materia de mecanismos de corrupción a sistemas (Kaur y et al., 2023) .

Bajo este panorama, el desarrollo de infraestructuras que permitan una integración más eficiente de la inteligencia artificial en la protección digital es una necesidad, de hecho, aprovechar las adaptaciones de la IA como es el análisis de grandes volúmenes de datos y la encriptación masiva con varias capas, hace que sea posible fortalecer esa barrera de seguridad para evitar que un ataque se materialice, y en este escenario, este puede ser mitigado según el rendimiento de la forma en que se llevan a cabo la protección.

Para mejorar la eficiencia de estos mecanismos de seguridad, se utiliza una exploración más profunda de los ataques recibidos en un Data Center y sobre métodos avanzados de aprendizaje automático que la IA posibilita, es posible una detección y mitigación más eficiente, porque es un sistema evolutivo que analiza el histórico y la forma del ataque y todas sus características, y sobre ello se toman medidas correctivas, las cuales, de acuerdo con Li & Liu (2021) deben estar en una constante evolución, porque día tras día se desarrollan nuevos mecanismos para alterar, quebrantar o robar sistemas de información en línea, y los mecanismos de protección deben mejorar en la misma medida.

Principales Ataques a Data Centers

Para adaptar las estrategias de seguridad en un Data Center y evitar que una corrupción de información se materialice, es necesario primero analizar el tipo de ataque al cual es vulnerable o que puede comprometer la seguridad de la información. A partir de una identificación clara del tipo de ataque es que se pueden aplicar los mecanismos como el aprendizaje automático de la IA, justificado en la sección anterior, para preservar la seguridad de los datos.

En ese sentido, según Anžel et al. (2021) los Data Centers son objetivos críticos para ataques cibernéticos debido a la gran cantidad de información que almacenan y procesan, pero debido a la naturaleza de esa misma información, el tipo de ataque que puede realizarse también va a variar, ya que no es lo mismo corromper un sistema empresarial que robar información financiera para lucro económico, y en este punto, las dos formas de entrar y corromper el sistema de información van a variar. Las principales variaciones de ataques son:

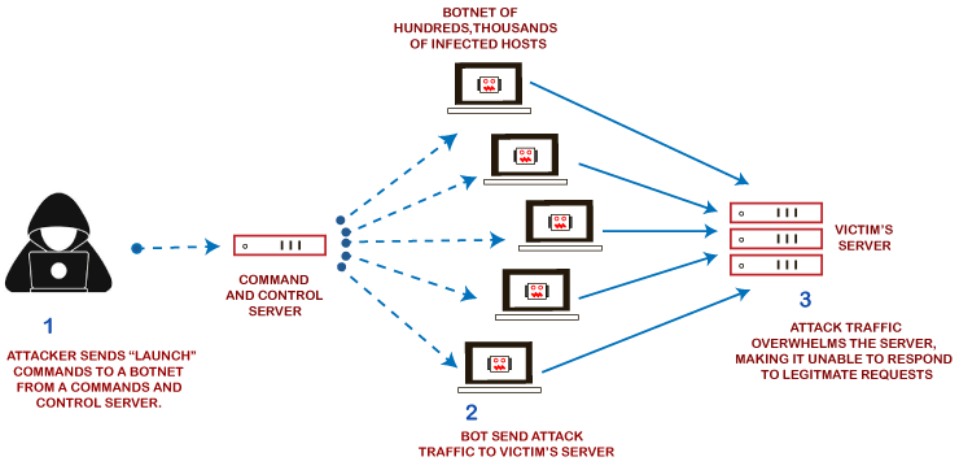
Ataques de Denegación de Servicio (DoS y DDoS)

Uno de los ataques más comunes es la denegación de servicios, siendo definida por Biswas et al. (2021) como ataques que buscan sobrecargar los servidores con un tráfico excesivo y errático, impidiendo el acceso legítimo a los sistemas y los datos, lo que corrompe su información y no permite que se puedan continuar las operaciones debido a un agotamiento de recursos sea de almacenamiento, procesamiento o respuesta.

Los DDoS (Distributed Denial of Service por sus siglas en inglés), se emplean diferentes dispositivos de forma simultánea infectados para generar tráfico masivo de 'bots' o 'botsnets', y al exceder la capacidad de procesamiento del sistema, se expulsan los usuarios legítimos y se interrumpe la operatividad del Data Center, y consigo, permitiendo acceso o daño de información (Biswas et al., 2021), su funciona básico se presenta a continuación mediante la Figura 1.

Figura 1

Proceso de Ataque DDoS



Nota: Pieza grafica de explicación del ataque DDoS. Tomado de Sadeghi (2024)

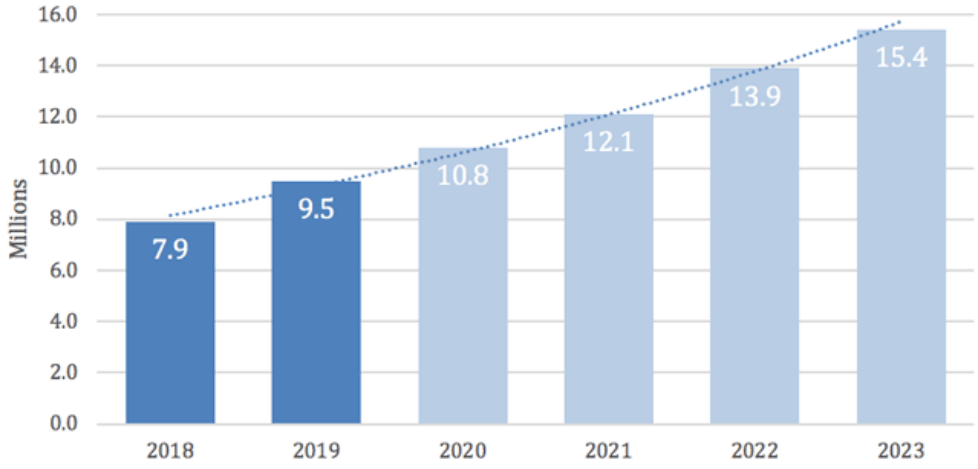
Uno de los problemas que se generan alrededor de esta situación es que se pueden provocar tiempos de inactividad prolongados, afectando la continuidad operativa de las empresas

que dependen del Data Center, sin embargo, Mahdavi & Rahmani (2023) afirman que una de las limitaciones es que los DDoS se puedne prevenir solo con evitar el tráfico al Data Center, pero esto implicaría que un usuario que realmente deba ingresar y operar con esta información, también tendrá restringido el paso, lo que ocasionaría que de igual forma, la operabilidad se afecte, y filtrar el acceso es una de las tareas más complejas, porque es común adaptar mecanismos como las VPN y la modificación de IP, para hacer pasar un acceso indebido como "válido".

Este tipo de ataque cibernético se emplea para sistemas donde el objetivo principal no es robar información, sino afectar la operabilidad de un sistema como una institución, y, de hecho, el reporte anual de ciberseguridad de Cisco (2023) citado por Haider (2024) afirma que este tipo de ataque aumenta su incidencia cada año, llegando a más de 15 millones de casos registrados en 2023. La Figura 2 muestra esa tendencia de incremento en ciberataques.

Figura 2

Tendencia de Incremento en Ciberataques DDoS



Nota: Analisis anual para revision historica. Tomado de Cisco (2023) citado por Haider (2024)

La preocupación se genera frente a esta situación, porque cada vez es más popular este tipo de ataque en Data Centers y por el servicio que se ofrece en este sistema de almacenamiento

de infromación, restringir el acceso es una idea compleja que puede afectar la operabilidad, así que se deben adoptar otros mecanismos como auditoría basada en IA o análisis masivo de registros para validar patrones específicos de acceso al Data Center -ver Acápite 7.3-.

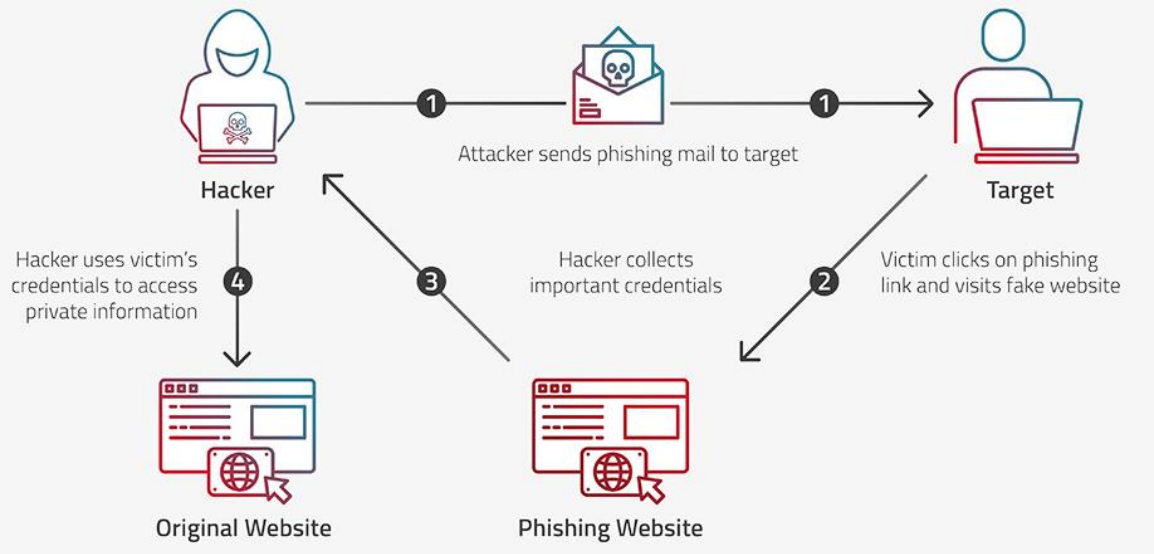
Ataques de Ingeniería Social y Phishing

El segundo tipo de ataque más común es la ingeniería social y Phishing, siendo definido por Nanda et al. (2024) como aquel en el que se emplean mecanismos poco convencionales para corromper un sistema informático y de almacenamiento de datos, con tácticas de manipulación digital, donde los atacantes engañan a empleados o personas que puedan acceder al Data Center mediante mensajes de texto, correos o cualquier otro esquema que busque acceder al sistema con solo ser abierto, obteniendo credenciales de acceso o información confidencial y consigo, la toma de datos.

El funcionamiento general de este tipo de ataque se presenta en la Figura 3.

Figura 3

Proceso de Ataque Phishing a un Data Center o Sistema de Información



Nota: Análisis gráfico de Phishing. Tomado de Radware (2024)

La forma en la cual el acceso se da, es cuando se envía un mensaje de texto, mail o enlace por algún sistema de información en línea a alguna persona que tenga acceso al Data Center (Target), esta persona lo abre, considerando que este enlace va maquillado para hacerse ver como un enlace tradicional de acceso o algo de seguridad para prevención de fallos.

Ante el acceso, el hacker tiene el acceso al portal de información, y una vez dentro, con las credenciales de la persona que tiene acceso al Data Center, puede realizar su ataque, considerando que, para efectos de registro en sistema, se detecta un acceso normal con la IP y credenciales normales de una persona autorizada, y es allí donde se deben aplicar mecanismos especiales de detección de fallos y mecanismos de respuesta para fortalecer la seguridad.

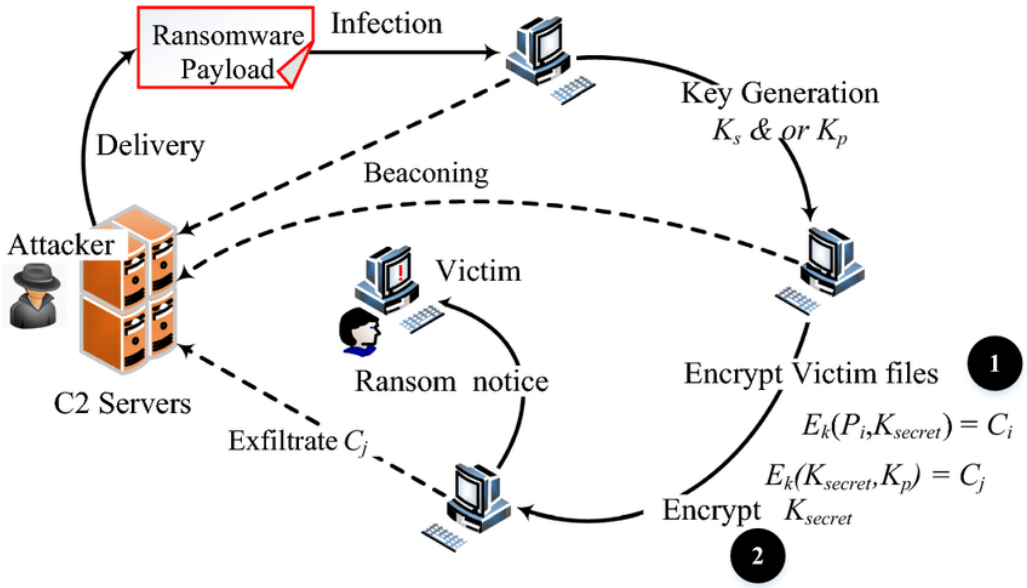
Ransomware

Es un tipo de malware que cifra los datos del Data Center y exige un pago para su liberación, este es común por temas económicos, donde se amenaza con afectar el funcionamiento del Data Center a cambio de una cuantía económica, y estos ataques pueden paralizar operaciones fundamentales de funcionamiento y generar grandes pérdidas económicas para el sistema informático (McIntosh et a., 2024).

La forma de funcionar se presenta a continuación mediante la Figura 4, en la que se muestra el mecanismo y paso por partes para materializar un ataque de este tipo, donde se encripta información tras un acceso no autorizado por mecanismos como Phishing para poder quebrantar el sistema.

Figura 4

Ataque Ransomware a un Data Center o Sistema de Información



Nota: Pieza grafica de proceso de ataque Ransomware. Tomado de (Zimba & Chishimba, 2019, pág. 10)

Ataques de Inyección SQL y Credential Stuffing

Este tipo de ataques ocurren cuando un atacante inserta código malicioso en consultas SQL para acceder, modificar o eliminar información en bases de datos, por lo que su objetivo tiende a enfocarse hacia la corrupción del sistema y no hacia el robo de información, con el fin de comprometer la integridad de los datos almacenados. Los atacantes utilizan software automatizado para probar múltiples combinaciones de contraseñas hasta obtener acceso con el Stuffing y se emplean credenciales robadas en otros sitios para intentar acceder a los sistemas del Data Center (Marwan et al., 2024).

Malware y Spyware

Los malware pueden infectar los sistemas del Data Center, dañando archivos o permitiendo el acceso remoto a los atacantes. El spyware recopila información de manera clandestina y la envía a actores malintencionados (Sowka et al., 2025).

Ataques a la Infraestructura Física

Uno de los problemas que tienen los Data Centers, es que operan en línea todo el tiempo, pero su esquema de desarrollo es en infraestructura física, lo cual es necesario, pero puede hacerlo vulnerable frente a ataques que puedan hacerse en físico, como autorizaciones no permitidas de acceso, o incluso ataques dados por suministros de energía (con cortes), e incluso generando daños a la estructura física.

Ataques Man-in-the-Middle (MITM)

Estos ataques ocurren cuando un atacante intercepta la comunicación entre dos sistemas para robar o alterar la información transmitida (Sowka et al., 2025).

Principales Estrategias de Seguridad

Una vez comprendida la amenaza constante que ataña las operaciones y que puede afectar el rendimiento de un Data Center, es importante desarrollar un esquema estructurado y completo para la protección de la información y prevención ante los ataques. Si bien se ha demostrado que la IA puede ser potencialmente una estrategia de desarrollo, esta debe estar guiada con mecanismos tradicionales, como los que se presentan más adelante, y de modo que permita garantizar la seguridad en un Data Center.

A continuación, se presentan los mecanismos de seguridad para garantizar la protección de datos e información en un Data Center según avances actuales, estos se han organizado de lo macro hasta lo específico, por lo que se empieza hablando de las estrategias de seguridad dadas por factores físicos, y termina con adaptaciones puntuales para mejorar este esquema desde los mecanismos específicos, la inteligencia artificial y demás.

Las Ocho Capas de la Protección Física en Data Center

El primer mecanismo es la protección física, y es que, Praveen (2024) afirma que para que un Data Center se mantenga operante, este debe tener una infraestructura capaz de almacenar toda la información que se alberga allí, y a pesar de ser administrada, modificada y gestionada por medios digitales de forma remota, físicamente el Hardware es muy vulnerable, siguiendo el séptimo ataque principal más común hacia los Data Centers.

En ese sentido, Praveen (2024) propone un mecanismo dado por ocho capas de protección para garantizar que físicamente, un Data Center pueda garantizar seguridad en su sistema de desarrollo. Estos pasos son:

Perímetro de Seguridad. Un Data Center solo debe permitir el acceso a personal autorizado, razón por la que es importante que se implementen barreras físicas para restringir el acceso no autorizado y proteger la instalación de ataques externos y desastres naturales, considerando que un desastre natural puede afectar el funcionamiento de un Data Center y hacerlo propenso a un Ciberataque.

Caseta de Vigilancia Perimetral. En todo Data Center se debe realizar un control más apropiado de acceso con registro de visitantes, verificación de antecedentes y autorización previa para poder entrar al centro de información, en caso de que un Rack de Información sea quebrantado, se pueden generar graves impactos -ver Marco teórico-.

Entrada al Edificio. Los Data Center se encuentran en instalaciones que deben estar ventiladas y apropiadas para el almacenaje de información, en este espacio es fundamental contar con sistemas de entrada más apropiados que solo un guarda, se deben instalar detectores de metales y sistemas de rayos X para evitar el ingreso de elementos prohibidos o peligrosos que puedan afectar o vulnerar el rack de información.

Acceso a la Zona Segura. Cuando se pasan los filtros anteriores, se deben establecer esclusas de acceso con control de peso, garantizando que no se transporten objetos no autorizados.

Control de Ascensores. Se restringe el acceso a ciertos pisos del centro de datos, permitiendo la movilidad solo a personas autorizadas, de modo que alguien, aún por error, no pueda acceder a un rack de información, ya que un error involuntario puede comprometer la seguridad del sistema.

Pasillo Seguro de la Sala de Datos. Para los pasillos se deben utilizar cámaras de vigilancia y sensores de movimiento para monitorear constantemente el área y evitar accesos no autorizados, garantizando que, ante cualquier novedad, se cuente con registro de datos.

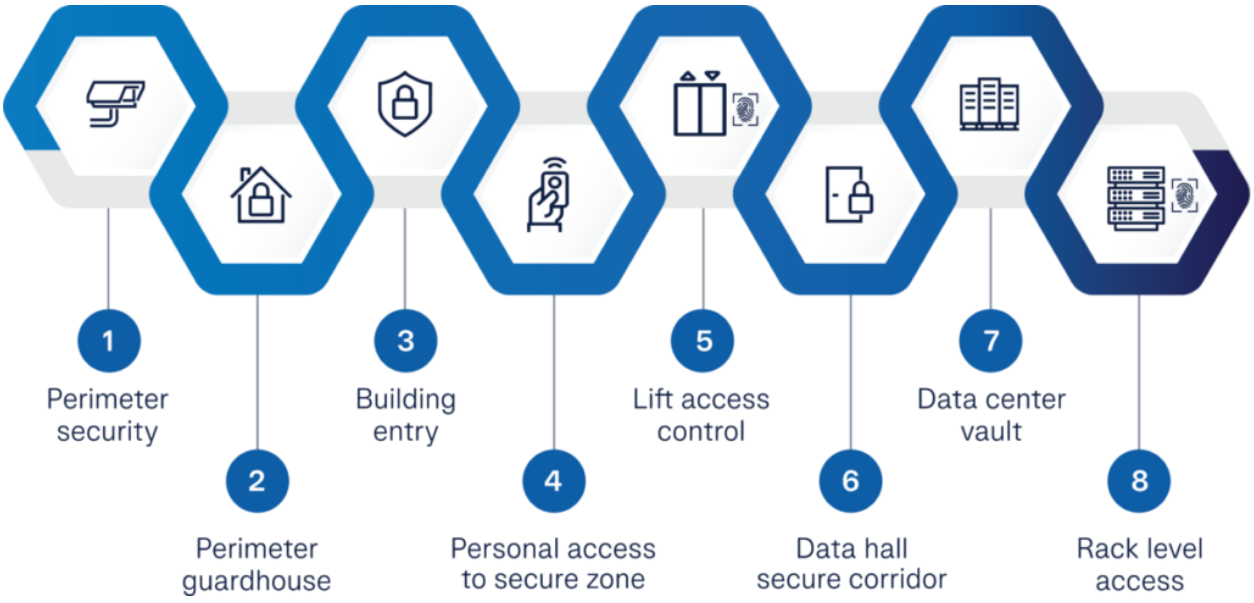
Bóveda del Centro de Datos. Se mantiene una supervisión continua mediante CCTV y control de personal para garantizar la seguridad de los servidores.

Acceso a Nivel de Rack. Solo personas previamente autorizadas pueden acceder a los racks mediante autenticación biométrica, lo que garantiza la confidencialidad de la información almacenada y la protección de la información.

El resumen general se presenta en la Figura 5.

Figura 5

Sistema de Protección General para un Data Center



Nota: Capas de seguridad física. Tomado de Praveen (2024)

Controles de Seguridad con Servidor Avanzado

Una vez se han adaptado todos los mecanismos físicos posibles para garantizar la seguridad en un Data Center, se procede a evaluar formas de control y protección de información desde el ciberespacio. Inicialmente, Goldman & Dessouky (2022) plantean que una solución integral podría ser aquella que involucra la contratación de un tercero especializado, y en caso de no hacerlo, se debe profundizar en adaptar nuevos mecanismos para proteger la información.

La protección debe integrar infraestructuras de virtualización (como VMware) y gestionar los accesos, par aadmitir únicamente la instalación de agentes en los endpoints como el uso de un Security Virtual Appliance (SVA) para protección sin agente. Para garantizar la seguridad, Goldman & Dessouky (2022) plantean que es necesario adaptar una consola de gestión unificada (llamada UMC Server), siendo la interfaz web que permite registrar, configurar y administrar las diferentes funciones del sistema.

Es un sistema que inicia desde el servidor UMC que se integra de forma física, con un servidor de gestión independiente que, ante una posible corrupción al Data Center, esta no se ve afectada porque actúa como un agente externo, y permiti distribuir la supervisión en tiempo real para prevenir alteraciones de seguridad o patrones inadecuados de comportamiento en el Data Center.

Por otro lado, el servidor de gestión de la UMC debe adaptarse en un software como Tomcat, porque es el núcleo que coordina la comunicación segura entre la consola, los agentes y otros componentes, de modo que ante un fallo, puede responder de forma dinámica el problema y garantizar operatibilidad, con funciones complementarias como la gestión de alertas, el almacenamiento masivo y seguro de eventos, y la distribución de políticas de asignación, todo en conjunto para hacer el sistema escalable y operativo.

Otro elemento clave son agentes de seguridad que se despliegan en sistemas operativos Windows, UNIX y Linux, de modo que tienen múltiples facetas y tienen la función de interceptar llamadas al sistema, alteraciones de comportamiento, aplicar políticas de prevención, monitorear eventos y registrar cambios en el sistema para posibles ataques, lo que permite identificar de forma inmediata agentes que ingresen y no sean autorizados, como mainframes o sistemas legacy.

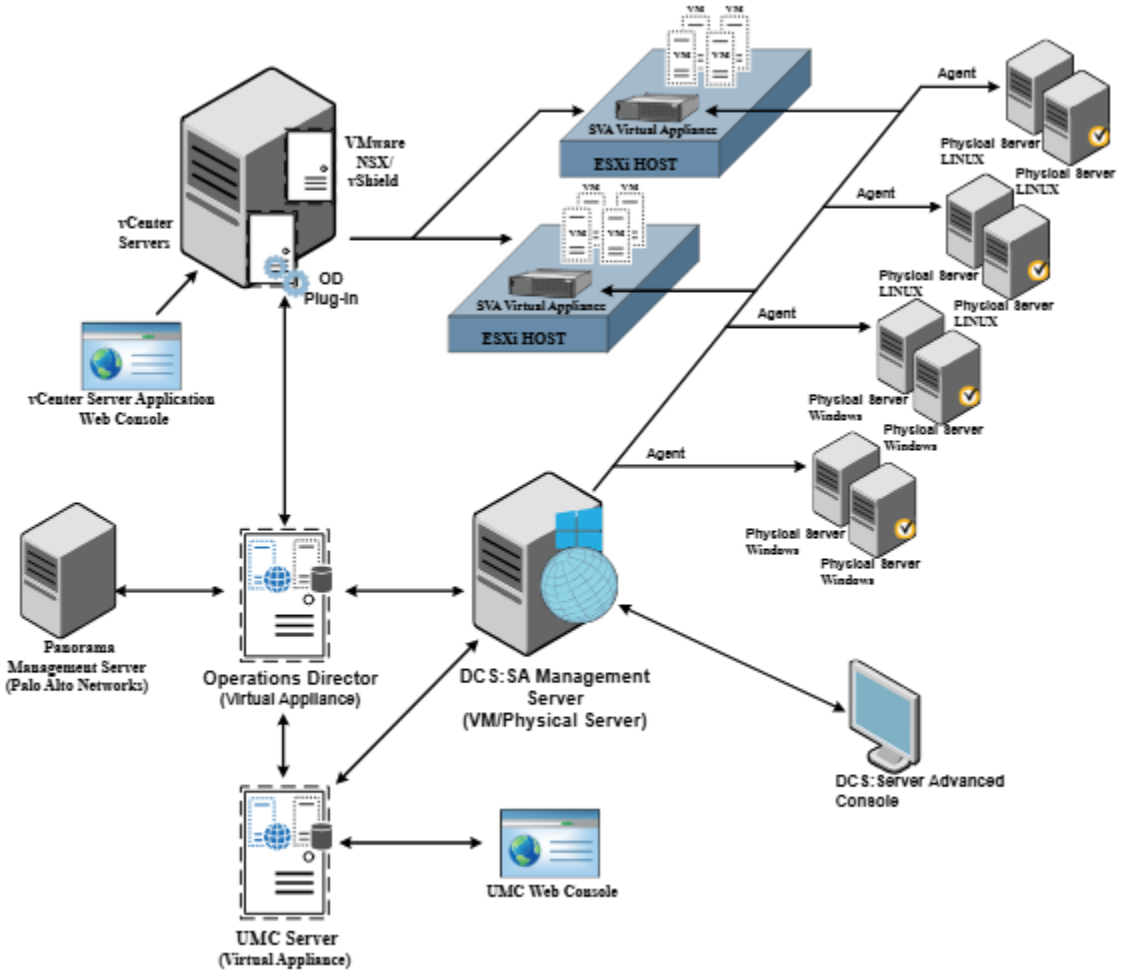
Los agentes están optimizados para operar en entornos virtuales, permitiendo detectar y prevenir amenazas en máquinas virtuales. Otro elemento indispensable es el Security Virtual Appliance (SVA), que es la protección específica anti-malware y de red sin la necesidad de instalar un agente en cada máquina virtual, lo que permite optimizar el funcionamiento de plataformas como NSX o vShield que emplean la mayoría de Data Centers. Durante la

implementación, se utiliza un número reducido de puertos configurables, con la excepción del puerto 8443, que es fijo.

Con esto, se asegura una comunicación eficiente y segura entre los componentes, incluso en entornos con NAT, y la estructura debe estar centralizada al administrador, dónde se integran múltiples capas de seguridad. Al combinar el servidor de gestión centralizado, agentes distribuidos, un SVA para entornos virtualizados y herramientas de automatización, se responde a la seguridad, siguiendo el esquema de la Figura 6.

Figura 6

Sistema de Protección General para un Data Center por Servidor Avanzado



Nota: Descripción de protección para los servidores. Tomado de Goldman & Dessouky (2022)

Resumen de Estrategias de Seguridad

Los ataques a un Data Center pueden tener un impacto considerable, pero la mejor herrmienta para combatirlos es la prevención, así, la seguridad en estos mecanismos de información digital se sustenta en dos pilares complementarios: la protección física y los controles cibernéticos avanzados, a lo que, por un lado, se implementa una infraestructura física más fuerte, es necesario que tenga un perímetro de seguridad fuerte, restringiendo el acceso únicamente al personal autorizado, y se refuerza mediante casetas de vigilancia perimetral y sistemas de control en la entrada del edificio, donde se utilizan detectores de metales y rayos X para impedir la entrada de objetos peligrosos.

Una vez dentro, se deben asignar de zonas seguras que incluyen esclusas de acceso con control de peso y ascensores de acceso restringido para limitar la movilidad en áreas propensas a ataques en el Data Center, y en todo caso, deben haber pasillos monitorizados con cámaras y sensores de movimiento, y una bóveda de servidores con supervisión continua mediante CCTV y control de personal.

Además, el acceso a nivel de rack, que es el punto más critico del proceso, se debe proteger con mecanismos como la autenticación biométrica, asegurando la confidencialidad y la integridad de la información desde el medio físico.

Ahora bien, en lo que respecta la seguridad cibernética se refuerza con controles basados en servidores avanzados que gestionan la infraestructura virtualizada, permitiendo la distribución de agentes de seguridad en sistemas operativos como Windows, UNIX y Linux, lo scuales, al ser interoperativos, hacen que no sea solo un mecanismo el que pueda afectar el sistema informático, sino tener un esquema más robusto con diferentes servidores para garantizar protección de

información ante un posible ataque a alguno de los servidores, donde los otros actuarán como respaldos del proceos.

Estos agentes interceptan llamadas al sistema, registran eventos y detectan accesos no autorizados, de modo que ante cualquier novedad, pueden generar altertas y evitar que se materialice un riesgo.

Por otro lado, la incorporación de un Security Virtual Appliance (SVA) permite garantizar la protección anti-malware y de red en entornos virtualizados, mientras que una consola de gestión unificada centraliza la administración de alertas, la configuración de políticas de seguridad y el almacenamiento seguro de eventos, facilitando una respuesta dinámica ante incidencias.

Todos estos mecanismos se pueden optimizar para garantizar mayor seguridad gracias a mecanismos como la Inteligencia Artificial, de modo que esta funcione como un apoyo programado para evitar que de cierto modo, un ataque de materialcie al tener un análisis más fuerte y adaptado a análsiis de grandes volúmenes de datos con Machine Learning. En conjunto, la integración de estas estrategias tanto físicas como digitales, mejora el sistema de seguridad escalable, y si bien no garantiza al 100%, si aumenta las probabilidades de protección de ataques cibernéticos a Data Center de manera integral la infraestructura, los datos y la operatividad del sistema para cualquier amenaza.

Conclusiones

La información es considerada el elemento más importante de una empresa, involucra datos de cualquier índole, desde registros de clientes, ventas, información sensible e incluso datos de tarjetas de pago, por eso salvaguardar la integridad de dicha información es una acción indispensable para las organizaciones, y esta reposa en Data Centers, que, en caso de ser vulnerables frente a algún ataque, las consecuencias pueden ser muy negativas.

Los Data Center son propensos a múltiples ataques, desde lo físico hasta lo virtual, y por ello es indispensable fortalecer la seguridad en estos sistemas informáticos, dada su vulnerabilidad ante amenazas cibernéticas que cada vez son más modernas y peligrosa, y es que la digitalización ha impulsado la adopción de estos centros como ejes fundamentales para el almacenamiento y gestión de datos en diferentes sectores económicos y gubernamentales, pero al mismo tiempo, ha expuesto nuevas brechas de seguridad que pueden comprometer la confidencialidad, integridad y disponibilidad de la información. Por esta razón, la seguridad de los Data Centers no solo debe enfocarse en ataques cibernéticos convencionales, sino también incluir medidas para evitar filtraciones, corrupción de datos y fallos operativos que podrían generar pérdidas económicas y reputacionales.

En ese sentido, la adopción de soluciones basadas en inteligencia artificial (IA) y aprendizaje automático (machine learning) para la detección y respuesta en tiempo real ante amenazas cibernéticas es una estrategia de alta efectividad e innovación, porque son tecnologías que permiten establecer un esquema de ciberseguridad proactiva y adaptativa, al identificar patrones anómalos de comportamiento mediante el análisis continuo de grandes volúmenes de datos. A través del entrenamiento con datos históricos, los algoritmos de machine learning pueden anticipar y mitigar ataques previamente registrados que dificultan su distribución, donde

la IA se consolida como un componente de alto impacto dentro de los sistemas modernos de ciberdefensa, gracias a las capacidades avanzadas de detección temprana, automatización de respuestas y mejora continua en la protección frente a ciberamenazas.

De esta forma, con el uso de aprendizaje automático se puede analizar la información ya recopilada y almacenada (historial) sobre ataques cibernéticos, sumando también casos externos gracias a su capacidad para procesar gran cantidad de datos y variables. Esto permite crear un esquema de seguridad más efectivo, capaz de detectar y responder a amenazas de forma proactiva y adaptativa. Aunque no garantiza eliminar por completo los ciberataques, sí ayuda a reducir de forma importante la probabilidad de que ocurran. Aun así, siempre habrá un margen de riesgo, ya que la prevención total no es posible., un.

En respuesta a esto la IA opera en tiempo real, por lo que no tiene la limitación de actualización constante o revisiones periódicas manuales, sino que, con una programación previa y de acuerdo a las necesidades tiene el potencial de realizar ciclos de análisis automáticos cada ciertos intervalos de tiempo, y con esta medida, es posible identificar entre cada uno de estos ciclos de análisis, alguna anomalía en grandes volúmenes de datos para identificar alguna novedad o dato atípico y neutralizarlo para prevenir que se genere o ejecute una posible amenaza.

La IA tiene un potencial fuerte de operación para garantizar la seguridad en Data Center, sin embargo, por sí sola no está en capacidad de proteger datos ya que permite la detección proactiva de amenazas mediante el análisis predictivo y el aprendizaje automático, optimizando la respuesta ante incidentes y reduciendo los tiempos de recuperación en caso de ataques, pero debe estar adaptada con otros mecanismos como un Software, un auditor y un Hardware especializado a la seguridad. Entonces es solo un complemento a los protocolos de seguridad

tradicionales, como el cifrado de datos, los firewalls, los sistemas de detección y prevención de intrusiones, y la autenticación multifactor; esta se debe adaptar a los principales ataques que afectan a los Data Centers, como la denegación de servicio (DDoS), el phishing, el Ransomware y la inyección de SQL, cada uno con su propio impacto y mecanismos de mitigación.

En ese sentido, la protección física adecuada en los Data Centers es importante porque no solo las amenazas digitales son un riesgo, sino también factores externos como desastres naturales, accesos no autorizados y fallos eléctricos que pueden comprometer la seguridad, y metodologías como el esquema de ocho capas de seguridad física para mitigar estos riesgos, incluyendo controles de acceso biométricos, monitoreo por CCTV y redundancia energética.

Recomendaciones

Para futuras investigaciones de la misma línea, se recomienda explorar áreas que complementen y amplíen los hallazgos de este estudio, como la aplicación de Blockchain en ciberseguridad, y modernidad en los sistemas seguridad, pues aunque se ha identificado que la IA es una herramienta de alto valor e impacto para la detección y respuesta a amenazas, aún existen desafíos en la precisión de los resultados, análisis predictivos y en la capacidad de adaptación a nuevas formas de ataques, por ello investigar sobre formas de mejorar esta situación es una forma de conseguir mejores resultados.

Otra línea de investigación relevante es la seguridad en infraestructuras híbridas y en la nube, pues con el crecimiento del almacenamiento descentralizado, los Data Centers han evolucionado hacia modelos combinados con la nube, lo que plantea nuevos riesgos en términos de accesibilidad y control de datos.

Referencias Bibliográficas

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond, K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security, 119(22), 1027-1045*, https://doi.org/10.1016/j.cose.2022.102754.

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. *IEEE Access, 9(2), 57792-57807*, DOI: 10.1109/ACCESS.2021.3073203.

Anžel, A., Heider, D., & Hattab, G. (2021). The story of data storage: From storage properties to user interfaces. *Computational and Structural Biotechnology Journal, 19(18), 4904-4918*, https://doi.org/10.1016/j.csbj.2021.08.031.

AWS Amazon. (2020). Capital One completa la migración desde los centros de datos hacia AWS y se convierte en el primer banco de Estados Unidos en anunciar la adopción de la nube de forma integral. *AWS en Español*, en línea: https://aws.amazon.com/es/solutions/case-studies/capital-one-all-in-on-aws/ [consultado el 3 de mayo de 2025].

Biswas, R., Kim, S., & Wu, J. (2021). Sampling rate distribution for flow monitoring and DDoS detection in datacenter. *IEEE Transactions on Information Forensics and Security, 16(17), 2524 - 2534*, DOI: 10.1109/TIFS.2021.3054522.

Bonnie, E., & Fitzgerald, A. (2025). 110+ of the Latest Data Breach Statistics. *Securframe, sitio oficial*, en línea: https://secureframe.com/blog/data-breach-statistics [consultado el 23 de julio de 2025].

Canchig, V., & Patricio, E. (2022). Comparación de Métodos de Seguridad entre Cloud Computing y DataCenter Convencionales utilizando normas ISO 27001 Y 27017. *Repositorio*

Universidad de Israel [tesis de pregrado], URI: http://repositorio.uisrael.edu.ec/handle/47000/3369.

Cárdenas, C., & Olarte, F. (2022). Análisis de seguridad entre microservicios con Amazon Web Service. *Revista Logos Ciencia & Tecnología, 14(2), 202-213*, https://doi.org/10.22335/rlct.v14i2.1546 .

Cardenas, J. (2023). Modelo de gestión de la seguridad de la arquitectura PAAS de datacenter. *Repositorio Institucional UPC [tesis de pregrado]*, URI: http://hdl.handle.net/10757/667380.

Casasempere, A. (2020). Análisis documental bibliográfico. Obteniendo el máximo rendimiento a la revisión de la literatura en investigaciones cualitativas. *New Trends in Qualitative Research, 4, 247–257*, URI: https://publi.ludomedia.org/index.php/ntqr/article/view/44.

Colombia, C. d. (2009). *funcionpublica.gov.co*. Retrieved from funcionpublica: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Colombia, C. d. (2012). *funcionpublica.gov.co*. Retrieved from funcionpublica: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Cordova, R. (2024). Inteligencia artificial generativa en el ámbito de la ciberseguridad: una revisión sistemática de literatura. *Repositorio UCC [tesis de Maestría]*, URI: https://dspace.ucacue.edu.ec/items/d8a02685-cb57-438f-96eb-09078532732d.

Engström, V., Johnson, P., Lagerström, R., Ringdahl, E., & Wällstedt, M. (2023). Automated security assessments of Amazon Web services environments. *ACM Transactions on Privacy and Security, 26(2), 771-789*, https://doi.org/10.1145/3570903.

Espinoza, M., & Quevedo, A. (2025). Impacto de la Inteligencia Artificial en los Procesos de Ciberseguridad en la seguridad industrial. Revisión narrativa. *MQRInvestigar, 9(1), 68-77*, https://doi.org/10.56048/MQR20225.9.1.2025.e68.

Fox, J. (2024). Top Cybersecurity Statistics for 2024. *Cobalt, sitio web oficial*, en línea: https://www.cobalt.io/blog/cybersecurity-statistics-2024 [consultado el 23 de julio de 2025].

Gautam, R., Jain, M., Moazzam, J., & Kant, S. (2020). Cloud Computing Security: Aws Data Security Credentials. *Studies in Indian Place Names, 40(3), 6385-6390*, URI: https://d1wqtxts1xzle7.cloudfront.net/104104871/CLOUD_COMPUTING_SECURITY_AWS_DATA_SECURITY_CREDENTIALS-libre.pdf?1688791833=&response-content-disposition=inline%3B+filename%3DCloud_Computing_Security_Aws_Data_Securi.pdf&Expires=1746409114&Signature=Y.

Goerlich, J. (2019). Innovación, digitalización y relaciones colectivas de trabajo. *Treball Journal, Economía y Societat, 12(92), 122-148*, URI: https://www.ces.gva.es/sites/default/files/2019-09/art10_0.pdf.

Goldman, L., & Dessouky, G. (2022). About the Data Center Security: Server Advanced infrastructure. *Broadcom Official Site*, en línea: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/data-center-security [consultado el 24 de marszo de 2025].

Green Mountain. (2025). Data Center Security. *Online*, URI: https://greenmountain.no/.

Haider, S. (2024). Five Most Famous DDoS Attacks and Then Some. *A10 International Cibersecurity [official site]*, en línea: https://www.a10networks.com/blog/5-most-famous-ddos-attacks [consultado el 24 de marzo de 2025].

Helali, L., & Nazih, M. (2021). A survey of data center consolidation in cloud computing systems. *Computer Science Review, 39(12), 87-94*, https://doi.org/10.1016/j.cosrev.2021.100366.

Hernández, R., & Mendoza, C. (2019). Metodología de la investigación las rutas cuantitativa cualitativa y mixta. *Editorial Mc Graw Hill Education, Ciudad de México*, https://doi.org/10.22201/fesc.20072236e.2019.10.18.6.

IBM. (2024). What is an intrusion detection system (IDS)? *IBM Oficial*, en línea: https://www.ibm.com/think/topics/intrusion-detection-system [consultado el 10 de marzo de 2025].

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97(23), 1018-1024*, https://doi.org/10.1016/j.inffus.2023.101804.

Kim, J., Choi, H., Lee, S., & Lee, H. (2025). Computational study of single-phase immersion cooling for high-energy density server rack for data centers. *Applied Thermal Engineering, 264(1), 1952-1967*, https://doi.org/10.1016/j.applthermaleng.2025.125476.

Li, N., Li, Y., Gong, X., & Tao, W. (2024). Innovative server simulator for data centers and critical indices of performance evaluation. *Energy and Buildings, 324(19), 1137-1149*, https://doi.org/10.1016/j.enbuild.2024.114937.

Li, Y., & Liu, A. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7(11), 8176-8186*, https://doi.org/10.1016/j.egyr.2021.08.126.

Liu, X., Hou, L., & Yang, L. (2024). Optimizing data center energy consumption via energy complementarity scheduling. *Energy Reports, 12(6), 5990-5997*, https://doi.org/10.1016/j.egyr.2024.11.032.

Long, S., Li, Y., Huang, J., Li, Z., & Li, F. (2022). A review of energy efficiency evaluation technologies in cloud data centers. *Energy and Buildings, 260(61), 1118-1132*, https://doi.org/10.1016/j.enbuild.2022.111848.

Lundvall, B., & Rikap, C. (2022). China's catching-up in artificial intelligence seen as a co-evolution of corporate and national innovation systems. *Research Policy, 51(1), 1043-1059*, https://doi.org/10.1016/j.respol.2021.104395.

Mahdavi, S., & Rahmani, R. (2023). Interactive anomaly-based DDoS attack detection method in cloud computing environments using a third party auditor. *Journal of Parallel and Distributed Computing, 178(13), 82-99*, https://doi.org/10.1016/j.jpdc.2023.04.003.

Marwan, M., Temghart, A., Ouhmi, S., & Lazaar, M. (2024). Security, QoS and energy aware optimization of cloud-edge data centers using game theory and homomorphic encryption: Modeling and formal verification. *Results in Engineering, 24(6), 1029-1038*, https://doi.org/10.1016/j.rineng.2024.102902.

McIntosh, T., Susnjak, T., Liu, T., Xu, D., Watters, P., Liu, D., . . . Halgamuge, M. (2024). Ransomware reloaded: Re-examining its trend, research and mitigation in the era of data exfiltration. *ACM Computing Surveys, 57(1), 57-69*, https://doi.org/10.1145/36913.

MinTIC, M. d. (2022). *mintic.gov.co*. Retrieved from Ministerio de Tecnologias de la Información y las Comunicaciones: https://normograma.mintic.gov.co/mintic/compilacion/docs/resolucion_mintic_0746_2022.htm

Nanda, M., Saraswat, M., & Kumar, P. (2024). Enhancing cybersecurity: A review and comparative analysis of convolutional neural network approaches for detecting URL-based

phishing attacks. *e-Prime - Advances in Electrical Engineering, Electronics and Energy, 8(12), 251-267*, https://doi.org/10.1016/j.prime.2024.100533.

Naseer, I. (2023). AWS Cloud Computing Solutions: Optimizing Implementation for Businesses. *Statistics, computing and interdisciplinary research, 5(2), 338-350*, https://doi.org/10.52700/scir.v5i2.138.

Özkan, B., Erdem, M., & Özceylan, E. (2022). Evaluation of Asian Countries using Data Center Security Index: A Spherical Fuzzy AHP-based EDAS Approach. *Computers & Security, 122(61), 5231-5237*, https://doi.org/10.1016/j.cose.2022.102900.

Paredes, E. (2024). Seguridad en redes de datos con la ayuda del IDS Snort en Kali Linux en el Datacenter del Cuerpo de Bomberos de Babahoyo. *Repositorio Institucional de la UTB [tesis de pregrado]*, URI: https://dspace.utb.edu.ec/handle/49000/17060.

Patel, S. (2021). Challenges and technological advances in high-density data center infrastructure and environmental matching for cloud computing. *International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal, 12(1), 662-671*, DOI: 10.48175/568.

Pesantez, D., Chalan, R., Figueras, G., & Avila, M. (2022). Cybersecurity Policies for Network Switching Devices in Hospital Data Centers: A Case Study. *ESPOCH Congresses: The Ecuadorian Journal of S.T.E.A.M, 2(2), 507-518*, DOI 10.18502/espoch.v2i2.11413.

Polo, A. (2020). Sociedad de la información, sociedad digital, sociedad de control. *Inguruak. Revista Vasca De Sociología Y Ciencia Política, 68(3), 234-251*, https://doi.org/10.18543/inguruak-68-2020-art05.

Prakash, S., Mishra, R., & Kumari, U. (2025). Neural secret key enabled secure cloud storage with efficient packet checker algorithm. *Cyber Security and Applications, 3(2), 257-269*, https://doi.org/10.1016/j.csa.2024.100071.

Praveen, B. (2024). The 8 layers of security your data center must have. *Space DC, Ciberseguridad*, en línea: https://spacedc.com/the-8-layers-of-security-your-data-center-must-have/ [consultado el 25 de marzo de 2025].

Prieto, L. (2025). Despliegue de Cisco ACI. *Administració de xarxes i sistemes operatius [trabajo de grado]*, URI: https://openaccess.uoc.edu/handle/10609/151945.

Radware. (2024). Pishing Cyberattack. *Radware online*, en línea: https://www.radware.com/cyberpedia/bot-attacks/phishing-attack/ [consultado el 24 de marzo de 2025].

Sadeghi, R. (2024). What is DDoS Attack? *Pointech Official Site*, en línea: https://www.tpointtech.com/what-is-ddos-attack [consultado el 24 de marzo de 2025].

Sowka, K., Palade, V., Jiang, X., & Jadidbonab, H. (2025). Towards the generation of hierarchical attack models from cybersecurity vulnerabilities using language models. *Applied Soft Computing, 171(64), 1127-1140*, https://doi.org/10.1016/j.asoc.2025.112745.

Swatisipra, D., Minati, R., Kumar, R., & Jyoti, M. (2024). A secure, privacy-preserving, and cost-efficient decentralized cloud storage framework using blockchain. *Journal of King Saud University - Computer and Information Sciences, 36(10), 1267-1284*, https://doi.org/10.1016/j.jksuci.2024.102260.

Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in Biology and Medicine, 129(39), 1041-1059*, https://doi.org/10.1016/j.compbiomed.2020.104130.

Townend, P., Clement, S., Burdett, D., Yang, R., Shaw, J., & Slater, B. (2019). Improving data center efficiency through holistic scheduling in kubernetes. *IEEE International Conference on Service-Oriented System Engineering (SOSE), 525-530*, DOI: 10.1109/SOSE.2019.00030.

Vasilachis, I. (2020). Estrategias de investigación cualitativa. *Gedisa, 2(1), 81-87*, URI: https://www.gedisa.com/gacetillas/240022.pdf.

Velazco, L. (2025). Evolución digital o revolución cultural. *Editorial Universidad Peruana de Ciencias Aplicadas, 2(1), 4-15*, URI: https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/623756/AltamiraEvoluci%C3%B3nDigital.pdf.

Vijayakumar, R., & Duraimutharasan, N. (2024). Data Center Security Analysis Based on The Principle of Defense-In-Depth with Fuzzy Clustering. *Journal of Electrical Systems, 20(10), 212-239*, URI: https://www.journal.esrgroups.org/jes/article/view/5914.

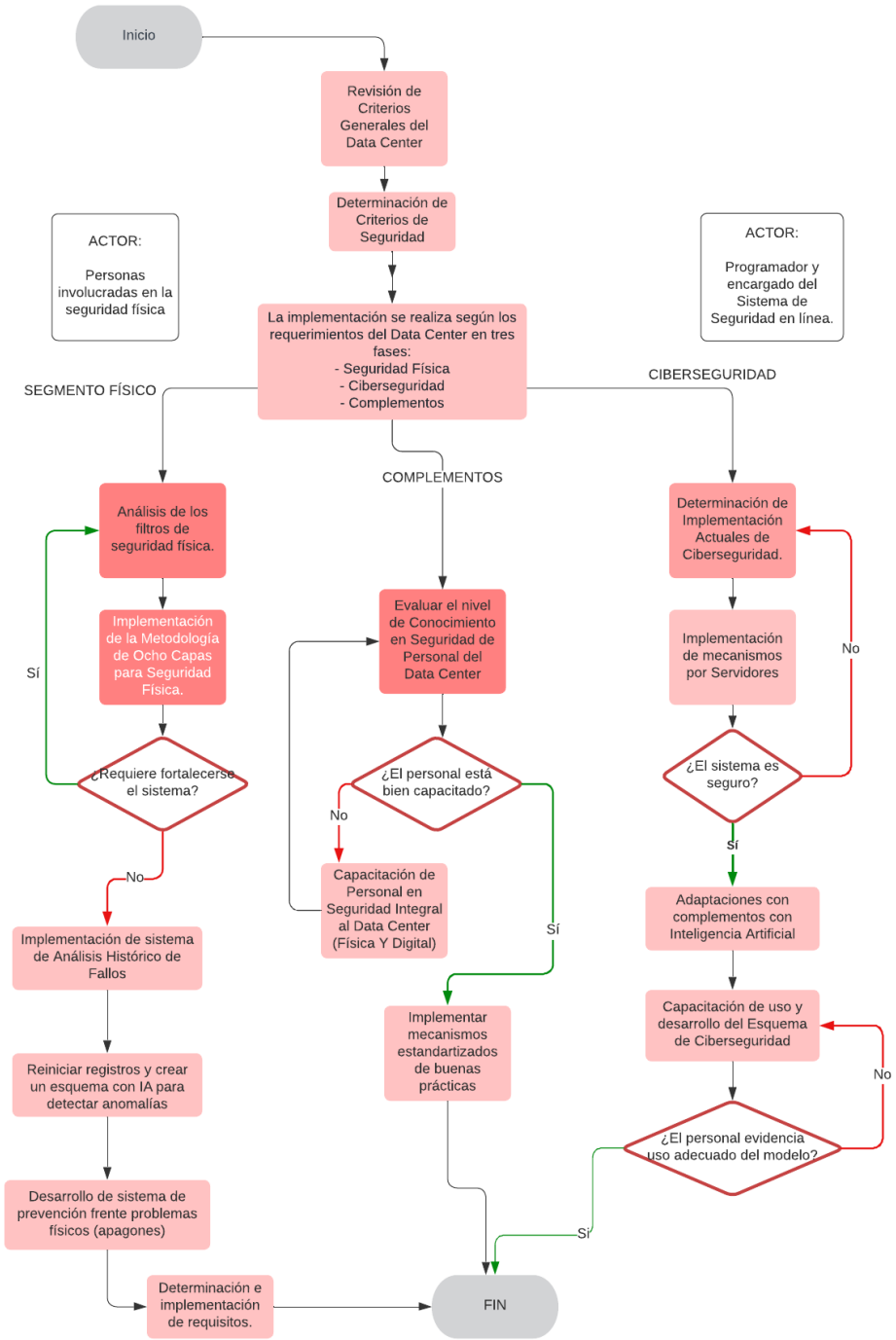
Vinoth, S., Vemula, H., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. *Materials Today Proceedings, 51(8), 2172-2175*, https://doi.org/10.1016/j.matpr.2021.11.121.

Zimba, A., & Chishimba, M. (2019). On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems. *European Journal for Security Research, 4(3), 3-31*, https://doi.org/10.1007/s41125-019-00039-8.

Apéndices

Apéndice A

Flujograma Propuesto para Seguridad en Data Center



Apéndice B

Manual de Instrucciones y Buenas Prácticas para fortalecer Seguridad en un Data Center

Objetivo

Este instructivo tiene como finalidad establecer buenas prácticas y medidas para proteger la infraestructura física y lógica de un Data Center, reduciendo riesgos de intrusiones, fallas, pérdidas de datos o interrupciones en el servicio.

Seguridad Física. Controlar el acceso físico e implementar. Implementar sistemas de autenticación multifactor (tarjeta + biometría), preferiblemente guiado por el sistema de las ocho capas de la seguridad física, determinando que el visitante al Data Center no tenga objetos externos en su cuerpo que puedan alterar o quebrantar la seguridad, Registrar todas las entradas y salidas mediante logs de acceso, Utilizar cámaras de vigilancia 24/7 en puntos estratégicos (entradas, racks, zonas comunes), Asegurar el recinto con puertas blindadas, cerraduras electrónicas y sensores de apertura, Monitoreo constante de temperatura, humedad y partículas, Sistemas contra incendios con detección temprana (VESDA) y extinción con gas limpio, Seguridad Lógica y de Red, Separar redes de gestión, usuarios y servicios críticos mediante VLANs o firewalls internos, Desplegar zonas desmilitarizadas (DMZ) para servicios expuestos al público, Implementar firewalls perimetrales, IPS/IDS, con sistemas de detección y prevención de intrusiones, Monitoreo continuo con SIEM, Utilizar VPN seguras con autenticación multifactor para acceso remoto y revisar y auditar cuentas privilegiadas de forma periódica.

Respaldo y Recuperación. Desarrollar una política de recuperación de datos (Backup) dada por:

Realizar copias de seguridad automáticas y programadas cada cierto tiempo corto, como cada 30 minutos, Mantener al menos una copia fuera del sitio (off-site o en la nube), Verificar

integridad de respaldos de forma periódica, Documentar y probar escenarios de recuperación por fallas, ataques o desastres naturales y contar con procedimientos de continuidad operativa.

Capacitación del Personal. Formación continua en conciencia de seguridad, protocolos internos y respuesta a incidentes, Restringir acceso según el principio de mínimo privilegio, Establecer un manual de seguridad IT con protocolos ante incidentes, cambios, accesos y mantenimiento. Revisión y actualización periódica del plan de seguridad, Auditorías físicas y lógicas programadas y evaluación de vulnerabilidades

Estrategias Adicionales. Aplicar actualizaciones críticas de software y firmware en todos los dispositivos, Mantener inventario actualizado de activos de hardware y software, Definir roles y responsables ante incidentes, Registrar eventos de seguridad y activar el plan de respuesta según el tipo de incidente.