Diseño de un modelo de gestión de ciberresiliencia para hacer frente a un ataque al Directorio Activo en una entidad financiera peruana con patrimonio neto superior a los 12 mil millones de soles

Trabajo de Investigación para obtener el grado de Maestro en Gestión de la Ciberseguridad y Privacidad por:

Jose Danny Chininin Mogollon

Gleny Margot Fernandez Requejo

Dick Williams León Jara

Programa de la Maestría en Gestión de la Ciberseguridad y Privacidad

Lima, 30 de Junio de 2025

Tesis de Maestría en Ciberseguridad

INFORME DE ORIGINALIDAD

0%	0%	2%	0%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

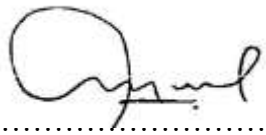
FUENTES PRIMARIAS

Excluir citas	Activo	Excluir coincidencias	< 2%
Excluir bibliografía	Activo		

Este trabajo de investigación

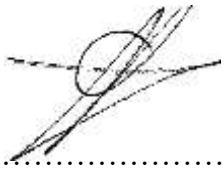
Diseño de un modelo de gestión de ciberresiliencia para hacer frente a un ataque al Directorio Activo en una entidad financiera peruana con patrimonio neto superior a los 12 mil millones de soles.

Ha sido aprobado.



……

Gianncarlo Gómez Morales (Asesor)



……

Genís Margarit Contel (Asesor)

……

Javier Benvenuto Servat (Jurado)

……

Iñigo Echavarri Beloqui (Jurado)

Universidad ESAN

2025

Dedico esta tesis a mi familia y mis raíces, que forjaron mi carácter.

A cada obstáculo que transformé en impulso para salir adelante.

Gleny Fernández Requejo

A mi familia, por su apoyo incondicional.

A mis hijos, por darme razones para seguir y sonrisas que me sostuvieron en los días más duros.

Este logro también es de ustedes.

Dick León Jara

A mis padres: Modesto y María, por su amor incondicional, esfuerzo y guía en cada paso. A mis hijos, por ser mi inspiración constante y la luz de mis días.
Esta meta es también suya, con todo mi amor y gratitud.

José Danny Chininín Mogollón

GLENY FERNÁNDEZ REQUEJO

Profesional con más de 10 años de experiencia en gestión de riesgos, seguridad de la información, ciberseguridad y protección de datos personales, con una sólida trayectoria en sectores altamente regulados como el financiero, seguros y retail.

Actualmente desempeñando el rol de Principal Manager de Gobierno en Ciberseguridad en BBVA Perú, liderando auditorías internas y externas, garantizando el cumplimiento normativo y la implementación de estrategias de seguridad alineadas con marcos locales e internacionales. Amplia experiencia en la gestión de riesgos tecnológicos y operacionales, diseño e implementación de políticas de seguridad, programas de concienciación en ciberseguridad, y análisis de indicadores estratégicos de riesgo.

Experiencia previa en firmas líderes de consultoría como Ernst & Young y Deloitte, donde gestionó revisiones de controles generales de TI (ITGC) y proyectos de transformación del riesgo. Participación en la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI) y cumplimiento con la Ley de Protección de Datos Personales (Ley 29733) en el Perú.

FORMACIÓN Y CERTIFICACIONES:

- Ingeniera de Sistemas por la Universidad Nacional Pedro Ruiz Gallo
- Diplomado en Seguridad y Auditoría TI
- Especialización en Gestión de la Ciberseguridad
- Certificaciones internacionales:
    - ISO/IEC 27032 Lead Cybersecurity Manager (PECB)
    - Lead Cybersecurity Professional Certificate (LCSPC)
    - Cyber Security Foundation Professional Certificate (CSFPC)
    - Scrum Master Professional Certificate (SMPC)

DICK LEÓN JARA

Ingeniero Industrial con sólida formación técnica y más de 20 años de experiencia en telecomunicaciones, redes y ciberseguridad, enfocado en la eficiencia operativa, la mejora continua y la continuidad de servicios críticos. Profesional orientado a resultados, con capacidad para liderar proyectos estratégicos de optimización de procesos e infraestructura tecnológica en entornos de alta exigencia.

Desde 2013, forma parte de Entel Perú, donde actualmente se desempeña como Especialista Senior de Ciberseguridad, habiendo ocupado previamente cargos de responsabilidad en redes CORE-IP. Experiencia internacional consolidada en Nokia Siemens Networks (Portugal, Brasil y Perú), con liderazgo en operaciones de red y soporte de infraestructura crítica. Trayectoria previa en Nextel, Telefónica del Perú y Wi-Net, con desempeño destacado en análisis de redes, soporte técnico y gestión operativa.

Complementa su formación con una Maestría en Gestión de la Ciberseguridad y Privacidad (en curso) y diversos diplomados en gerencia de proyectos y gestión empresarial, lo que le otorga una visión integral para integrar la tecnología con la estrategia organizacional.

FORMACIÓN Y CERTIFICACIONES:

- Ingeniero Industrial por la Universidad Nacional de Trujillo.
- Diplomados en Gerencia de ProyectosCertificaciones internacionales:
    - Certified Ethical Hacker (CEH)
    - Cisco Certified Network Professional (CCNP)
    - Cisco Certified Network Associate (CCNA)
    - Optimizing Converged Cisco Networks
    - Microsoft Certified Systems Engineer
    - Sun Certified System Administrator for Solaris 9

CHININ MOGOLLON JOSE DANNY

Profesional en Ingeniería Informática con más de 22 años de experiencia en desarrollo de aplicaciones web, especializado como Full Stack Developer, con dominio tanto del Front End como del Back End, y fuerte orientación hacia la ciberseguridad, redes informáticas y soporte a infraestructura tecnológica.

Cuenta con amplia experiencia en configuración de redes LAN/WAN/MAN y soporte a servidores web, respaldado por múltiples certificaciones en hacking ético, gestión de proyectos, cloud computing, blockchain e inteligencia artificial.

A lo largo de su trayectoria ha colaborado con empresas nacionales e internacionales en Perú y Suecia, diseñando, desarrollando y administrando sitios web y sistemas de gestión empresarial. Además, posee habilidades en diseño gráfico, auditoría de sistemas, asesoría informática y administración de proyectos tecnológicos.

FORMACIÓN Y CERTIFICACIONES:

- Ingeniería Informática por la Universidad Nacional de Piura.
- Formación complementaria en administración, ética, filosofía, sociología y psicología aplicada.
- Certificaciones internacionales:
    - Cybersecurity Awareness Professional Certification (CAPC)
    - Scrum Foundation Professional Certification
    - Ethical Hacking, CyberSOC, Pentesting Web
    - Cloud Computing (AWS, Azure, Google Cloud)
    - ISO/IEC 27001: Gestión de Seguridad de la Información
    - Fundamentos de Blockchain y Gestión de Proyectos (PMI)

Contenido

Lista de tablas

Lista de figuras

RESUMEN EJECUTIVO

En el contexto actual de amenazas cibernéticas cada vez más sofisticadas, el Directorio Activo (AD) se ha convertido en un blanco prioritario para los atacantes, dada su función crítica en la administración de identidades, accesos y políticas dentro de las organizaciones. Esta investigación parte de la necesidad urgente de fortalecer la capacidad de respuesta y recuperación de las entidades financieras peruanas frente a un posible ataque al AD, desarrollando un modelo de ciberresiliencia adaptado al entorno nacional, pero basado en estándares internacionales como NIST CSF, ISO/IEC 27001 y la Ley DORA.

Se aplicó un enfoque metodológico mixto, combinando análisis documental, entrevistas con expertos, y un cuestionario de diagnóstico técnico aplicado a una entidad representativa del sector financiero. Los resultados revelaron brechas significativas en la protección del AD, especialmente en áreas como gestión de privilegios, monitoreo, y recuperación ante incidentes.

A partir de estos hallazgos, se diseñó un modelo práctico, modular y escalable, que incluye autenticación multifactor, monitoreo en tiempo real con inteligencia artificial, gestión de accesos privilegiados con Microsoft Entra ID, planes de recuperación validados y una arquitectura basada en los principios de Zero Trust.

El modelo fue complementado con un plan de implementación en cinco fases, un simulacro de presupuesto y una serie de indicadores para medir su efectividad a lo largo del tiempo. Como conclusión, se afirma que la resiliencia digital no es un estado, sino una capacidad que debe ser cultivada activamente. Este trabajo ofrece una hoja de ruta concreta para lograrlo en organizaciones que gestionan información crítica a través del Directorio Activo.

1. Introducción

1.1. Planteamiento del problema

El auge de la digitalización de las compañías, impulsado por la conectividad global y el uso de plataformas de terceros en la nube, provoca un aumento constante en la complejidad y el alcance tecnológico que requiere protección.

En ese contexto, como lo señala la Agencia de la Unión Europea para la Ciberseguridad (ENISA), en su Informe de Panorama de Amenazas de Ciberseguridad del año 2023 (ENISA Threat Landscape 2023), el panorama de la ciberseguridad muestra un aumento significativo tanto en la variedad como en la frecuencia de los ataques, así como en sus consecuencias. El informe identifica y analiza las principales amenazas actuales, tales como, ransomware, malware, ingeniería social, brecha de datos, denegación de servicio (ddos), manipulación de la información y ataques a la cadena de suministros (supply chain) (European Union Agency for Cybersecurity, 2023).

Frente a este escenario, el 14 de diciembre del año 2022 el Parlamento Europeo y el Consejo de la Unión Europea publicaron la Ley de Resiliencia Operativa Digital (DORA). Esta Ley, establece los requisitos y obligaciones para la gestión del riesgo de las tecnologías de información y comunicaciones (TIC), la notificación de incidentes, la realización de pruebas de resiliencia operativa, el establecimiento de acuerdos de intercambio sobre ciberamenazas y la supervisión del riesgo en la cadena de suministro de las entidades financieras (Diario Oficial de la Unión Europea, 2022).

No obstante, a pesar de los esfuerzos del regulador europeo por mantener al sector financiero a la vanguardia tecnológica y en ciberseguridad, los principales bancos enfrentan grandes desafíos en la implementación de DORA. Esta situación se torna aún más compleja en los países latinoamericanos de economías emergentes, donde, en la mayoría de los casos, carecen normativas definidas que establezcan requisitos para que las organizaciones desarrollen y fortalezcan sus capacidades para resistir, adaptarse y recuperarse rápidamente ante un incidente de ciberseguridad.

En el Perú, la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS) mediante la Resolución S.B.S. Nº 504-2021, aprobó el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, este reglamento exige a las entidades financieras asegurar un entorno seguro y confiable para ofrecer productos y servicios a sus clientes. Asimismo, el 04 de marzo del 2025, la SBS publicó la Resolución SBS N° 00814-2025, la cual establece la implementación de planes y estrategias para prevenir o reducir el impacto de eventos que interrumpan la prestación de servicios a través de canales digitales. Sin embargo, a pesar de que la principal preocupación de las entidades financieras se centra en la seguridad de los canales digitales para garantizar la continuidad del servicio, a menudo descuidan un componente fundamental y básico de su infraestructura como la protección del Directorio Activo (Superintendencia de Banca, Seguros y AFP, 2024).

Particularmente, el sector financiero peruano está compuesto por 18 bancos (Banco Central de Reserva del Perú, 2025), de los cuales 4 son los más representativos y cuentan con un patrimonio superior a los 12 mil millones de soles. Sin embargo, de estos 4 bancos, solo 1 ha comenzado a trabajar en la implementación de un modelo de ciberresiliencia. Ésta situación, subraya la urgente necesidad de adoptar enfoques más sólidos para enfrentar la creciente amenaza cibernética, especialmente cuando se trata de activos críticos como el Directorio Activo (Active Directory, AD), que es esencial para estructurar los sistemas dentro de una red y controlar los permisos y accesos a dichos sistemas.

El Active Directory es el sistema operativo de red (Network Operating System, NOS) de Microsoft y se ha convertido en el estándar predominante para la administración de redes (Microsoft, 2024). Su uso es tan extendido que cerca del 90% de las empresas de la lista Fortune 1000 lo emplean como su principal herramienta para gestionar la autenticación y autorización de manera eficiente y sin complicaciones.

Antes de la llegada del Active Directory, Microsoft utilizaba un modelo descentralizado basado en Windows NT (Novel Networks), que constaba de

un sistema de dominios basado en listas de control de acceso y bases de datos SAM (Security Account Manager), sin embargo, dicho modelo presentaba limitaciones, tales como:

- Cada dominio tenía su propia base de datos de usuarios.
- La replicación de datos entre dominios era complicada.
- No existía un sistema jerárquico eficiente para organizar los recursos.

El Active Directory fue publicado por primera vez como "Windows 2000 Server" el 17 de febrero del 2000, introduciendo un modelo jerárquico y escalable basado en LDAP (Lightweight Directory Access Protocol), la integración con DNS (Domain Name System) y la administración centralizada mediante GPOs (Group Policy Objects). Dichas innovaciones facilitaron la administración de grandes infraestructuras de TI, mejorando la seguridad y la eficiencia en la gestión de usuarios y recursos (Microsoft, 2024).

Desde su lanzamiento inicial, el Active Directory ha evolucionado continuamente durante 25 años, mejorando con cada nueva versión para establecer un estándar más alto y ofrecer mayor valor a las organizaciones.

- **Windows Server 2003:** Incorporó la confianza entre bosques, particiones de aplicaciones, objetos dinámicos y vinculaciones LDAP concurrentes. También incluyó funciones como el registro del último inicio de sesión, la herramienta de línea de comandos y la capacidad de renombrar dominios y controladores de dominio. Redujo la frecuencia de replicación intrasitio de 5 minutos a 15 segundos. Además, implementó soporte para TLS (Transport Layer Security) y mejoró la seguridad con el cifrado del tráfico LDAP (Microsoft, 2024).
- **Windows Server 2008:** Introdujo mejoras significativas en Active Directory, centrándose en seguridad, administración y rendimiento. Implementó la separación de roles administrativos, nuevas funcionalidades para el servidor DNS (Domain Name System) y permitió a las organizaciones personalizar sus propias políticas de contraseñas. También optimizó la auditoría y el registro de accesos y amplió la longitud

máxima de la clave de cifrado AES (Advanced Encryption Standard) de 128 bits a 256 bits (Microsoft, 2024).

- **Windows Server 2008 R2:** La incorporación más destacada fue la Papelera de reciclaje de Active Directory que permite recuperar objetos eliminados sin perder atributos. En cuanto a funcionalidad, mejoró el balanceo de carga en servidores (Microsoft, 2024).

- **Windows Server 2012:** Introdujo mejoras significativas en Active Directory, destacando la virtualización segura de controladores de dominio, la activación basada en Active Directory y la clonación de controladores de dominio en entornos virtualizados.

  Se implementó el Control de Acceso Dinámico (DAC) para mejorar la seguridad basada en atributos de usuario y dispositivo, y las Cuentas de Servicio Administradas de Grupo (gMSAs) para optimizar la gestión de credenciales en múltiples servidores. Además, la Consola de Administración de Directivas de Grupo (GPMC) incorporó informes sobre el estado de las directivas.

  Se mejoró la administración de Active Directory con una interfaz más fácil de usar en el Centro de Administración de Active Directory (ADAC), permitiendo una gestión más sencilla de usuarios y configuraciones. También facilitó la conexión de computadoras a la red de la empresa sin necesidad de estar físicamente en la oficina, gracias a la unión de dominio sin conexión con DirectAccess.

  El proceso de instalación y actualización de servidores se hizo más intuitivo con un nuevo asistente en el Administrador del Servidor. Finalmente, se mejoró la seguridad en servidores virtualizados, detectando posibles problemas y evitando errores en la sincronización de datos (Microsoft, 2024).

- **Windows Server 2016:** Introduce una serie de mejoras y nuevas funcionalidades de seguridad diseñadas para proteger los sistemas, los datos y las credenciales de usuario. Estas mejoras están centradas en

reducir la superficie de ataque, minimizar los privilegios de los administradores y reforzar la protección contra amenazas avanzadas.

Windows Server 2016 fue diseñado con un enfoque *cloud-ready*, incorporando tecnologías inspiradas en Microsoft Azure para facilitar la implementación de entornos híbridos y en la nube. Su arquitectura permite a las empresas modernizar su infraestructura local y extenderla sin problemas a servicios en la nube (Microsoft, 2024).

- **Windows Server 2019:** Fue diseñado con un fuerte enfoque en la nube híbrida, permitiendo a las organizaciones aprovechar los beneficios de Microsoft Azure sin necesidad de migrar completamente a la nube. Su integración con servicios en la nube facilita la modernización de infraestructuras, la administración remota y la mejora en la seguridad. Además, refuerza la seguridad a través de múltiples capas de protección, desde la infraestructura hasta la administración de identidades.

  Por otro lado, con el objetivo de simplificar la administración, reducir costos y optimizar el rendimiento, Windows Server 2019 presenta un nuevo enfoque de gestión mediante Infraestructura Hiperconvergente (HCI), la cual, es un modelo de arquitectura de centros de datos que integra cómputo, almacenamiento y redes en una única plataforma definida por software. Esto elimina la necesidad de sistemas tradicionales separados, como servidores, almacenamiento y hardware de red dedicado (Microsoft, 2024).

- **Windows Server 2022:** Desde Windows Server 2016, Microsoft ha mantenido su enfoque por los servicios y el alojamiento en la nube. Consciente del crecimiento y las ventajas de las Infraestructuras Hiperconvergentes, Windows Server 2022 permite gestionar cargas de trabajo en cualquier entorno (centro de datos de la organización y en la nube) mientras ofrece protección avanzada contra amenazas emergentes y resguarda los datos. Además, ofrece:

  - Seguridad multicapa: Seguridad integral desde el hardware hasta la nube, abarcando firmware y sistema operativo, para prevenir

proactivamente posibles ataques. Además, garantiza una conectividad segura con protocolo de transferencia de hipertexto cifrado (HTTPS) y cifrado AES-256.

- Integración híbrida con Azure: Facilita la administración, seguridad y migración de Windows Server en entornos locales, perimetrales o multinube desde Azure, optimizando el uso de ancho de banda con compresión de archivos. Además, permite inventariar y trasladar datos desde sistemas heredados y centralizar archivos en Azure Files, manteniendo rendimiento y compatibilidad. Integra análisis predictivo basado en un modelo de inteligencia artificial y aprendizaje automático.
- Plataforma adaptable para aplicaciones: Permite a desarrolladores y equipos de TI construir aplicaciones de manera ágil, optimizando el desarrollo y ampliando la compatibilidad con cargas de trabajo clave (Microsoft, 2024).

- **Windows Server 2025:** Incorpora mejoras de seguridad para prevenir ciberataques y ofrece capacidades avanzadas para entornos de nube híbrida, brindando una plataforma de alto rendimiento compatible con inteligencia artificial. Además, proporciona una línea base de seguridad conforme al Center for Internet Security (CIS) y solo permite el uso de protocolos y estándares criptográficos aprobados por National Institute of Standards and Technology (NIST) (Microsoft, 2025).
- **Microsoft Entra ID:** Es la solución de gestión de identidades en la nube de Microsoft que permite controlar de forma segura el acceso a usuarios, dispositivos y aplicaciones, aplicando reglas de acceso (como la ubicación del usuario, el tipo de dispositivo o el horario). Integra funciones como autenticación multifactor (MFA), inicio de sesión único (SSO) y detección de riesgos en tiempo real con inteligencia artificial. Bajo el enfoque de Zero Trust, valida cada acceso según su nivel de riesgo, ayudando a reducir amenazas y proteger infraestructuras híbridas que dependen del Directorio Activo (Microsoft, 2025).

1.2. Objetivos

- Objetivo general
  - Diseñar un modelo de gestión de ciberresiliencia para hacer frente a un ataque al Directorio Activo en una entidad financiera peruana con patrimonio neto superior a los 12 mil millones de soles.
- Objetivos específicos
  - Determinar los controles tecnológicos y organizacionales para la protección del Directorio Activo y su capacidad de recuperación ante incidentes.
  - Proponer un conjunto de indicadores clave de desempeño (KPIs) para medir la efectividad del modelo de gestión de ciberresiliencia propuesto.
  - Elaborar un diagrama del dominio de autenticación de usuarios, enfocado en incrementar la seguridad y la resiliencia del sistema de autenticación.

1.3. Justificación

Según el Decreto Supremo N.° 106-2017-PCM, que aprueba el Reglamento para la identificación, evaluación y gestión de riesgos de los Activos Críticos Nacionales (ACN), el mercado financiero, en adelante sector financiero, es considerado un Activo Crítico Nacional, ya que resulta esencial e imprescindible para que los peruanos podamos atender nuestras necesidades vitales y desarrollar nuestra vida cotidiana con normalidad (Gobierno del Perú, 2024).

La dependencia del sector financiero de herramientas tecnológicas de última generación es fundamental para su supervivencia en un entorno cada vez más digitalizado y competitivo. La adopción de innovaciones como la inteligencia artificial, el blockchain y los sistemas de pagos en tiempo real no solo optimiza la eficiencia operativa, sino que también mejora la experiencia del cliente, ofrece soluciones más seguras y permite una mayor personalización

de los servicios. En este contexto, la capacidad de adaptarse a nuevas tecnologías se ha convertido en un factor determinante para la sostenibilidad de las instituciones financieras, ya que les permite mantenerse competitivas, responder rápidamente a cambios del mercado y garantizar la seguridad frente a amenazas cibernéticas.

Los bancos en Perú están supervisados por la Superintendencia de Banca, Seguros y AFP (SBS), entidad adscrita al Ministerio de Economía y Finanzas. Ante el creciente nivel de interconectividad, la adopción de canales digitales para la prestación de servicios y la virtualización de productos en el sistema financiero, de seguros y de pensiones, la SBS ha reconocido la necesidad de que las instituciones financieras fortalezcan sus capacidades protección y recuperación ante posibles ciberataques (Gobierno del Perú, 2024).

Por ello, mediante la Resolución SBS N.º 504-2021, publicó el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad (Superintendencia de Banca, Seguros y AFP, 2021). No obstante, muchas entidades aún tienen la oportunidad de fortalecer su enfoque integral en la gestión de riesgos cibernéticos, debido a los desafíos que implica en términos de inversión presupuestaria y asignación de recursos.

Además, mediante la Resolución SBS N.º 00814-2025, establece la obligación de contar con planes y estrategias que permitan prevenir o mitigar interrupciones en los servicios digitales, asegurando su restablecimiento dentro de los tiempos y condiciones previamente definidos por cada institución (Superintendencia de Banca, Seguros y AFP, 2025).

Las ciberamenazas son cada vez más sofisticadas y las consecuencias de no estar adecuadamente preparado pueden ser devastadoras, tanto para la organización como para el sistema financiero en su conjunto, por tal motivo, urge la necesidad de diseñar un modelo de gestión de ciberresiliencia para hacer frente a un ataque al Directorio Activo.

El Directorio Activo es uno de los componentes más críticos en la infraestructura tecnológica de las entidades financieras, ya que centraliza la gestión de identidades, autenticación y autorización en los sistemas de

información. Sin embargo, debido a su relevancia estratégica, también se ha convertido en un objetivo principal para los atacantes, quienes buscan vulnerar para obtener acceso a datos confidenciales, manipular sistemas críticos y generar impactos operativos significativos.

1.4. Alcance

La presente tesis tiene como propósito diseñar un modelo de gestión de ciberresiliencia para hacer frente a un ataque al Directorio Activo en una entidad financiera peruana con patrimonio neto superior a los 12 mil millones de soles.

El estudio se enmarca en el análisis y diseño de un modelo de gestión aplicable a entidades financieras peruanas con gran patrimonio. Se abordará el ciclo completo de la ciberresiliencia (anticipación, protección, detección, respuesta y recuperación) centrado en ataques al AD. El análisis técnico se desarrollará con base en las versiones de Windows Server desde 2016 a 2022, abarcando configuración segura, monitoreo, backup, detección de anomalías y recuperación.

No se considera el desarrollo de una plataforma tecnológica, pero sí se planteará un modelo que pueda ser adoptado por áreas de seguridad, arquitectura de TI e infraestructura en bancos u otras instituciones financieras con características similares.

1.5. Contribución

El desarrollo del presente trabajo de investigación permitirá el diseño de un modelo de gestión de ciberresiliencia, el cual, además de velar por el cumplimiento regulatorio y alineamiento con estándares internacionales. Esta tesis ofrece una solución innovadora, estructurada y contextualizada al problema de los ataques al Directorio Activo, específicamente en el ámbito financiero peruano. Las principales contribuciones incluyen:

- Crear un marco de trabajo que sirva como base para una gestión proactiva de los riesgos, optimizando la capacidad de recuperación ante posibles ciberataques o fallos del AD.

- Actuar como un marco de referencia para la gestión y supervisión de los proveedores de servicios tecnológicos.
- Ser un modelo eficiente, de fácil adopción y flexible a organizaciones de todos los sectores económicos.

2. Marco Conceptual

Este capítulo desarrolla los conceptos fundamentales que sustentan la presente investigación. Se abordan la ciberresiliencia, los riesgos inherentes al Directorio Activo (AD), su papel central en la arquitectura de TI, su integración con Entra ID, y los principales marcos normativos y estándares internacionales que respaldan el diseño de un modelo de gestión de ciberresiliencia en el contexto financiero.

2.1. Ciberresiliencia

La ciberresiliencia se define como la capacidad de una organización para anticipar, resistir, responder y recuperarse frente a incidentes de seguridad que comprometan sus activos digitales, procesos críticos o continuidad operativa. Según el NIST SP 800-160 Vol. 2, implica una combinación de seguridad proactiva, tolerancia a fallos, recuperación operativa y aprendizaje organizacional.

El Instituto Nacional de Estándares y Tecnología (NIST) define la resiliencia cibernética como la capacidad de anticipar, resistir, recuperarse y adaptarse a condiciones adversas, ciberataques o brechas en los sistemas que emplean o se habilitan mediante recursos cibernéticos. Además, señala que el propósito de la resiliencia cibernética es asegurar el logro de los objetivos del negocio en un entorno de constante transformación y acelerado proceso de digitalización (National Institute of Standards and Technology, 2020).

El Foro Económico Mundial describe la resiliencia cibernética como la capacidad de una organización para reducir al mínimo las consecuencias de incidentes cibernéticos graves que puedan comprometer sus metas y objetivos fundamentales, demandando un monitoreo permanente y una planificación estratégica continua (World Economic Forum, 2025).

La Agencia de la Unión Europea para la Ciberseguridad (ENISA), describe a la ciberresiliencia como la capacidad de una organización para resistir, responder y recuperarse de ciberataques, manteniendo la continuidad de sus operaciones y aprendiendo de los incidentes para fortalecer su postura de seguridad (European Union Agency for Cybersecurity, 2024).

Según IBM, la resiliencia cibernética es la capacidad de una institución para prevenir, resistir y recuperarse de ciberataques. Además, señala que la ciberresiliencia contribuye en la capacidad de una organización para mantener su operación (IBM, 2025).

El Banco Central Europeo establece que la ciberresiliencia es la capacidad de resguardar los datos y sistemas electrónicos frente a los ciberataques, además de restablecer las actividades comerciales rápidamente en caso de que un ataque tenga éxito (European Central Bank, 2025).

El Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, define a la resiliencia operativa digital como la capacidad de una entidad financiera para garantizar la continuidad y calidad operativa de sus servicios financieros, incluso en caso de perturbaciones, ya sea mediante el uso de servicios TIC propios y/o subcontratado a proveedores (European Union Agency for Cybersecurity, 2023).

El BBVA señala que el propósito del Reglamento Europeo de Resiliencia Operativa Digital (DORA) es reforzar la capacidad de defensa de las instituciones financieras frente a ciberataques, permitiéndoles resistir y recuperarse tanto de incidentes cibernéticos como aquellos vinculados con las tecnologías de la información (BBVA, 2025).

La Superintendencia de Banca, Seguros y AFP (SBS) del Perú considera la resiliencia operacional, como la capacidad de las empresas para garantizar la continuidad de sus actividades esenciales incluso frente a interrupciones (Superintendencia de Banca, Seguros y AFP, 2024).

Según Microsoft, la resiliencia operativa es la capacidad de recuperarse de un ciberataque, una interrupción u otra alteración con un tiempo de inactividad o interrupción de los servicios mínimos o nulos (Microsoft, 2025).

El Reglamento Europeo de Resiliencia Operativa Digital (DORA) además de definir los requisitos para fortalecer la resiliencia digital en las entidades financieras, establece obligaciones para los proveedores de servicios TIC críticos que les brindan soporte, independientemente de su lugar de operación y tipo de infraestructura (dedicadas o nube) (Diario Oficial de la Unión Europea, 2022). Entre las principales exigencias contempla:

- Gestión del riesgo de terceros de servicios TIC.
- Establecimiento de acuerdos contractuales.
- Supervisión o auditorías a los proveedores de servicios críticos.
- Cumplimiento de los requisitos de DORA.

Microsoft es considerado un proveedor externo de servicios TIC crítico, debido a la relevancia de productos que provee, tales como el servicio de autenticación mediante el Directorio Activo (Microsoft, 2025). La empresa afirma cumplir con todas las leyes y regulaciones vigentes y garantiza que los acuerdos contractuales establecidos con sus clientes se ajustan a las disposiciones de DORA. Además, proporciona información de verificación de sus servicios, incluyendo certificaciones internacionales, datos de desempeño, informes de incidentes y análisis periódicos.

A diferencia de la ciberseguridad tradicional, centrada en la prevención y detección de amenazas, la ciberresiliencia incorpora una visión integral y estratégica que abarca desde la identificación de vulnerabilidades hasta la recuperación efectiva tras un incidente, pasando por la gestión del cambio organizacional y la cultura de seguridad.

En esta tesis, la ciberresiliencia se aborda como un modelo de gestión adaptativo, orientado a minimizar el impacto operativo y reputacional de un ataque al Directorio Activo, alineado con buenas prácticas internacionales como Zero Trust, y considerando dimensiones críticas como:

- Controles técnicos (MFA, PAM, respaldo, monitoreo).
- Continuidad operativa y recuperación ante desastres.
- Gobernanza y cumplimiento normativo (DORA, NIST CSF v2.0, ISO/IEC 27001:2022 e ISO/IEC 22301: 2019).

- Evaluación de madurez y planes de mejora continua.

2.2. Directorio Activo (Active Directory) y su rol en la seguridad

El Directorio Activo (AD) es un servicio de directorio desarrollado por Microsoft, utilizado por la mayoría de las organizaciones empresariales a nivel global. Su función es centralizar la gestión de identidades digitales, políticas de acceso, autenticación y autorización dentro de una red basada en Windows Server.

En el sector financiero, el AD es considerado una infraestructura crítica, ya que controla el acceso a servicios transaccionales, aplicativos bancarios, sistemas de información financiera y bases de datos sensibles. Cualquier compromiso al AD puede traducirse en pérdida total de control, interrupción operativa o diseminación lateral de malware.

La gestión segura del AD requiere un enfoque integral que contemple segmentación de privilegios, hardening, monitoreo de eventos, auditorías periódicas y políticas de recuperación frente a secuestros del dominio.

Como se menciona en el primer capítulo de esta investigación, el Directorio Activo es un activo fundamental en cualquier organización, ya que estructura los sistemas dentro de una red y controla los permisos y accesos. En este sentido, si el AD llegara a verse comprometido, resulta crucial llevar a cabo una recuperación eficiente para impedir que la brecha de seguridad se mantenga y garantizar la pronta restauración de los servicios del dominio.

Cuando hablamos del compromiso del Directorio Activo nos referimos a la manera en que un atacante puede obtener acceso y comprometer su integridad. Por ello, para entender los posibles escenarios de afectación, es fundamental conocer tanto su estructura como los elementos que lo conforman.

El Directorio Activo está estructurado en una serie de niveles jerárquicos que abarca desde los objetos hasta los bosques (Microsoft, 2025):

- **Objeto:** Es la unidad más básica del Directorio Activo. Representa un recurso, como un usuario, equipo, grupo o impresora.

- **Unidad Organizativa (OU):** Permite organizar y agrupar los objetos dentro del Directorio Activo.
- **Dominio**: Es una unidad administrativa dentro del Directorio Activo. Contiene una colección de objetos y unidades organizativas.

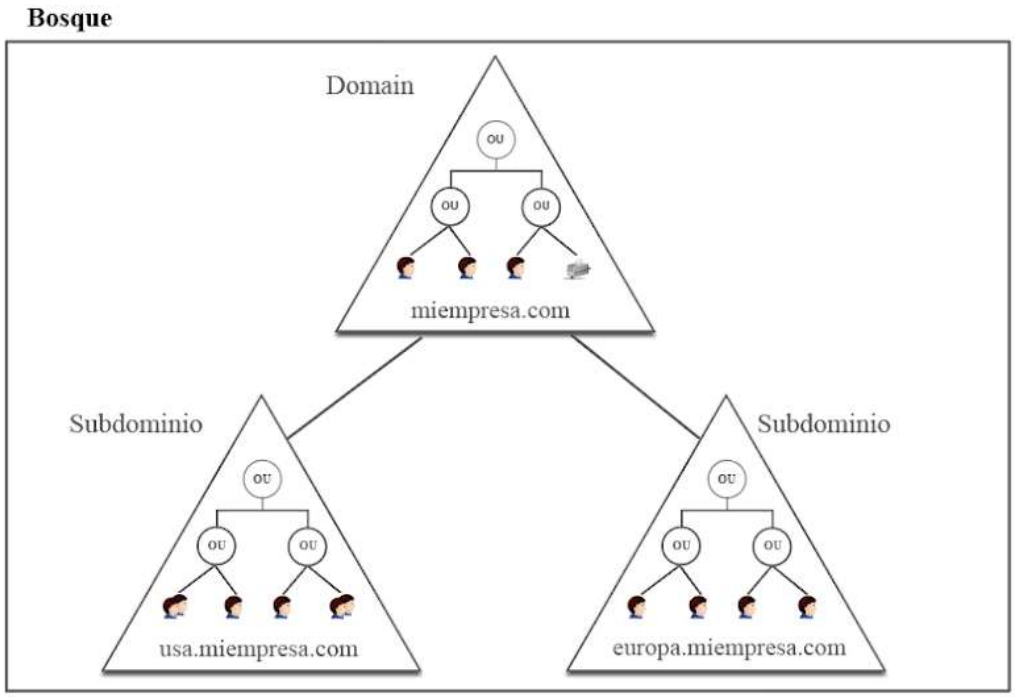
El Controlador de Dominio (CD) es un componente esencial para el adecuado funcionamiento de un dominio. Su principal responsabilidad es la gestión de la autenticación de los usuarios y equipos dentro de dicho dominio. Opera como un inspector, verificando las credenciales de los usuarios y determinando si concede o deniega el acceso (Microsoft, 2025).

- **Árbol de Dominios:** Es un grupo de dominios interconectados que comparten un mismo esquema de nombres y están unidos mediante relaciones de confianza (Microsoft, 2025).
- **Bosque de Directorio Activo:** Es el nivel más alto dentro de la jerarquía del Directorio Activo, compuesto por una agrupación de dominios y/o árboles de dominios (Microsoft, 2025).

La siguiente Figura 1 se ilustra el esquema de esta estructura jerárquica:

Figura 1

Estructura Jerarquía del Directorio Activo



Nota. Fuente: Elaboración propia

2.2.1. Amenazas frecuentes al AD

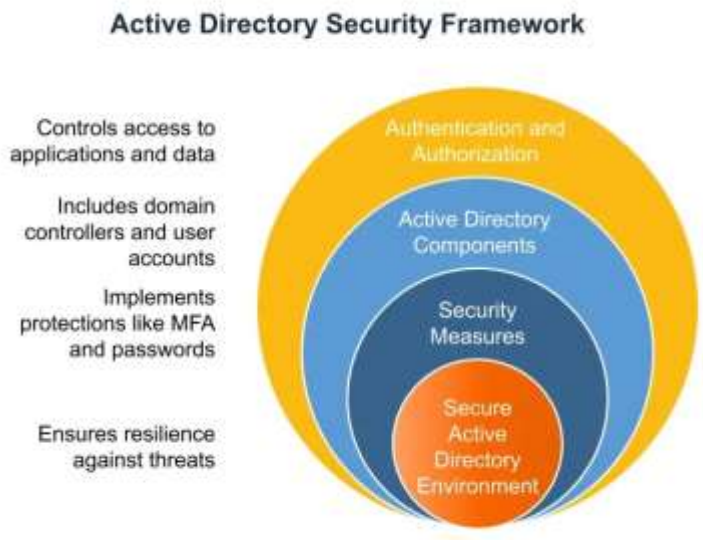
Entre las amenazas más comunes al AD destacan:

- Ataques de fuerza bruta o pass-the-hash contra controladores de dominio.
- Escalada de privilegios mediante vulnerabilidades de delegación o relaciones de confianza mal configuradas.
- Persistencia mediante técnicas de Golden Ticket o Silver Ticket, que otorgan privilegios de dominio a atacantes.
- Ransomware dirigido que primero compromete el AD para luego distribuir cargas maliciosas a toda la red.
- Rogue Domain Controllers, que permiten a un atacante emular un controlador legítimo y obtener credenciales.

Estas amenazas, ampliamente documentadas en el marco: MITRE ATT&CK for Active Directory, justifican la necesidad de controles avanzados de seguridad, como monitoreo de replicación, MFA obligatorio para administradores y políticas PAM.

Figura 2

Active Directory Framework



Nota. Fuente: Fidelis Security, 2025.

El compromiso del Directorio Activo por parte de un atacante puede derivar en movimientos laterales, escalamiento de privilegios, cifrado del AD, eliminación de cuentas e incluso la desactivación total del servicio. Estas acciones representan un riesgo significativo para cualquier organización, ya que pueden afectar la disponibilidad e integridad de sus sistemas. Por ello, es esencial que las organizaciones utilicen un sistema operativo confiable que les permita enfrentar amenazas cada vez más avanzadas.

La presente investigación propone la implementación de una arquitectura híbrida de Active Directory, combinando la infraestructura tradicional de Microsoft Windows Server 2025 con los servicios en la nube de Microsoft Entra ID. Esta decisión responde a la necesidad de garantizar mayor flexibilidad, seguridad y continuidad operativa. Gracias a este enfoque híbrido, es posible aprovechar lo mejor de ambos entornos. Se conserva el control local sobre los recursos internos y sistemas heredados esenciales para las operaciones diarias, mientras se

incorporan capacidades avanzadas de seguridad y administración disponibles exclusivamente en la nube:

- Autenticación Multifactor (MFA): Añade una capa adicional de seguridad al proceso de inicio de sesión.
- Protección de Identidad: Utiliza el aprendizaje automático para identificar actividades inusuales y posibles vulnerabilidades.
- Acceso Condicional: Permite establecer políticas que limitan el acceso basado en el comportamiento del usuario y otros factores.
- Gestión de Privilegios Justo a Tiempo (JIT): Limita el acceso a recursos sensibles sólo cuando es necesario.
- Escalabilidad y Adaptabilidad: Sin necesidad de depender únicamente del hardware interno.

2.2.2. Herramientas de ataque al AD

Los actores maliciosos emplean herramientas ofensivas, muchas de ellas de uso legítimo en pruebas de penetración, que permiten mapear, explotar y controlar entornos con AD. Las más utilizadas incluyen:

- Mimikatz: para extraer credenciales en memoria.
- BloodHound: para mapear rutas de privilegios en el dominio.
- PowerSploit y Nishang: marcos ofensivos basados en PowerShell.
- Cobalt Strike: usado para persistencia, explotación y movimiento lateral.

Estas herramientas, cuando son usadas sin detección, permiten a un atacante tomar control total del dominio y preparar la infraestructura para un ataque destructivo.

2.2.3. Entra ID y su integración con AD

Microsoft Entra ID (anteriormente Azure Active Directory) es la plataforma de identidad basada en la nube que complementa al AD tradicional, ofreciendo autenticación federada, acceso condicional, protección contra amenazas e integración con aplicaciones SaaS.

En entornos híbridos, Entra ID permite extender la seguridad del AD mediante:

- MFA obligatorio y adaptable según riesgo.
- Privileged Identity Management (PIM) para controlar el uso temporal de privilegios.
- Auditorías centralizadas y reportes de seguridad en tiempo real.
- Microsoft Defender for Identity para detección avanzada de amenazas en AD local.

La integración AD + Entra ID será fundamental en el modelo propuesto de esta tesis, al permitir una defensa más robusta basada en visibilidad, automatización y respuesta orquestada.

2.3. Marcos normativos y estándares de ciberresiliencia

El modelo de gestión de ciberresiliencia que se propone en esta investigación se fundamenta en los principales marcos regulatorios y normativos reconocidos a nivel internacional. Estos proporcionan principios, controles y estructuras metodológicas que guían la construcción de una arquitectura segura y resiliente.

2.3.1. Ley de Resiliencia Operativa Digital (DORA)

DORA (Digital Operational Resilience Act), promovida por la Unión Europea, tiene como objetivo garantizar que todas las entidades del sistema financiero puedan resistir, responder y recuperarse de incidentes TIC severos (Diario Oficial de la Unión Europea, 2022). Establece cinco pilares clave:

- Gestión de riesgos TIC.
- Gestión de incidentes.
- Pruebas de resiliencia operativa digital.
- Gestión de riesgos de terceros.
- Compartición de información sobre amenazas.

Aunque aún no se aplica formalmente en Perú, DORA representa una referencia normativa clave para el fortalecimiento de la resiliencia financiera. Su adopción voluntaria puede elevar el nivel de madurez institucional frente a ataques sofisticados, como los dirigidos al AD.

2.3.2. NIST Cybersecurity Framework (CSF)

El NIST CSF, desarrollado por el Instituto Nacional de Estándares y Tecnología de EE. UU., organiza la ciberseguridad en cinco funciones centrales (National Institute of Standards and Technology, 2024):

- Identificar: activos críticos, riesgos, dependencias.
- Proteger: a través de controles técnicos y administrativos.
- Detectar: amenazas mediante monitoreo continuo y análisis.
- Responder: con protocolos definidos ante incidentes.
- Recuperar: asegurando continuidad y lecciones aprendidas.

El NIST CSF será utilizado para estructurar tanto el modelo como el cuestionario de evaluación de ciberresiliencia, permitiendo medir el nivel de madurez de la organización frente a cada función clave.

2.3.3. ISO/IEC 27001 e ISO/IEC 22301

- ISO/IEC 27001: Norma internacional que define los requisitos para establecer, implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI). Proporciona un marco de gobernanza de la seguridad aplicable al entorno del AD.
- ISO/IEC 22301: Norma de gestión de la continuidad del negocio, que garantiza la capacidad de la organización para recuperarse ante disrupciones severas.

Estas normas complementan los marcos anteriores al reforzar los aspectos operativos, estratégicos y de cumplimiento del modelo propuesto.

3. Marco Contextual

El presente capítulo contextualiza la problemática investigada en relación con el entorno global, regional y local, resaltando la criticidad del Directorio Activo en las

entidades financieras. Se abordan los patrones de amenazas cibernéticas emergentes, las experiencias regionales en ataques al AD y las particularidades del sistema financiero peruano, tanto a nivel macro como micro, para justificar la necesidad del modelo propuesto.

3.1. Contexto Global

La ciberseguridad se ha transformado en un componente esencial de la estabilidad económica global. Organismos como el World Economic Forum han identificado los ciberataques a infraestructuras críticas como una de las cinco principales amenazas para la economía mundial (World Economic Forum, 2025). En este contexto, el Directorio Activo (Active Directory, AD) se ha convertido en un objetivo predilecto de actores maliciosos debido a su rol estratégico en la gestión de identidades y accesos en entornos Windows Server.

Estudios de Microsoft indican que más del 90% de los ataques dirigidos avanzados (APT) implican algún grado de compromiso del AD (Microsoft, 2022). Este tipo de ataques permite a los adversarios escalar privilegios, mantener persistencia y propagar malware de forma masiva. Casos como los de SolarWinds, Hafnium y Lapsus$ demuestran cómo la explotación de servicios de identidad, incluido el AD, facilita compromisos a gran escala y afecta a gobiernos, bancos y corporaciones multinacionales.

Ante esta amenaza creciente, organizaciones internacionales han comenzado a adoptar modelos de ciberresiliencia, basados en principios como Zero Trust, segmentación de privilegios, automatización de respuesta y planes de recuperación robustos. Así, el enfoque tradicional de “defensa perimetral” ha evolucionado hacia una gestión integrada del riesgo digital, en la cual el AD figura como una prioridad estratégica de protección.

3.1.1. Unión Europea

El concepto de ciberresiliencia está ganando cada vez más aceptación y uso a nivel mundial, consolidándose como un componente clave de las estrategias organizacionales. A diferencia del enfoque tradicional de la seguridad de la información, centrado principalmente en proteger la información y evitar que ocurran incidentes,

la ciberresiliencia parte de la premisa de que los incidentes son inevitables y pueden afectar transversalmente a diversas áreas de una organización. Esto incluye no solo la infraestructura tecnológica, sino también la gestión de procesos, las operaciones y los planes de continuidad del negocio. Su objetivo no es solo la prevención, sino también garantizar que las organizaciones puedan responder, adaptarse y recuperarse rápidamente ante ciberamenazas, minimizando disrupciones y asegurando la continuidad operativa en un entorno cada vez más complejo y dinámico.

En ese contexto, y ante el aumento exponencial de ciberataques sofisticados que impactan sectores críticos como la banca, la energía, la salud y las comunicaciones, los gobiernos, organismos multilaterales y entidades regulatorias han comenzado a emitir regulaciones internacionales con el fin de elevar los estándares mínimos de ciberseguridad y resiliencia.

Un ejemplo destacado de este tipo de normativa es la Ley de Resiliencia Operativa Digital (Reglamento DORA), publicada por el Parlamento Europeo y el Consejo de la Unión Europea el 14 de diciembre de 2022 y entró en vigor el 16 de enero de 2023. A partir de esa fecha, las entidades financieras dispusieron de un plazo de dos años para adecuarse a sus disposiciones. El 17 de enero del año 2025, comenzó el proceso formal de supervisión por parte de las autoridades competentes (Diario Oficial de la Unión Europea, 2022). Esta regulación aplica a diversas entidades del sistema financiero de la Unión Europea:

- Bancos comerciales y de inversión.
- Compañías de seguros y reaseguros.
- Gestores de fondos.
- Sociedades de valores.
- Plataformas de negociación.

- Proveedores de servicios de compensación y liquidación de valores.
- Agencias de calificación crediticia.

Asimismo, el Reglamento DORA se compone de:

- Considerandos: Los 106 considerandos son explicaciones que desarrollan y justifican el porqué de cada obligación o artículo del reglamento.
- Artículos: Los 64 artículos organizados en seis capítulos. Constituyen la parte jurídicamente vinculante, dado que, establecen las obligaciones específicas.

En la Tabla 1, se describe la estructura de los capítulos y artículos del Reglamento DORA

Tabla 1

Estructura de los Capítulos y Artículos del Reglamento DORA

Capítulo	Tema	Artículos
I. Disposiciones generales	Ámbito, definiciones	1 - 6
II. Gestión del riesgo TIC	Políticas internas, protección	7 - 14
III. Gestión de incidentes TIC	Notificación y respuesta a incidentes	15 - 21
IV. Pruebas de resiliencia	Tests periódicos y avanzados	22 - 27

Capítulo	Tema	Artículos
V. Riesgo de terceros TIC	Contratos, subcontratación, proveedores	28 - 39
VI. Disposiciones finales	Supervisión, sanciones, entrada en vigor	40 - 64

Nota. Fuente: Ley de Resiliencia Operativa Digital (DORA)

- **Normativas Técnicas**: Son documentos jurídicos que desarrollan o explican cómo las entidades financieras deben cumplir con las obligaciones de resiliencia operativa digital. Además del cuerpo normativo principal, el Reglamento DORA se complementa con una serie de Normas Técnicas de Regulación (RTS) y Normas Técnicas de Ejecución (ITS), redactadas por las Autoridades Europeas de Supervisión (AES) y aprobadas por la Comisión Europea. Las AES están conformadas por:

- Autoridad Bancaria Europea (EBA), con sede en París, Francia.
- Autoridad Europea de Valores y Mercados (ESMA), con sede en París, Francia.
- Autoridad Europea de Seguros y Pensiones de Jubilación (EIOPA), con sede en Frankfurt, Alemania.

A continuación, se describen las principales normas técnicas de regulación y ejecución adoptados por la Comisión Europea mediante reglamentos delegados:

- **Reglamento Delegado (UE) 2024/1774 - RTS sobre el Marco de Gestión de Riesgos de las TIC:** Desarrolla lo dispuesto en el artículo 15, párrafo cuarto, y el artículo 16, apartado 3, párrafo cuarto, del Reglamento (UE) 2022/2554. Mediante este acto delegado, se adopta la norma técnica de regulación que especifica las herramientas, métodos, procedimientos y políticas que las entidades

financieras deben implementar para identificar, prevenir y gestionar los riesgos TIC. Dicha norma tiene en cuenta el tamaño, la naturaleza, la complejidad y el perfil de riesgo de cada entidad, garantizando un enfoque proporcional y adaptado a sus características operativas (Diario Oficial de la Unión Europea, 2024).

- **Reglamento Delegado (UE) 2024/1772 - RTS sobre Clasificación de Incidentes de TIC:** Desarrolla lo dispuesto en el artículo 18, apartado 4, párrafo tercero, del Reglamento (UE) 2022/2554. Mediante este acto delegado, se adopta la norma técnica de regulación que especifica los criterios para clasificar los incidentes relacionados con las TIC y las ciberamenazas. Además, establece niveles de gravedad según el impacto que puedan tener estos incidentes en la actividad de una entidad financiera. También indica con detalle qué información debe incluirse cuando se notifica un incidente grave a las autoridades competentes (Diario Oficial de la Unión Europea, 2024).

- **Reglamento Delegado (UE) 2025/302 - RTS sobre el Informe de Incidentes de TIC:** Desarrolla lo dispuesto en el artículo 20, párrafo tercero, del Reglamento (UE) 2022/2554. Mediante este acto delegado, se adopta la norma técnica de regulación que establece qué información deben incluir las entidades financieras cuando informan sobre incidentes graves relacionados con la tecnología, como fallos informáticos o ciberataques. También define los plazos para enviar el aviso inicial, el informe intermedio y el informe final. Precisa también el contenido de las notificaciones voluntarias cuando una entidad detecta una posible amenaza cibernética importante, aunque no se haya materializado (Diario Oficial de la Unión Europea, 2025).

- **Reglamento Delegado (UE) 2024/1773 - RTS sobre Política de Terceros en Materia de TIC:** Desarrolla lo dispuesto en el artículo 28, apartado 10, párrafo tercero, del Reglamento (UE) 2022/2554. Mediante este acto delegado, se adopta la norma técnica de regulación que especifica el detalle qué debe contener la política

interna de las entidades financieras cuando contratan servicios tecnológicos esenciales o importantes (como servicios en la nube, procesamiento de datos, etc.) con proveedores externos. El objetivo es asegurar que estos contratos estén bien gestionados, documentados y supervisados, especialmente cuando los servicios son críticos para el funcionamiento de la entidad financiera (Diario Oficial de la Unión Europea, 2024).

- **Reglamento Delegado (UE) 2025/2956 - ITS del Registro de Información de Proveedores:** Desarrolla lo dispuesto en el artículo 29, apartado 9, párrafo segundo, del Reglamento (UE) 2022/2554. Mediante este acto delegado, se adopta la norma técnica de ejecución en lo que respecta a las plantillas estandarizadas que las entidades financieras deben utilizar para registrar y mantener la información sobre los servicios tecnológicos que contratan con proveedores externos. Estas plantillas ayudan a garantizar que la información se encuentre organizada y completa, lo que facilita su revisión por las autoridades competentes y mejora el gobierno de los servicios tecnológicos clave (Diario Oficial de la Unión Europea, 2025).

- **Reglamento Delegado (UE) 2024/1502 - RTS sobre los Criterios de Designación de Proveedores Críticos TIC:** Desarrolla lo dispuesto en el artículo 31, apartado 6, del Reglamento (UE) 2022/2554. Mediante este acto delegado, se adopta la norma técnica de regulación que especifica los criterios para la designación de proveedores terceros de servicios (Diario Oficial de la Unión Europea, 2024).

- **Reglamento Delegado (UE) 2025/420 - RTS sobre los Criterios y Procedimientos del Equipo de Supervisión:** Desarrolla lo dispuesto en el artículo 41, apartado 2, párrafo segundo, del Reglamento (UE) 2022/2554. Mediante este acto delegado, se adopta la norma técnica de regulación donde se especifican los criterios para conformar el equipo conjunto de examinadores, asegurando una representación equilibrada entre el personal de las Autoridades

Europeas de Supervisión y las autoridades competentes correspondientes. También se especifican los procedimientos para su designación, las funciones que desempeñarán y la forma en que llevarán a cabo su labor (Diario Oficial de la Unión Europea, 2025).

- **Reglamento Delegado (UE) 2025/295 - RTS sobre la Armonización de las Condiciones de Supervisión:** Desarrolla lo dispuesto en el artículo 41, apartado 2, párrafo segundo, del Reglamento (UE) 2022/2554. Mediante este acto delegado, se adopta la norma técnica de regulación que establece reglas comunes para facilitar que las autoridades de supervisión puedan realizar su labor de forma coherente y coordinada en toda la Unión Europea (Diario Oficial de la Unión Europea, 2025).
- **Reglamento Delegado (UE) 2025/1505 - RTS sobre las Tarifas de Supervisión a Proveedores Críticos:** Desarrolla lo dispuesto en el artículo 43, apartado 2, del Reglamento (UE) 2022/2554. Mediante este acto delegado, se adopta la norma técnica de regulación mediante el cual se establecen las reglas para calcular cuánto deben pagar los proveedores terceros esenciales de servicios de TIC por la supervisión que reciben. También se explican las formas en que deben hacer estos pagos al supervisor principal (Diario Oficial de la Unión Europea, 2024).

Además, de la emisión del Reglamento de Ciberresiliencia; así como de las Normas Técnicas de Regulación (RTS) y Normas Técnicas de Ejecución (ITS), en el año 2024 el Banco Central Europeo llevó a cabo el primer ejercicio sobre ciberresiliencia, en el que evaluaron las capacidades de recuperación y respuesta de 109 entidades financieras frente a un ciberataque (European Central Bank, 2024).

La narrativa del ejercicio se basó en un escenario ficticio en el que fallaban todas las medidas preventivas y un ciberataque comprometía gravemente las bases de datos de los principales

sistemas de la entidad. Por tanto, la evaluación se centró en analizar la eficacia de los planes de respuesta ante crisis, incluída la restauración de los datos desde copias de seguridad, la coordinación con proveedores de servicios externos críticos, la gestión de las comunicaciones externas, la identificación de los servicios afectados, y la estimación de las pérdidas directas e indirectas derivadas del ciberincidente (European Central Bank, 2024).

En términos generales, los resultados del ejercicio fueron satisfactorios y demostró que las entidades cuentan con marcos de respuesta y recuperación. No obstante, se identificaron oportunidades de mejora, entre ellas: la necesidad de evaluar de forma adecuada las dependencias de proveedores externos críticos de TIC y de estimar con mayor precisión las pérdidas económicas ocasionadas por un ciberataque (European Central Bank, 2024).

En conclusión, la implementación del Reglamento DORA, junto con la adopción de las Normas Técnicas de Regulación y Ejecución, así como el ejercicio de prueba de ciberresiliencia liderado por el Banco Central Europeo en 2024, reflejan el sólido compromiso de la Unión Europea con el fortalecimiento de la ciberresiliencia en el sector financiero. Estas iniciativas no solo elevan los estándares de protección ante amenazas digitales, sino que posicionan al sistema financiero europeo a la vanguardia y referente global en materia de ciberresiliencia.

3.1.2. Estados Unidos de América (EEUU)

La Federal Financial Institutions Examination Council (FFIEC) fue establecida por el congreso de Estados Unidos en marzo de 1979 con el propósito de emitir estándares uniformes y promover supervisión de los riesgos tecnológicos en las instituciones financieras. Aunque los estándares publicados por la FFIEC no tienen poder regulatorio directo, en la práctica se convierten en obligatorios, ya que son adoptados e implementados por las agencias federales reguladoras de los bancos,

instituciones de crédito, entre otros (Federal Financial Institutions Examination Council, 2025).

La FFIEC ha publicado una serie de guías que abordan aspectos clave de la gestión de tecnologías de la información y conforman el Manual de Examen de Tecnologías de la Información (IT Examination Handbook). No obstante, el presente trabajo de investigación abordará aquellas guías que tratan sobre la continuidad del negocio, la seguridad de la información y la relación y supervisión de proveedores de servicios tecnológicos, ya que son fundamentales para garantizar la capacidad de una entidad de anticipar, resistir, recuperarse y adaptarse ante ciberataques o interrupciones operativas (Federal Financial Institutions Examination Council, 2025).

- **Gestión de la Continuidad del Negocio:** Establece un marco integral para que las entidades financieras aseguren la continuidad de sus operaciones ante eventos disruptivos. Su objetivo es promover tanto la recuperación posterior a incidentes como una resiliencia operativa continua, integrando la gestión de continuidad al ciclo de vida del riesgo, la planificación estratégica y la gobernanza corporativa (Federal Financial Institutions Examination Council, 2025).

  Las estrategias de continuidad deben ser proporcionales al perfil de riesgo de la entidad y considerar aspectos clave como el personal, la tecnología, las instalaciones, las telecomunicaciones y los proveedores. Destacando aquellas estrategias orientadas a la ciberresiliencia, las cuales son fundamentales frente a la creciente sofisticación y frecuencia de los ciberataques (Federal Financial Institutions Examination Council, 2025).

  Por otro lado, enfatiza que los ejercicios y pruebas son esenciales para validar la efectividad del plan de continuidad. Estos ejercicios deben incluir escenarios tipo “tabletop”, escenarios realistas, probar sistemas alternativos y verificar tiempos de recuperación.

Asimismo, se deben involucrar a proveedores clave y servir como base para identificar mejoras y reforzar la preparación institucional (Federal Financial Institutions Examination Council, 2025).

- **Seguridad de la Información**: Ofrece una guía integral para que las instituciones financieras desarrollen, implementen y mantengan programas efectivos de seguridad de la información. Enfatiza que la protección de los sistemas y datos sensibles es fundamental para la solidez operativa y financiera de cualquier entidad. Por ello, la seguridad de la información debe integrarse plenamente en los procesos organizacionales, contar con el respaldo de la alta dirección y ser evaluada periódicamente mediante revisiones independientes. Su enfoque se basa en los principios de confidencialidad, integridad y disponibilidad de la información, y en la necesidad de protegerla frente a acciones maliciosas o accidentales que puedan comprometer la operatividad o la reputación institucional (Federal Financial Institutions Examination Council, 2025).

  La guía recomienda adoptar prácticas rigurosas de contratación, que incluyan la verificación de antecedentes y revisiones periódicas, especialmente para puestos con acceso privilegiado. Todo empleado o contratista con acceso a sistemas o datos debe firmar acuerdos de confidencialidad y uso autorizado. En cuanto a la cadena de suministro, se aconseja adquirir productos tecnológicos únicamente de proveedores confiables, aplicar revisiones técnicas y resguardar la identidad institucional en los procesos de compra, con el fin de mitigar el riesgo de componentes comprometidos (Federal Financial Institutions Examination Council, 2025).

  Asimismo, se establece la necesidad de supervisar a los proveedores de servicios externos mediante procesos de due diligence previos a la contratación, inclusión de cláusulas específicas de seguridad en los contratos, realización de

auditorías periódicas y coordinación en los planes de respuesta a incidentes. La responsabilidad sobre la seguridad de la información no se delega, por lo que la entidad financiera debe asegurar el cumplimiento continuo de sus estándares por parte de los terceros (Federal Financial Institutions Examination Council, 2025).

Finalmente, la guía señala que para garantizar la efectividad del programa de seguridad, éste debe someterse a auditorías periódicas cuyos resultados deben facilitar la toma de decisiones informadas y la mejora continua de los controles y procesos (Federal Financial Institutions Examination Council, 2025).

- **Relación y Supervisión de Proveedores de Servicios Tecnológicos**: Proporciona orientación sobre la gestión de riesgos asociados con la subcontratación de servicios tecnológicos, incluyendo la evaluación de la resiliencia cibernética de los proveedores externos y la planificación de la continuidad del negocio con estos actores (Federal Financial Institutions Examination Council, 2025).

La guía añade que la selección de proveedores debe basarse en una definición de requisitos claros, un proceso riguroso de diligencia debida y análisis de factores como estabilidad financiera, experiencia, cumplimiento legal y capacidades tecnológicas. Una vez contratado el servicio del proveedor, la institución debe mantener un monitoreo continuo del cumplimiento de los niveles de servicio, controles de seguridad, planes de continuidad y auditorías externas (Federal Financial Institutions Examination Council, 2025).

En referencia a relaciones con múltiples proveedores, ya sea de forma directa o a través de un proveedor principal, se requiere supervisión activa para garantizar el cumplimiento de estándares de seguridad y coordinación entre servicios. Además, si la

> subcontratación involucra servicios en el extranjero, deben evaluarse riesgos legales, regulatorios y de soberanía de datos, así como asegurar el cumplimiento normativo y el acceso de los supervisores a la información (Federal Financial Institutions Examination Council, 2025).

Las guías de la FFIEC establecen un marco esencial para que las instituciones financieras fortalezcan su ciberresiliencia ante amenazas tecnológicas, a través de la gestión de la continuidad del negocio, la seguridad de la información y la supervisión de proveedores tecnológicos, se busca asegurar la operatividad, protección de datos y cumplimiento normativo. Por tanto, aplicar estos lineamientos de forma rigurosa y con respaldo de la alta dirección no solo es una buena práctica, sino una necesidad estratégica para garantizar la confianza, solidez y sostenibilidad del sector financiero frente a un entorno de riesgos tecnológicos en constante evolución.

Por otro lado, y además de las guías emitidas por la FFIEC, Estados Unidos ha emitido la NIST SP 800-53 como un marco técnico diseñado para fortalecer la resiliencia operativa y la seguridad cibernética de las instituciones.

El objetivo del NIST SP 800-53 es proporcionar un catálogo integral de controles de seguridad y privacidad para proteger los sistemas de información y las organizaciones frente a amenazas cibernéticas, vulnerabilidades y riesgos operativos (National Institute of Standards and Technology, 2024). Se trata de un marco de referencia desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), por lo que su implementación es opcional, salvo en aquellos casos en que sea exigida por normativas específicas, como en ciertas entidades federales que gestionan información o sistemas en nombre del gobierno de Estados Unidos, conforme a lo establecido en la Ley Federal de Modernización de la Seguridad de la Información (FISMA). En ese sentido, su aplicación es obligatoria para:

- Agencias del Gobierno Federal de EE. UU.
- Departamentos y Organismos del Poder Ejecutivo (incluyendo la NASA).
- Contratistas y Proveedores Federales.

La NIST SP 800-53 se complementa con dos documentos clave:

- **NIST SP 800-53B:** Proporciona la línea base de controles seguridad y privacidad que deben implementarse según el nivel de riesgo del sistema. Su propósito es simplificar la selección de controles, ya que permite personalizarlos o ajustarlos conforme a las necesidades específicas de la organización, asegurando que no se implementen controles innecesarios ni se omitan aquellos que son críticos para la protección del sistema (National Institute of Standards and Technology, 2024).
- **NIST SP 800-53A:** Se enfoca en la evaluación y validación de los controles de seguridad y privacidad establecidos en NIST SP 800-53. Proporciona una serie de procedimientos y métodos de evaluación para determinar si los controles implementados son efectivos y si los riesgos asociados a los sistemas de información están siendo gestionados adecuadamente. Además, incorpora enfoques de valoración tanto cualitativos como cuantitativos, lo que permite obtener una visión integral y equilibrada del panorama de riesgos, facilitando así decisiones informadas sobre la seguridad y la resiliencia operativa (National Institute of Standards and Technology, 2024).

  El NIST SP 800-53, junto con sus documentos complementarios SP 800-53A y SP 800-53B, ofrece un marco técnico sólido para fortalecer la resiliencia operativa y la seguridad cibernética. Además, su acceso gratuito, enfoque adaptable y aplicabilidad a cualquier industria y tamaño de organización han hecho que su uso se extienda ampliamente a nivel mundial.

Del análisis realizado sobre el contexto global de la ciberresiliencia, se concluye que está evolucionando rápidamente como respuesta a un panorama de amenazas cada vez más complejo, frecuente y sofisticado. En ese escenario, las principales economías del mundo, como la Unión Europea y Estados Unidos, han adoptado enfoques sólidos, para proteger sus sectores financieros y garantizar la continuidad operativa. Al hacerlo, se consolidan como referentes y marcan el camino para que otras jurisdicciones establezcan sus propios marcos de resiliencia cibernética.

3.2. Contexto Regional

En América Latina, la transformación digital ha avanzado de manera desigual. Si bien los servicios financieros han adoptado tecnologías modernas, la madurez en ciberseguridad y resiliencia aún es limitada, lo que los convierte en blancos atractivos para grupos criminales y campañas de ransomware.

Casos relevantes incluyen:

3.2.1. Argentina

El Banco Central de la República Argentina (BCRA) ha desarrollado un marco regulatorio integral y robusto para fortalecer la ciberseguridad, la gestión de ciberincidentes y el control de los riesgos tecnológicos en el sistema financiero. Estas directrices buscan asegurar la resiliencia operativa del ecosistema ante amenazas cibernéticas, en línea con las mejores prácticas internacionales como las del Consejo de Estabilidad Financiera (FSB) (Banco Central de la República Argentina, 2025).

a) **Comunicación "A" 7724 - Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información:** Establece requisitos mínimos para gestionar y controlar los riesgos asociados a la tecnología y la seguridad de la información. Promueve un enfoque integral que abarca desde el gobierno corporativo y la gestión de riesgos hasta la continuidad del negocio, la ciberseguridad y la relación con terceros (Banco Central de la República Argentina, 2025).

b) **Comunicación "A" 7266: Respuesta y recuperación ante ciberincidentes (RRCI)**: Define lineamientos para la respuesta y recuperación ante ciberincidentes, con el objetivo de proteger la estabilidad financiera y fortalecer la ciberresiliencia del sistema. Fomenta la preparación anticipada, la coordinación efectiva, la documentación de incidentes y la implementación de medidas correctivas, promoviendo una cultura proactiva y colaborativa frente a amenazas cibernéticas (Banco Central de la República Argentina, 2025).

3.2.2. Brasil

El Banco Central de Brasil ha emitido regulaciones específicas para fortalecer la gestión de la seguridad de la información en el sistema financiero. La Resolución CMN Nº 4893, publicada en 2021 y aprobada por el Consejo Monetario Nacional, establece las directrices que deben seguir las instituciones financieras en relación con la política de seguridad cibernética y la contratación de servicios relevantes de procesamiento y almacenamiento de datos, incluidos los servicios prestados mediante computación en la nube. Su objetivo principal es reforzar la resiliencia operativa del sistema financiero frente a amenazas cibernéticas, garantizando la confidencialidad, integridad y disponibilidad de los datos y sistemas de información (Banco Central Do Brasil, 2025).

3.2.3. Chile

La Comisión para el Mercado Financiero (CMF) de Chile ha establecido un conjunto de regulaciones orientadas a fortalecer la gestión integral de riesgos en las entidades del sector financiero. Estas normativas, recogidas en los capítulos 20-8, 20-9 y 20-10 de la Recopilación Actualizada de Normas (RAN), abordan aspectos críticos como la seguridad de la información, la gestión de incidentes operacionales y la continuidad del negocio (Comisión del Mercado Financiero, 2025).

- **Capítulo 20-8 Información de Incidentes Operacionales**: Regula la gestión y el reporte de incidentes operacionales, con un enfoque especial en aquellos relacionados con la ciberseguridad. Establece que las entidades deben contar con sistemas que les permitan identificar, registrar, evaluar, mitigar y reportar estos incidentes. Además, dispone que las entidades deben notificar a la CMF dentro de los 30 minutos de ocurrido el incidente, sin importar el día ni la hora, y comunicar a los clientes si sus servicios se ven afectados. También se fomenta el intercambio de información entre entidades para prevenir la propagación de amenazas. Esta norma fue reforzada por la Norma de Carácter General N° 515, que exige un responsable designado para el reporte de incidentes y faculta a la CMF para solicitar planes de recuperación e informes forenses (Comisión del Mercado Financiero, 2025).
- **Capítulo 20-9 Gestión de la Continuidad del Negocio**: Establece lineamientos para asegurar la continuidad de los servicios críticos ante eventos disruptivos. Requiere una estrategia de continuidad aprobada por el Directorio, sustentada en análisis de impacto y riesgo (BIA y RIA), así como planes de contingencia actualizados y probados al menos una vez al año. También exige una infraestructura tecnológica resiliente, mecanismos de comunicación, capacitación continua y auditorías periódicas (Comisión del Mercado Financiero, 2025).
- **Capítulo 20-10 Gestión de Seguridad de la Información y Ciberseguridad**: Define lineamientos mínimos para una adecuada gestión de la seguridad de la información. Los principios fundamentales incluyen la protección de la confidencialidad, integridad y disponibilidad de la información, y la mitigación de riesgos del entorno digital. La norma exige estructuras organizacionales claras, políticas aprobadas por el Directorio, identificación de activos críticos, respuesta ante incidentes, auditorías y pruebas como análisis forense y pentesting,

fomentando una cultura de gestión de riesgos cibernéticos (Comisión del Mercado Financiero, 2025).

América Latina ha avanzado en la adopción de marcos regulatorios sólidos para fortalecer la ciberresiliencia en el sector financiero, con enfoques integrales en países como Argentina, Brasil y Chile. Aunque existen desafíos en su implementación y en la cooperación regional, el compromiso con la seguridad digital es creciente. Para consolidar estos avances, será clave seguir invirtiendo en tecnología, capacitando al personal y promoviendo una cultura de ciberseguridad institucional y colaborativa.

Estos eventos evidencian la ausencia de modelos estructurados de ciberresiliencia enfocados en el Directorio Activo, así como una limitada adopción de controles como PAM, MFA, backup automatizado y monitoreo continuo. Además, las regulaciones regionales varían en su exigencia, lo que deja margen a la adopción voluntaria de estándares internacionales como DORA, NIST CSF v2.0, ISO/IEC 27001:2022 e ISO/IEC 22301: 2019.

3.3. Contexto Local

3.3.1. Macroentorno

El sistema financiero peruano es uno de los más sólidos de la región. Según datos de la SBS y del BCRP, algunas entidades bancarias superan los 12 mil millones de soles en patrimonio neto, manejando millones de operaciones digitales cada mes. Este nivel de criticidad operativa hace que el sector esté expuesto a riesgos cibernéticos de alto impacto.

Desde 2021, la Superintendencia de Banca, Seguros y AFP (SBS) ha fortalecido su marco regulatorio en materia de ciberseguridad con la emisión de la Resolución SBS N.° 5049-2021, que obliga a las entidades financieras a establecer políticas de gestión de seguridad de la información, identificar activos críticos, y reportar incidentes relevantes (Superintendencia de Banca, Seguros y AFP, 2021).

No obstante, la normativa no incluye aún un enfoque explícito sobre ciberresiliencia ni establece requerimientos detallados para la protección del Directorio Activo, lo que genera una brecha significativa en la preparación frente a amenazas avanzadas. Asimismo, no se hace referencia directa a marcos como: DORA, NIST CSF v2.0, ISO/IEC 27001:2022 e ISO/IEC 22301: 2019.

En este contexto, el presente estudio se alinea con una necesidad creciente: dotar al sector financiero peruano de herramientas y modelos técnicos que permitan enfrentar ciberataques con mayor preparación, respuesta y capacidad de recuperación.

El avance digital del Perú se aceleró significativamente durante la pandemia del COVID-19, al igual que en muchos otros países de América Latina. Empresas e instituciones públicas se vieron obligadas a migrar rápidamente hacia modelos digitales con el fin de garantizar la continuidad de sus operaciones. No obstante, esta adopción tecnológica acelerada dejó al descubierto múltiples vulnerabilidades estructurales. En este contexto, la ciberresiliencia, entendida como la capacidad para anticiparse, resistir, recuperarse y adaptarse a incidentes cibernéticos, se posicionó como una prioridad emergente.

Las brechas en ciberseguridad son especialmente evidentes en los sectores con menor madurez digital. Según un informe de Microsoft del año 2022, en América Latina sólo el 41% de las pequeñas y medianas empresas (pymes) invierte en soluciones básicas de ciberseguridad, y en el caso del Perú, esta cifra es incluso menor (Microsoft, 2022). Las Pymes representan el 99.5% del total de empresas del País y generan más del 60% del empleo, pero en su mayoría carecen de políticas de seguridad de la información, planes de continuidad operativa o personal especializado.

Industrias críticas como salud, energía, transporte y manufactura también presentan deficiencias significativas en ciberresiliencia. En el sector salud, por ejemplo, la implementación de historias clínicas

electrónicas y plataformas de atención remota ha sido fragmentada y desorganizada, lo que ha generado múltiples vectores de exposición a ciberataques. En 2023, el Ministerio de Salud fue víctima de un ciberataque que evidenció la falta de segmentación de redes, protocolos de respuesta y capacidades de monitoreo preventivo (Secretaría de Gobierno y Transformación Digital, 2023). De forma similar, en diciembre del mismo año, el Registro Nacional de Identificación y Estado Civil (RENIEC) sufrió un ataque cibernético que resultó en la filtración y posible venta de datos personales de millones de ciudadanos peruanos, incluyendo información sensible como nombres completos, números de DNI y direcciones (Gestión, 2025). Ambos incidentes revelan una preocupante exposición de los sistemas estatales y la necesidad urgente de fortalecer las defensas digitales del aparato público.

Ahora bien, si bien la legislación en ciberseguridad ha mostrado avances en los últimos años, persisten vacíos normativos, superposición de competencias y una escasa articulación entre entidades del sector público. En respuesta a estos desafíos, el Estado Peruano, a través de la Presidencia del Consejo de Ministros (PCM), ha establecido órganos con roles diferenciados pero complementarios: la Secretaría de Gobierno y Transformación Digital (SGTD) y el Centro Nacional de Seguridad Digital (CNSD) (Presidencia del Consejo de Ministros, 2025).

La SGTD es el órgano rector del gobierno digital en el país, y su misión es modernizar el Estado mediante el uso estratégico de tecnologías digitales, promoviendo una gestión pública más eficiente, transparente, segura y centrada en el ciudadano. Esta secretaría tiene competencia sobre las entidades públicas y lidera la implementación de normativas clave como la Ley de Gobierno Digital, promulgada mediante el Decreto Legislativo N.° 1412, y la Ley de Interoperabilidad Digital, aprobada mediante el Decreto de Urgencia N.° 006-2020 (Presidencia del Consejo de Ministros, 2025).

Por su parte, el CNSD actúa como el órgano especializado en ciberseguridad nacional, encargado de prevenir, detectar y coordinar la respuesta ante incidentes cibernéticos que puedan afectar la infraestructura crítica o comprometer la continuidad de servicios esenciales. Su función es principalmente operativa y técnica, y actúa como un ente articulador entre los CSIRT del Estado y del sector privado, priorizando la gestión integral de riesgos digitales a nivel estratégico y táctico (Presidencia del Consejo de Ministros, 2025).

3.3.2. Microentorno

En el ámbito interno de las entidades financieras de gran escala en Perú, se observa el uso extensivo de entornos híbridos que combinan infraestructura on-premises con servicios en la nube. En estos entornos, el Directorio Activo opera como núcleo de autenticación y control de accesos para aplicaciones financieras, recursos internos y conexiones remotas.

Las principales vulnerabilidades detectadas en este microentorno incluyen:

- Administración inadecuada de cuentas privilegiadas.
- Ausencia de segmentación entre dominios y zonas críticas.
- Falta de políticas de respaldo confiables y probadas frente a ataques al AD.
- Monitoreo reactivo o inexistente de eventos críticos del dominio.
- Mínima integración con Entra ID y nulo uso de herramientas como PIM, Sentinel o Defender for Identity.

El sector financiero, dada su importancia crítica para la estabilidad económica del país, es uno de los más avanzados en términos de ciberseguridad. Este sector opera bajo las regulaciones emitidas por la Superintendencia de Banca, Seguros y AFP (SBS), la cual ha desarrollado un marco normativo orientado a fortalecer la ciberresiliencia de las entidades supervisadas, tales como la Resolución SBS N.º 504-2021 y la Resolución SBS N.º 877-2020.

La Resolución SBS N.º 504-2021, emitida en 2021, aprueba el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, el cual establece la obligación de implementar un Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C) (Superintendencia de Banca, Seguros y AFP, 2021). Este sistema debe incluir políticas, procesos, procedimientos y responsabilidades claramente definidos, y estar alineado con estándares internacionales como la ISO/IEC 27001 y el marco del NIST. Además, el SGSI-C debe ajustarse al tamaño, naturaleza y complejidad de cada entidad y estar orientado a garantizar los principios de confidencialidad, integridad y disponibilidad de la información.

El Reglamento también contempla la implementación de un Programa de Ciberseguridad (PG-C), enfocado en la identificación, protección, detección, respuesta y recuperación frente a incidentes, así como en el aprendizaje continuo a partir de estos eventos (Superintendencia de Banca, Seguros y AFP, 2021).

Asimismo, entre sus disposiciones más relevantes, se incluyen medidas específicas para fortalecer los controles de acceso, la gestión de incidentes, la seguridad en entornos de computación en la nube y la supervisión de servicios contratados a terceros. En este último caso, se exige a las entidades realizar evaluaciones de riesgo, establecer cláusulas contractuales precisas y verificar el cumplimiento de certificaciones internacionales como ISO/IEC 27017, ISO/IEC 27018 y SOC 2 Tipo 2, especialmente cuando los servicios se presten desde el extranjero (Superintendencia de Banca, Seguros y AFP, 2021).

Asimismo, el Reglamento estipula aspectos técnicos clave como el uso de Interfaces de Programación de Aplicaciones (API), la autenticación reforzada para operaciones en canales digitales, el enrolamiento seguro de usuarios y el monitoreo continuo de transacciones, con el fin de mitigar el riesgo de fraudes y accesos no autorizados (Superintendencia de Banca, Seguros y AFP, 2021).

La Resolución SBS N.º 877-2020 establece el Reglamento para la Gestión de la Continuidad del Negocio, con el objetivo de asegurar que las entidades financieras y previsionales puedan mantener o restablecer sus operaciones críticas ante eventos de interrupción. El reglamento exige la implementación de un Sistema de Gestión de la Continuidad del Negocio (SGCN) que contemple el análisis de impacto, diseño de estrategias, planes de respuesta, pruebas periódicas, capacitación y mejora continua. Precisa que SGCN debe ser proporcional al tamaño y complejidad de cada entidad (Superintendencia de Banca, Seguros y AFP, 2020).

También establece el reporte oportuno de interrupciones significativas a la SBS y el monitoreo mediante indicadores trimestrales. Además, impone requisitos adicionales como redundancia tecnológica, canales alternativos de comunicación y mayor resiliencia operativa (Superintendencia de Banca, Seguros y AFP, 2020).

A pesar del marco normativo avanzado, el sector financiero peruano enfrenta amenazas cibernéticas cada vez más complejas, como fraudes digitales, suplantación de identidad y ataques a infraestructuras críticas. Además, persiste una desigualdad en la madurez cibernética entre los grandes bancos y entidades más pequeñas como cajas y cooperativas, que enfrentan limitaciones técnicas y presupuestarias. Esta brecha representa un riesgo sistémico, ya que la debilidad de un solo actor puede afectar la resiliencia de todo el ecosistema financiero.

4. Metodología de Investigación

Este capítulo detalla el enfoque metodológico seguido para desarrollar esta investigación, desde el diseño del estudio hasta las herramientas empleadas para recolectar y analizar la información. El objetivo es sustentar con claridad cómo se abordó la problemática planteada y de qué manera se validó el modelo de gestión de ciberresiliencia propuesto para proteger el Directorio Activo en una entidad financiera peruana.

4.1. Diseño de Investigación

El presente estudio tiene un tipo de investigación aplicada, ya que busca ofrecer una solución concreta a una necesidad real en el sector financiero: la falta de un modelo específico de ciberresiliencia frente a ataques al Directorio Activo. Más allá de generar teoría, esta investigación pretende diseñar una herramienta práctica que pueda ser usada por profesionales del sector para elevar sus niveles de preparación ante amenazas cibernéticas.

El nivel de investigación es descriptivo y propositivo. Por un lado, se describe el estado actual de la seguridad del Directorio Activo en entornos financieros peruanos, identificando vulnerabilidades, amenazas y brechas. Por otro lado, se propone un modelo de gestión fundamentado en estándares internacionales, buenas prácticas y requerimientos adaptados al contexto local.

Respecto al diseño metodológico, se optó por un enfoque no experimental y transversal, ya que no se manipulan variables directamente y el análisis se realiza sobre una situación existente, en un momento determinado. El estudio adopta un enfoque mixto, combinando herramientas cualitativas y cuantitativas, lo que permite tener una visión más completa del problema y de las soluciones posibles.

4.2. Muestreos

La investigación utilizó un muestreo intencional, seleccionando de forma deliberada a mínimo cinco expertos con experiencia comprobada en el sector financiero, gestión de Directorio Activo, incidentes cibernéticos y cumplimiento normativo. Este tipo de muestreo es adecuado para estudios donde se requiere una comprensión profunda y especializada del fenómeno estudiado.

Los criterios de inclusión considerados fueron:

- Experiencia laboral mínima de 5 años en áreas de ciberseguridad o TI bancaria.
- Participación en la gestión o mitigación de incidentes de seguridad.
- Conocimiento o gestión directa del Directorio Activo o su integración con soluciones híbridas.

4.3. Instrumentos de Medición

4.3.1. Análisis Documental

Se revisaron y analizaron documentos oficiales relacionados con normativas y marcos internacionales de ciberresiliencia, tales como: DORA, NIST CSF v2.0, ISO/IEC 27001:2022 e ISO/IEC 22301: 2019, así como guías técnicas de Microsoft sobre la seguridad del Directorio Activo y su integración con Entra ID. Esta revisión documental fue clave para construir el marco conceptual y para sustentar el diseño del modelo.

Para sistematizar esta etapa, se emplearon fichas de análisis documental, que permitieron extraer los elementos más relevantes de cada estándar, ley o guía técnica. Estas fichas facilitaron la comparación entre enfoques, así como la identificación de prácticas adaptables al entorno financiero peruano.

4.3.2. Entrevistas a Expertos

Como parte de la recolección de información cualitativa, se realizaron entrevistas semiestructuradas a profesionales especializados en ciberseguridad, operaciones TI y cumplimiento normativo del sector financiero. Las entrevistas tuvieron como propósito conocer la experiencia directa de estos expertos frente a incidentes que involucren el AD, así como sus percepciones sobre la resiliencia institucional actual.

Las preguntas se agruparon en torno a los siguientes ejes:

- Conocimientos sobre ataques reales al AD y su impacto.
- Evaluación del nivel de preparación institucional.
- Opinión sobre los controles técnicos y organizativos vigentes.
- Perspectivas sobre la utilidad de un modelo de ciberresiliencia.

4.3.3. Lista de Cotejo Técnica

Se elaboró una lista de verificación técnica para evaluar el grado de implementación de controles clave en entornos con AD, como:

- Uso de autenticación multifactor (MFA).
- Existencia de backups del AD y frecuencia de pruebas de restauración.
- Gestión de accesos privilegiados (PAM).
- Monitorización de eventos críticos.
- Segmentación de identidades y servicios.

Este instrumento sirvió como guía para identificar brechas y contrastarlas con las mejores prácticas descritas en el marco conceptual.

4.3.4. Matriz de Evaluación de Brechas

A partir del análisis anterior, se construyó una matriz de brechas que permitió contrastar la situación actual observada con el nivel de madurez esperado según estándares internacionales. Esta matriz orientó la propuesta del modelo y ayudó a definir prioridades en la arquitectura de resiliencia.

4.3.5. Cuestionario de Diagnóstico de Ciberresiliencia

Se diseñó un cuestionario dirigido a los responsables de seguridad y tecnología de la entidad financiera evaluada, con preguntas que permiten medir el nivel de madurez institucional en temas como:

- Prevención y protección del AD.
- Capacidades de respuesta a incidentes.
- Planes de recuperación ante desastres.
- Integración con herramientas modernas como Sentinel o Entra ID.

Este cuestionario también servirá para validar, en una siguiente fase, la efectividad del modelo diseñado.

4.4. Técnicas y Procedimientos

Para el tratamiento de la información recolectada, se aplicaron técnicas de análisis mixto, tanto cualitativo como cuantitativo:

- **Análisis cualitativo:** La información obtenida mediante entrevistas y análisis documental fue codificada y categorizada temáticamente. Se

identificaron patrones, convergencias y percepciones clave que aportaron profundidad al entendimiento del contexto institucional y de los riesgos asociados al AD.

- **Análisis cuantitativo:** Los datos obtenidos a partir de la lista de cotejo y del cuestionario fueron tabulados y analizados estadísticamente. Se calcularon niveles de cumplimiento por cada control evaluado, lo que permitió elaborar un diagnóstico del estado actual de la resiliencia en la entidad financiera.
- **Contraste con estándares y buenas prácticas:** Los hallazgos fueron confrontados con estándares internacionales y con los pilares del modelo propuesto, permitiendo ajustar su diseño, asegurar su aplicabilidad y garantizar su relevancia para el entorno financiero local.

5. Análisis de Resultados

Este capítulo presenta y analiza los hallazgos obtenidos a partir de la aplicación del cuestionario de diagnóstico de ciberresiliencia, entrevistas a expertos y revisión técnica de controles en el entorno del Directorio Activo (AD) de una entidad financiera peruana. El objetivo es identificar brechas, patrones y niveles de madurez en la gestión de la ciberresiliencia, con énfasis en la capacidad de la organización para anticiparse, resistir y recuperarse de un ataque dirigido al AD.

5.1. Resultados Cualitativos

Las entrevistas realizadas a especialistas en ciberseguridad, operaciones TI y cumplimiento normativo revelaron varios hallazgos relevantes que ayudan a comprender el estado real de la ciberresiliencia en el entorno financiero nacional:

- **Falta de conciencia sobre la criticidad del AD:** Muchos responsables de seguridad reconocen que, aunque el AD es el corazón de la infraestructura tecnológica, su protección no siempre es priorizada al nivel que merece.
- **Controles aplicados de forma parcial:** Existen políticas de respaldo y monitoreo, pero no se aplican de manera uniforme ni se validan periódicamente. Esto genera una falsa sensación de seguridad.

- **Baja cultura de prueba y simulación:** Prácticamente ninguno de los entrevistados había participado en simulacros reales que incluyan escenarios de compromiso del AD, lo cual representa un riesgo latente frente a ataques reales.
- **Desconocimiento o subutilización de herramientas avanzadas:** Tecnologías como Microsoft Sentinel, Defender for Identity o PIM están disponibles, pero no son ampliamente usadas ni configuradas adecuadamente.

Estas percepciones reforzaron la necesidad de contar con un modelo específico de ciberresiliencia que brinde claridad, orientación y mecanismos de evaluación continua.

5.2. Resultados Cuantitativos

Con base en la aplicación del cuestionario de diagnóstico de ciberresiliencia a responsables técnicos de una entidad financiera, se obtuvo en la siguiente Tabla 2, la puntuación promedio por bloque temático (sobre un máximo de 5 puntos):

Tabla *2*

Resultados obtenidos de las encuestas

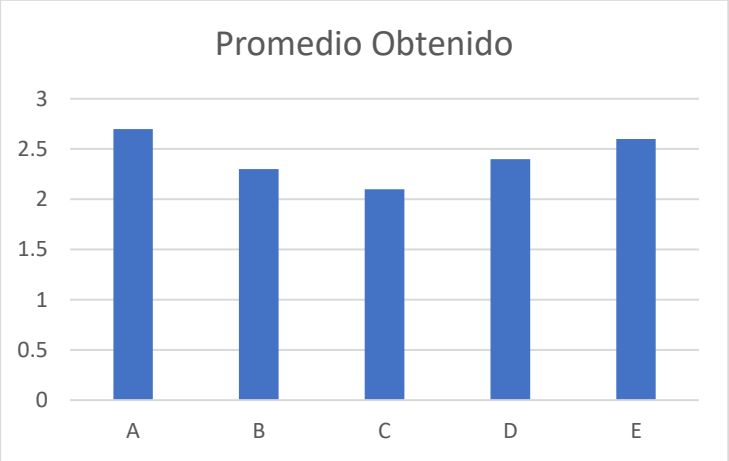
Bloque	Tema Evaluado	Promedio Obtenido
A	Controles técnicos sobre el AD	2.7
B	Gestión de identidades privilegiadas	2.3
C	Detección y respuesta a incidentes	2.1
D	Recuperación y continuidad	2.4
E	Cumplimiento normativo y gobierno	2.6

Nota. Elaboración propia

Estos resultados revelan un nivel de madurez medio-bajo, con mayor debilidad en la respuesta a incidentes y la gestión de privilegios, dos aspectos clave para mitigar el impacto de ataques dirigidos al AD.

Figura *3*

Gráfico de barras de los resultados obtenidos de las encuestas



Nota. Fuente Elaboración propia

Principales observaciones:

- Aunque se cuenta con medidas básicas de protección (como backups y monitoreo limitado), no se han implementado soluciones PAM ni se realiza segmentación de identidades sensibles.
- El MFA no está activado para todos los roles administrativos, lo cual representa una exposición directa ante ataques como: credential stuffing o pass-the-hash.
- Las pruebas de restauración del AD no se ejecutan de forma sistemática, y los planes de recuperación no contemplan escenarios de ransomware o corrupción del dominio.
- No se aplica ningún marco normativo de forma estructurada (NIST, DORA, ISO), aunque se reconoció su importancia y algunos elementos están parcialmente adoptados.

5.3. Análisis de Brechas

A partir de los resultados obtenidos y de la comparación con estándares internacionales, se construyó una matriz de brechas en la Tabla 3, que identifica los puntos críticos que deberán ser abordados por el modelo propuesto:

Tabla 3

Matriz de Brechas

Dimensión Evaluada	Estado Actual	Recomendación según estándares (NIST, DORA, ISO)	Brecha Identificada
MFA para cuentas privilegiadas	Parcialmente implementado	Obligatorio y aplicado por riesgo	Alta
PAM	No implementado	Recomendado en Zero Trust y NIST	Crítica
Monitoreo del AD	Básico	Automatizado y en tiempo real	Moderada
Backups del AD	Realizados pero no probados	Deben probarse regularmente	Alta
Segmentación de accesos	No existe	Segmentación lógica y física	Crítica
Plan de recuperación específico del AD	No documentado	Requerido (DORA, ISO 22301)	Alta

Nota. Elaboración propia

El análisis confirma que existe una brecha significativa entre el estado actual de la organización y el nivel de ciberresiliencia deseado. Si bien existen esfuerzos aislados y buena disposición por parte del equipo técnico, no hay un modelo estructurado que guíe la preparación, respuesta y recuperación frente a ataques al AD.

Este diagnóstico justifica y da fundamento a la siguiente fase de esta tesis: el diseño de un modelo de gestión de ciberresiliencia específico, contextualizado al entorno peruano, que integre controles técnicos, normativos y estratégicos.

6. Plan de Acción

6.1. Propuesta de Modelo de Gestión de Ciberresiliencia

A partir del diagnóstico realizado en los capítulos anteriores y considerando las buenas prácticas internacionales, se plantea un modelo de gestión especialmente diseñado para fortalecer la capacidad de una entidad financiera peruana frente a ataques dirigidos al Directorio Activo (AD). Esta propuesta de la Figura 4, busca ser práctica, contextualizada y adaptable, teniendo en cuenta tanto las condiciones reales de operación como las regulaciones y tecnologías disponibles. También especificamos un Esquema del Modelo de Gestión de Ciberresiliencia en el Anexo D.

Figura 4

Propuesta de Modelo de Gestión de Ciberresiliencia

Nota. Elaboración propia

6.1.1. Fundamentos del Modelo

El modelo parte de una premisa básica pero fundamental: la ciberresiliencia no puede depender únicamente de la tecnología, sino que debe ser gestionada como un proceso continuo que integra personas, procesos y herramientas. Por ello, se construye sobre cuatro pilares que interactúan entre sí:

- **Prevención:** evitar que los ataques lleguen a comprometer el AD.
- **Detección:** identificar de forma temprana cualquier actividad anómala o intrusión.
- **Respuesta:** actuar de manera rápida y coordinada cuando ocurre un incidente.
- **Recuperación:** restaurar los servicios afectados sin pérdida significativa de datos o reputación.

Estos pilares están alineados con los marcos NIST CSF, DORA e ISO/IEC 27001, y se traducen en prácticas concretas distribuidas a lo largo del modelo propuesto.

6.1.2. Arquitectura Técnica del Modelo

La arquitectura que se plantea no pretende reemplazar la infraestructura existente, sino complementarla y reforzarla con capas adicionales de control y resiliencia. A continuación, se detallan los componentes clave del diseño técnico:

a) Autenticación fuerte y segmentación

Se propone la implementación obligatoria de autenticación multifactor (MFA), sobre todo para cuentas administrativas y de alto riesgo. Asimismo, se sugiere dividir el entorno dl AD en zonas lógicas o unidades organizativas (OU) con diferentes niveles de control y visibilidad, reduciendo así el impacto en caso de una intrusión.

b) Gestión de accesos privilegiados (PAM)

Un aspecto esencial del modelo es el uso de soluciones de gestión de accesos privilegiados (PAM), como la integrada en Microsoft

Entra ID. Estas herramientas permiten limitar el tiempo, alcance y condiciones bajo las cuales un usuario puede tener privilegios elevados. También se propone establecer cuentas temporales y eliminar privilegios persistentes, reduciendo así el riesgo de escalamiento lateral.

c) **Monitoreo en tiempo real con IA**

Se recomienda integrar soluciones como Microsoft Sentinel y Defender for Identity, que permiten observar en tiempo real lo que ocurre dentro del AD. Estas herramientas hacen uso de inteligencia artificial y aprendizaje automático para detectar patrones anómalos y generar alertas automáticas. Con esto se busca reducir el tiempo entre la intrusión y la detección.

d) **Copias de seguridad robustas y verificadas**

El modelo contempla la creación de backups automáticos y cifrados del AD, almacenados fuera del dominio principal y probados de forma regular. La frecuencia de verificación debe ser mensual, y se sugiere contar con un procedimiento documentado de recuperación paso a paso, para garantizar que el restablecimiento del servicio pueda realizarse bajo presión y sin improvisación.

e) **Recuperación ante desastres**

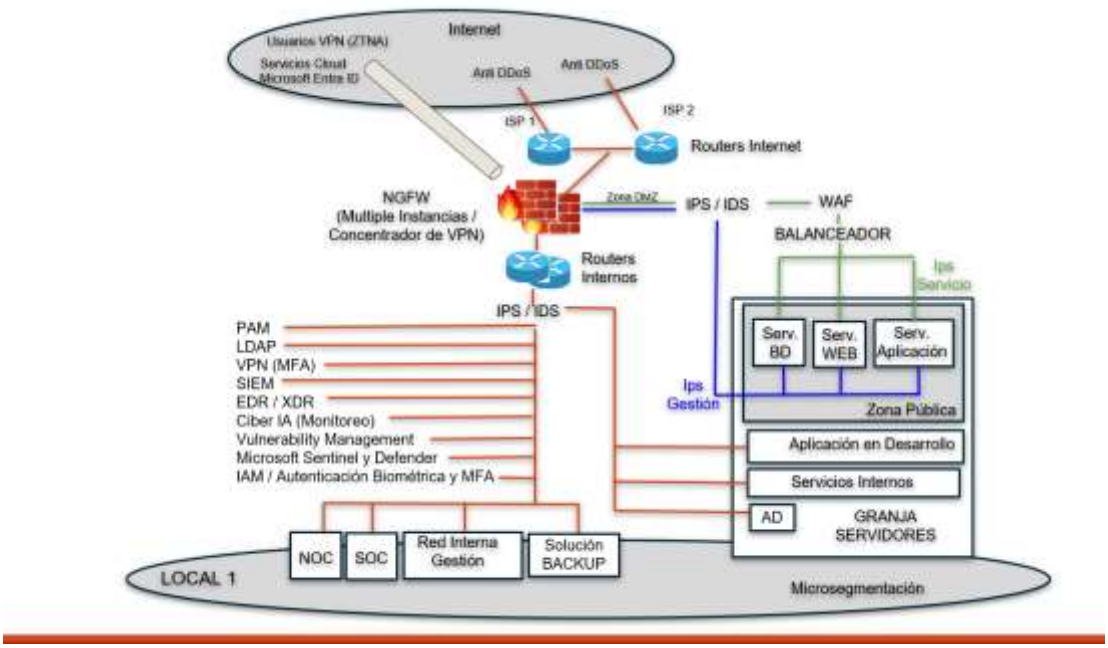
Dentro del modelo, la recuperación no se limita a restaurar datos, sino que incluye la reconstrucción del dominio en condiciones seguras. Se incorpora un plan de continuidad que contempla escenarios extremos como ransomware o destrucción intencionada del AD. Además, se establece una matriz de prioridades de servicios críticos que deben restablecerse de manera escalonada.

f) **Zero Trust y reducción de superficie de ataque**

El modelo adopta el enfoque de confianza cero (Zero Trust), en el cual ningún usuario o sistema es confiable por defecto. Toda acción sensible requiere verificación, validación contextual (por ejemplo, ubicación geográfica, hora, dispositivo) y registro. También se plantea minimizar la cantidad de servicios corriendo en el mismo dominio del AD, así como limitar la visibilidad entre redes internas.

Figura 5

Diagrama de Arquitectura Técnica del Modelo



Nota. Elaboración propia

6.1.3. Fases del Modelo

El modelo se despliega en cinco etapas prácticas y secuenciales que permiten una adopción ordenada:

a) Evaluación Inicial

- Aplicación del cuestionario de ciberresiliencia.
- Auditoría técnica del entorno AD actual.
- Identificación de brechas respecto a estándares internacionales.

b) Diseño y planificación

- Priorización de acciones según criticidad.
- Asignación de responsables y definición de plazos.
- Validación con el área de cumplimiento normativo.

c) Implementación técnica

- Activación de MFA, PAM, Sentinel, y segmentación de privilegios.
- Pruebas piloto en entornos controlados.

- Capacitación a los equipos técnicos y administrativos.

d) Pruebas y simulacros

- Simulación de incidentes (ransomware, secuestro de AD, etc.).
- Prueba de restauración a partir de copias de seguridad.
- Validación de alertas y respuesta automatizada.

e) Evaluación continua

- Reaplicación del cuestionario.
- Análisis de métricas de tiempo de respuesta y recuperación.
- Revisión del plan de continuidad y actualización del modelo.

6.1.4. Integración con AD y Entra ID

El modelo está diseñado para entornos híbridos, donde conviven AD tradicional (on-premise) y Microsoft Entra ID. Esta combinación permite fortalecer la seguridad sin necesidad de migrar completamente a la nube. Entre los beneficios de esta integración destacan:

- Control centralizado de identidades.
- Condiciones de acceso basadas en riesgo.
- Activación de funciones como Privileged Identity Management (PIM).
- Auditoría unificada y protección reforzada ante actividades sospechosas.

6.1.5. Indicadores de Madurez y Seguimiento

Para medir el avance y efectividad del modelo, se proponen los siguientes indicadores detallados en la Tabla 4:

Tabla 4

Indicadores de Madurez y Seguimiento

Indicador	Descripción	Frecuencia
Nivel promedio de cumplimiento del cuestionario	Promedio por bloque (de 1 a 5)	Trimestral
Tiempo medio de detección de incidentes	Desde la intrusión hasta la alerta	Mensual
Tiempo de recuperación del AD	Desde la caída hasta el restablecimiento total	Trimestral
Porcentaje de cuentas administrativas con MFA activo	Evaluación de cumplimiento técnico	Mensual
Número de accesos privilegiados temporales vs permanentes	Gestión de privilegios	Mensual

Nota. Elaboración propia

Estos indicadores permiten realizar ajustes periódicos al modelo, manteniendo su efectividad frente a amenazas nuevas o cambios tecnológicos.

Este modelo de gestión de ciberresiliencia no solo cubre los aspectos técnicos del Directorio Activo, sino que los articula con procesos de recuperación, cumplimiento normativo, y monitoreo continuo. Su adopción progresiva permite mejorar la preparación institucional sin exigir cambios disruptivos. Además, al estar basado en estándares reconocidos y experiencias reales, puede ser replicado por otras entidades del sector financiero en Perú o incluso adaptado a otros sectores críticos.

6.2. Plan de Implementación y Evaluación

Este capítulo describe cómo se puede llevar a la práctica el modelo de ciberresiliencia propuesto en el capítulo anterior. No basta con tener un buen diseño técnico; es igualmente importante contar con una estrategia clara de implementación que defina tiempos, responsabilidades, recursos necesarios y mecanismos para evaluar su efectividad. A lo largo de este capítulo se plantean un cronograma tentativo, un presupuesto estimado, los costos asociados a cada componente y una serie de métricas clave para monitorear su funcionamiento.

6.2.1. Cronograma Propuesto

La implementación del modelo se plantea en cinco fases, distribuidas en un período estimado de seis meses, aunque este plazo puede ajustarse de acuerdo con los recursos y la madurez tecnológica de cada institución, la cual describimos en la Tabla 5.

Tabla 5

Cronograma propuesto

Fase	Actividades principales	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6
Fase 1	Diagnóstico inicial y análisis de brechas	●	●				
Fase 2	Diseño detallado y planificación de acciones		●	●			
Fase 3	Implementación de controles técnicos (MFA, PAM, backups)			●	●		
Fase 4	Ejecución de simulacros y pruebas de restauración				●	●	
Fase 5	Revisión, ajustes y evaluación continua					●	●

Nota. Elaboración propia

Cada fase contempla tanto tareas técnicas como aspectos organizativos (capacitación, reuniones de coordinación, validación con las áreas legales o de auditoría interna).

6.2.2. Simulación de Presupuesto

Para facilitar la toma de decisiones, en la Tabla 6, Tabla 7, Tabla 8 y Tabla 9, se ha preparado una estimación de costos aproximada para la implementación del modelo en una organización con aproximadamente 5,000 usuarios gestionados a través de AD y Entra ID. Los valores son referenciales y pueden variar según acuerdos de licenciamiento, uso de servicios propios o de terceros, y tipo de infraestructura (híbrida, local o 100% nube).

a. Licenciamiento

Tabla 6

Costos Estimados de los Componentes

Componente	Descripción	Costo estimado (anual)
Microsoft Entra ID P2	Para MFA, PIM, auditoría avanzada	USD 9 por usuario x 5,000 = USD 45,000
Microsoft Sentinel	Licencia base + almacenamiento logs (estimado 50 GB/día)	USD 10,000
Windows Server CALs	Licencias de acceso al servidor AD	USD 20,000

Nota. Elaboración propia

b. Seguridad y gestión de privilegios

Tabla *7*

Costos Estimados de los Componentes

Componente	Descripción	Costo estimado
PAM de Microsoft (incluido en Entra ID P2)	Gestión de privilegios temporales	Incluido
Hardening y monitoreo con Defender for Identity	Sensor de detección AD	USD 8,000

Nota. Elaboración propia

c. Respaldo y recuperación

Tabla 8

Costos Estimados de los Componentes

Componente	Descripción	Costo estimado
Software de backup del AD (p. ej. Veeam, Azure Backup)	Licencia + almacenamiento	USD 5,000
Pruebas de recuperación documentadas	Recursos técnicos internos	USD 3,000 (estimado en HH)

Nota. Elaboración propia

d. Servicios y formación

Tabla 9

Costos Estimados de los Componentes

Componente	Descripción	Costo estimado
Servicios profesionales para configuración y pruebas	Partner especializado Microsoft	USD 12,000
Capacitaciones para personal técnico y administradores	Talleres internos y externos	USD 5,000

Nota. Elaboración propia

Total estimado inicial: **USD 108,000 anuales** (aproximado para un entorno de 5,000 usuarios)

Este presupuesto puede optimizarse si la organización ya dispone de licencias, equipos internos capacitados o herramientas equivalentes.

También detallamos en la Tabla 10, el Mapa de Riesgo Cuantitativo de Ciberresilencia en AD y Entra ID.

e. Costos

Considerando un escenario de interrupción continua de 24 horas, que abarca desde las 08:00 horas del primer día hasta las 08:00 horas del día siguiente, hemos establecido las siguientes premisas para analizar las pérdidas económicas:

- Pérdidas directas por ingresos diarios en el producto Banca Minorista: S/ 13,000,000
- Pérdidas directas por ingresos diarios en el producto de Banca Mayorista: S/ 20,000,000
- Pérdidas directas por ingresos diarios en el producto relacionado a la indisponibilidad de líneas de crédito y préstamos a personas naturales: S/ 20,000,000
- **Multa del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI):** La multa máxima impuesta previamente por el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) por eventos similares, y a instituciones del mismo sector, ha sido de 45 UIT. Por lo tanto, tomamos este valor como referencia. Cabe destacar que, el costo de una UTI en el año 2025 asciende a S/ 5,350 en consecuencia, los costos equivalen a 45*S/ 5,350 = S/ 240,750
- **Multa de la Superintendencia de Banca y Seguros (SBS):** La SBS califica las infracciones graves con multas que van desde

20 hasta 100 UITs. Para este caso de estudio, estamos utilizando el valor máximo, 100 UITs, debido a la relevancia de la entidad y la naturaleza del evento. En consecuencia, los costos equivalen a 100*S/ 5,350 = S/ 535,000

- **Autoridad Nacional de Protección de Datos Personales (ANPD):** La multa máxima impuesta previamente por la ANPD por eventos similares, y a instituciones del mismo sector, ha sido de 63 UIT. Por lo tanto, tomamos este valor como referencia, en consecuencia los costos equivalen a 63*S/ 5,350 = S/ 337,050
- **Reclamos y Devoluciones**: Considerando que aproximadamente 80,000 clientes realizan operaciones diarias con un promedio de S/ 500, se estima que todos ellos reclamarán la devolución de su dinero. Asumiendo que se fallará a favor del cliente en todos los casos procediendo con el reembolso total, los costos ascenderían a 80,000*S/ 500 = S/ 40,000,000
- Según el informe "Data Breach" de IBM del 2024, el costo promedio global de una filtración de datos fue de $4.88 millones de dólares. Para este caso de estudio, se asume que el incidente implica la pérdida de información confidencial y datos personales de clientes. Considerando un tipo de cambio de S/ 3.54 por dólar, se estima un costo equivalente a $4,880,000*S/ 3.54 = S/ 17,275,200

Tabla 10

Mapa de Riesgo Cuantitativo de Ciberresilencia en AD y Entra ID

Costo Asociado	Monto
Banca Minorista	S/ 13,000,000
Banca Mayorista	S/ 20,000,000
Personas Naturales	S/ 20,000,000

Multa INDECOPI	S/ 240,750
Multa SBS	S/ 535,000
Multa ANPD	S/ 337,050
Reclamos y Devoluciones	S/ 40,000,000
Costo de Brecha Datos	S/ 17,275,200
TOTAL	**S/ 111,388,000** **USD 31,465,536**

Nota. Elaboración propia

Justificación de Inversión:

El Retorno de Inversión en Seguridad (ROSI), se calcula de acuerdo a:

$$\text{ROSI} = \frac{(\text{ALE} * \text{Tasa de Mitigación}) - \text{Costo de la Inversión}}{\text{Costo de la Inversión}} \; x100$$

Donde:

- **Pérdida Anual (ALE)**: Es el costo financiero total esperado de los incidentes de seguridad si no se realiza la inversión.

  Se calcula multiplicando la Expectativa de Pérdida Única (SLE) por la Tasa Anual de Ocurrencia (ARO).

  - Expectativa de Pérdida Única (SLE): Costo monetario de un sólo incidente de seguridad.
  - Tasa Anual de Ocurrencia (ARO): Probabilidad de que un tipo específico de incidente de seguridad ocurra en un año.

  ALE =SLE * ARO

- **Tasa de Mitigación:** Porcentaje en que la inversión en seguridad reduce la pérdida anual (ALE).

- **Costo de la Inversión:** Costo total de implementar o mantener la solución de seguridad durante un período de tiempo.

Por tanto, el ROSI del siguiente trabajo de investigación es:

- Expectativa de Pérdida Única (SLE): USD 31,465,536
- Tasa Anual de Ocurrencia (ARO): 1
- Tasa de Mitigación: 80%
- Costo de Inversión: USD 108,000 anuales

⇨ ALE = USD 31,465,536 * 1= USD 31,465,536

$$\text{ROSI} = \frac{(\text{USD } 31{,}465{,}536 * 80\%) - \text{USD } 108{,}000}{\text{USD } 108{,}000} \; x100$$

ROSI ≈ 23,207.80 %

Este mapa ofrece evidencia cuantificable que el modelo no solo es técnicamente robusto, sino también financieramente racional.

6.2.3. Métricas de Evaluación del Modelo

Para garantizar que el modelo no solo se implemente, sino que realmente funcione, es necesario definir indicadores claros que permitan hacer seguimiento y ajustes. A continuación, en la Tabla 12, se proponen algunos:

Tabla 11

Indicadores de Seguimiento

Indicador	Qué mide	Frecuencia de revisión	Bench mark	Apetito Riesgo
Tiempo promedio de detección de incidentes en el AD	Eficacia del monitoreo	Mensual	≤5 minutos	≤10 minutos
Porcentaje de cuentas administrativas con MFA habilitado	Nivel de protección de accesos críticos	Mensual	100%	≥ 95%
Cantidad de accesos privilegiados temporales vs. permanentes	Madurez en gestión de privilegios	Trimestral	≥ 90%	≥ 85%
Tiempo promedio de recuperación del AD tras un incidente simulado	Eficiencia del plan de recuperación	Trimestral	≤4 horas	≤ 8 horas
Nivel de cumplimiento del cuestionario de diagnóstico	Evolución de la madurez organizacional	Semestral	≥ 85%	≥ 80%

Nota. Elaboración propia

El apetito de riesgo y el nivel de exposición que la organización está dispuesta a aceptar han sido definidos tomando como referencia estándares internacionales,

tales como el NIST CSF v2, ISO/IEC 22301, la Ley DORA, el enfoque Zero Trust, entre otros.

Asimismo, estas métricas pueden servir como insumo para auditorías, reportes de cumplimiento o decisiones estratégicas en el comité de riesgos de la organización.

Este plan busca demostrar que el modelo propuesto no solo es técnicamente viable, sino también económicamente razonable y organizativamente alcanzable. Al plantear fases claras, herramientas disponibles y formas de medir su impacto, se establece una hoja de ruta que puede ser seguida y ajustada según la realidad de cada entidad. La combinación de un enfoque estructurado y adaptable permitirá avanzar hacia una ciberresiliencia efectiva y sostenible en el tiempo.

7. Discusión

Este capítulo tiene como propósito reflexionar críticamente sobre los resultados alcanzados a lo largo de la investigación, valorar las implicancias del modelo propuesto y considerar tanto los logros como las limitaciones del trabajo realizado. Además, se exploran posibilidades de mejora continua y nuevos caminos de estudio que podrían complementar o fortalecer los hallazgos.

7.1. Implicancias

La elaboración de un modelo de ciberresiliencia orientado específicamente al Directorio Activo en una entidad financiera peruana de gran escala supone un aporte concreto, tanto técnico como estratégico. No se trata solo de una guía de buenas prácticas, sino de un marco aplicable, evaluable y adaptable a distintas realidades institucionales.

Uno de los hallazgos más relevantes del estudio es la existencia de una desconexión entre la seguridad declarada y la ciberresiliencia real. Aunque muchas entidades financieras cuentan con políticas de seguridad y herramientas tecnológicas, en la práctica, estas no siempre están bien integradas, actualizadas o alineadas con estándares internacionales como NIST CSF, DORA o ISO/IEC 27001.

La investigación también muestra que el Directorio Activo sigue siendo una infraestructura altamente vulnerable cuando no se aplica una estrategia específica de protección, monitoreo y recuperación. Este hallazgo refuerza la importancia de tratar al AD no como un simple componente técnico más, sino como un activo estratégico cuya caída o compromiso puede paralizar una organización entera.

En términos más amplios, la propuesta de un modelo escalable y estructurado podría servir como referencia para otros sectores críticos, como el de telecomunicaciones, energía o salud, que comparten desafíos similares en cuanto al manejo de identidades digitales y continuidad operativa.

7.2. Limitaciones del estudio

Si bien el modelo presentado se construyó sobre una base sólida de revisión técnica, entrevistas y estándares reconocidos, es importante reconocer sus alcances y limitaciones:

- **Enfoque centrado en una sola entidad:** La validación se realizó con expertos de un entorno financiero específico. Si bien esto aporta profundidad, limita la generalización inmediata a otros sectores sin ajustes previos.
- **Condicionamientos presupuestales:** El modelo incluye herramientas como Microsoft Sentinel o Entra ID P2, que requieren inversión. No todas las organizaciones pueden implementar de inmediato la versión completa del modelo si no cuentan con presupuesto o acuerdos corporativos.
- **Ejecución simulada, no real:** Debido al carácter académico del estudio, algunas fases del modelo (como simulacros de restauración o pruebas con ransomware) se plantearon en papel o a través de entrevistas, pero no fueron ejecutadas en entornos productivos, lo que deja espacio para ajustar ciertas propuestas en una implementación real.
- **Cambios tecnológicos constantes:** Dado el ritmo vertiginoso con el que evoluciona la tecnología y las amenazas cibernéticas, es probable que algunas herramientas o técnicas deban actualizarse o reemplazarse en un

futuro cercano. Esto exige que el modelo propuesto sea dinámico y esté abierto a revisión.

7.3. Agenda Futura

A partir de lo aprendido, se identifican varias oportunidades de profundización y mejora para estudios o implementaciones posteriores:

- **Implementación real y medición longitudinal:** Sería muy valioso aplicar el modelo completo en una organización durante un período prolongado y medir su evolución en tiempo real. Esto permitiría validar los beneficios del enfoque y ajustar variables técnicas o estratégicas con base en datos observables.
- **Integración de IA en la detección de amenazas:** Microsoft Sentinel, por ejemplo, ofrece funciones avanzadas de análisis basadas en inteligencia artificial. La exploración más profunda de estos algoritmos podría potenciar la capacidad predictiva y la detección temprana, algo que podría convertirse en una línea de investigación independiente.
- **Expansión del modelo a otros entornos críticos:** Tal como se mencionó antes, la lógica del modelo puede adaptarse a organizaciones públicas o privadas que manejen datos sensibles o servicios esenciales, más allá del sector financiero. Ajustar el modelo a entornos como educación, salud o energía podría generar aportes importantes para el país.
- **Automatización de métricas e informes de resiliencia:** Una futura línea de trabajo podría enfocarse en el desarrollo de dashboards automatizados que traduzcan los indicadores del modelo en gráficos y alertas, facilitando así el trabajo de los equipos de seguridad y la toma de decisiones ejecutivas.
- **Inclusión de normativas locales emergentes:** Si en los próximos años el Perú adopta formalmente normativas inspiradas en DORA o similares, será clave alinear el modelo propuesto con dichas regulaciones. Esta actualización garantizará su vigencia y utilidad a largo plazo.

La propuesta desarrollada en esta tesis demuestra que es posible diseñar e implementar un modelo realista, estructurado y técnicamente viable para fortalecer

la ciberresiliencia frente a ataques al Directorio Activo. Aunque existen limitaciones que deben reconocerse, los resultados sugieren que una gestión proactiva, estratégica y basada en estándares internacionales puede marcar la diferencia entre resistir un ataque y colapsar ante él.

Este modelo no es un punto final, sino un punto de partida para seguir fortaleciendo la seguridad digital de las instituciones más críticas del país.

8. Conclusiones y Recomendaciones

Este último capítulo reúne los principales aprendizajes de la investigación, sintetizando los hallazgos clave y destacando su valor tanto a nivel académico como práctico. Además, se presentan recomendaciones concretas dirigidas a distintos actores que podrían beneficiarse de la propuesta, como responsables de seguridad, tomadores de decisión institucional y futuros investigadores.

8.1. Conclusiones

El Directorio Activo sigue siendo un punto débil crítico en las organizaciones financieras A pesar de su rol esencial como columna vertebral en la gestión de usuarios, accesos y autenticación, el AD no siempre recibe la atención que merece en términos de protección. La investigación reveló que muchas de las prácticas implementadas son parciales, desactualizadas o dependen demasiado del conocimiento individual de técnicos sin una estrategia institucional consolidada.

La ciberresiliencia va más allá de la ciberseguridad tradicional. Una de las principales lecciones de este trabajo es que proteger un entorno no basta. Es necesario pensar en cómo resistir, cómo responder y cómo recuperarse cuando el ataque ya está en marcha o incluso ha tenido éxito. La ciberresiliencia incorpora una lógica de anticipación y adaptación continua, que no solo se apoya en tecnologías, sino también en procesos, personas y una cultura organizacional que valore la preparación.

Existe una brecha importante entre lo que indican los estándares internacionales y la realidad operativa local. Aunque normas como ISO/IEC 27001, DORA o el marco NIST CSF ofrecen directrices claras y validadas, su

adopción en las instituciones peruanas sigue siendo limitada o superficial. Esto genera vulnerabilidades que podrían evitarse con una mejor alineación entre lo técnico y lo normativo.

El modelo propuesto es viable, adaptable y necesario. El diseño presentado en esta tesis ha demostrado ser realista tanto desde el punto de vista técnico como económico. Su implementación no exige romper con la infraestructura existente, sino integrarse progresivamente a ella. Al ser modular y medible, puede ajustarse a distintas capacidades organizativas.

La medición del nivel de ciberresiliencia es clave para la mejora continua. A través del cuestionario y los indicadores definidos, se pudo comprobar que contar con herramientas de autoevaluación ayuda a visualizar claramente dónde se encuentran las debilidades, facilitando la toma de decisiones estratégicas para su corrección.

8.2. Recomendaciones

A partir de todo lo analizado, se proponen las siguientes acciones para asegurar que el modelo cumpla su propósito y pueda ser aprovechado al máximo:

Para las entidades financieras:

Adoptar el modelo de manera progresiva, comenzando por los elementos críticos como MFA, respaldo validado del AD y monitoreo en tiempo real. Posteriormente, avanzar hacia la automatización de privilegios y recuperación ante desastres.

No posponer las pruebas y simulacros. Es fundamental validar no solo que existen planes, sino que funcionan bajo presión. Hacer simulaciones de fallas en el AD es una forma segura de identificar fallos y corregirlos antes de que ocurra un incidente real.

Incluir la resiliencia digital en los planes de continuidad del negocio. No puede seguir tratándose como un aspecto separado. Las áreas de tecnología, operaciones y cumplimiento deben trabajar en conjunto.

Para los responsables de seguridad:

Integrar herramientas como Microsoft Entra ID, Sentinel y Defender for Identity, no solo por su potencia técnica, sino por su capacidad de ofrecer visibilidad centralizada y control granular sobre accesos críticos.

Promover la gestión activa de privilegios. Las cuentas con acceso amplio y sin control son uno de los principales vectores de ataque. La implementación de soluciones PAM no debe verse como un gasto, sino como una inversión en gobernabilidad tecnológica.

Medir y comunicar el nivel de ciberresiliencia. Las métricas propuestas en esta tesis pueden servir para reportes internos, auditorías o incluso decisiones de inversión tecnológica.

Para entes reguladores y legisladores:

Tomar como referencia los estándares internacionales y la Ley DORA para fortalecer la regulación nacional en materia de resiliencia operativa digital, especialmente en sectores críticos como el financiero.

Exigir indicadores de madurez y pruebas de recuperación como parte de la supervisión. Esto empujaría a las entidades a no quedarse solo en el cumplimiento documental, sino a demostrar capacidad real de respuesta.

Para futuras investigaciones:

Evaluar el impacto del modelo a largo plazo. Una implementación sostenida en el tiempo permitiría analizar cómo evoluciona el nivel de madurez y qué factores influyen en su mejora o estancamiento.

Ampliar la aplicación del modelo a otros sectores. Aunque esta tesis se centra en entidades financieras, muchas de las vulnerabilidades identificadas también están presentes en hospitales, universidades, organismos públicos o empresas de servicios.

Explorar la integración de ciberresiliencia con otras disciplinas. Por ejemplo, cómo se vincula con la gestión del cambio, la cultura organizacional o la inteligencia artificial para detección de amenazas.

Reflexión final

En tiempos donde las amenazas digitales crecen en volumen y sofisticación, pensar en ciberresiliencia ya no es una opción, sino una necesidad urgente. Proteger el Directorio Activo no solo significa evitar un ataque, sino garantizar que una organización pueda seguir funcionando, aun cuando algo falle. Esta tesis no pretende ser una receta única, sino una herramienta de base para construir capacidades más sólidas, más humanas y conscientes en la defensa de lo digital.

Referencias y Bibliografía

European Union Agency for Cybersecurity (ENISA). (2023). *THREAT LANDSCAPE 2023.*
Recuperado de: [https://www.enisa.europa.eu/publications/enisa- threat-landscape-2023?v2=1#contentList]

European Union Agency for Cybersecurity (ENISA). (2024). *THREAT LANDSCAPE 2024.*
Recuperado de: [https://www.enisa.europa.eu/publications/enisa- threat-landscape-2024]

Diario Oficial de la Unión Europea. (2022). *Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.o 1060/2009, (UE) n.o 648/2012, (UE) n.o 600/2014, (UE) n.o 909/2014 y (UE) 2016/1011.*
Recuperado de: [https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022R2554&qid=1737738747521]

Banco Central de Reserva del Perú (BCRP). (2025). *Entidades Financieras*
Recuperado de: [https://www.bcrp.gob.pe/sitios-de-interes/entidades-financieras.html]

Superintendencia de Banca, Seguros y AFP (SBS). (2021). *Resolución S.B.S. Nº 504-2021*.
Recuperado de: [https://intranet2.sbs.gob.pe/dv_int_cn/2046/v2.0/Adjuntos/504-2021.R.pdf]

Superintendencia de Banca, Seguros y AFP (SBS). (2025). *Resolución S.B.S. Nº 877-2020.*
Recuperado de: [https://intranet2.sbs.gob.pe/dv_int_cn/1894/v1.0/Adjuntos/877-2020.R.pdf]

National Institute of Standards and Technology (NIST). (2012). *Computer Security Incident Handling Guide*
Recuperado de: [https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf]

National Institute of Standards and Technology (NIST). (2020). *Security and Privacy Controls for Information Systems and Organizations*
Recuperado de: [https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf]

National Institute of Standards and Technology (NIST). (2021). *Developing Cyber-Resilient Systems*
Recuperado de: [https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1]

National Institute of Standards and Technology (NIST). (2024). *The NIST Cybersecurity Framework (CSF) 2.0*
Recuperado de: [https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf]

MICROSOFT. (2024). *Introducción a Active Directory Domain Services*
Recuperado de:]https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview]

MICROSOFT. (2024). *Introducción a Windows Serve*
Recuperado de: [https://learn.microsoft.com/es-mx/windows-server/get-started/get-started-with-windows-server]

ENAP. (2024). *CYBER-SURVEILLANCE*
Recuperado de: [https://dictionnaire.enap.ca/dictionnaire/docs/definitions/definitions_anglais/cyber_surveillance.pdf]

Decreto Supremo N.° 106-2017-PCM. (2017). *Decreto Supremo que aprueba el Reglamento para la identificación, evaluación y gestión de riesgos de los activos Críticos Nacionales (ACN).*
Recuperado de: [https://cdn.www.gob.pe/uploads/document/file/535679/DS_N_106-2017-PCM.pdf?v=1582930272]

Gobierno del Perú. (2024). *Activos Críticos Nacionales (ACN)*
Recuperado de: [https://www.gob.pe/10400-activos-criticos-nacionales-acn]

BBVA.(2025). *Así es DORA, la nueva regulación europea de ciber resiliencia financiera.*
Recuperado de: [https://www.bbva.com/es/innovacion/asi-es-dora-la-nueva-regulacion-europea-de-ciberresiliencia-financiera/]

IBM. (2025). *¿Qué es la resiliencia cibernética?.*
Recuperado de: [https://www.ibm.com/es-es/topics/cyber-resilience]

World Economic Forum (WEF). (2025). *Global Cybersecurity Outlook 2025.*
Recuperado de: [https://www.weforum.org/publications/global-cybersecurity-outlook-2025/]

World Economic Forum (WEF). (2025). *Unpacking Cyber Resilience.*
Recuperado de: [https://es.weforum.org/publications/unpacking-cyber-resilience/]

European Central Bank (ECB). (2025). *¿What is cyber resilience?.*
Recuperado de: [https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html]

Microsoft. (2025). *What is DORA?*

Recuperado de: [https://learn.microsoft.com/en-us/compliance/dora/dora-what-is-dora]

Microsoft. (2025). *Microsoft Entra ID*

Recuperado de: [https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id]

Federal Financial Institutions Examination Council (FFIEC). (2025). *Federal Financial Institutions Examination Council*

Recuperado de: [https://www.ffiec.gov/]

Banco Central de la República Argentina. (2025). *Ciberseguridad*

Recuperado de: [https://www.bcra.gob.ar/SistemasFinancierosYdePagos/Ciberseguridad.asp]

Banco Central Do Brasil. (2025). *RESOLUTION CMN 4,893 OF FEBRUARY 26, 2021*

Recuperado de: [https://www.bcb.gov.br/content/about/legislation_norms_docs/CMN_Resolution_No_4,893_2021.pdf]

Comisión del Mercado Financiero. (2025). *RAN Recopilación Actualizada de Normas de Bancos*

Recuperado de: [https://www.cmfchile.cl/portal/principal/613/w3-propertyvalue-29580.html]

Presidencia del Consejo de Ministros (PCM). (2025). *Secretaría de Gobierno y Transformación Digital*

Recuperado de: [https://www.gob.pe/7025-presidencia-del-consejo-de-ministros-secretaria-de-gobierno-y-transformacion-digital]

Presidencia del Consejo de Ministros (PCM). (2025). *Centro Nacional de Seguridad Digital*

Recuperado de: [https://www.gob.pe/cnsd]

Banco Interamericano de Desarrollo (BID). (2023). *Estado de la ciberseguridad en el sector financiero latinoamericano*.
Recuperado de: [https://publications.iadb.org]

Microsoft. (2022). *Cyber Signals: Amenazas y brechas en América Latina*.
Recuperado de [https://news.microsoft.com]

(ISC)². (2023). *Cybersecurity Workforce Study 2023*.
Recuperado de [https://www.isc2.org]

Fidelis Security, (2024). Active Directory Security

Recuperado de: [https://fidelissecurity.com/threatgeek/active-directory-security/major-active-directory-threats/]

Apéndices

Apéndice A. *Glosario de Términos*

Tabla 12

Definiciones de términos utilizados en la tesis

Término	Definición
Denegación de Servicio (DDoS)	El ataque de denegación de servicio (DDoS, por sus siglas en inglés) es un tipo de ataque cibernético en el cual los atacantes, a través de una red distribuida de sistemas comprometidos, generan tráfico de red masivo con el objetivo de debilitar, interrumpir o denegar el acceso a un servicio en particular.
Directorio Activo (AD)	El Directorio Activo (AD por sus siglas en inglés) almacena información acerca de los objetos de una red y facilita su búsqueda y uso por parte de los usuarios y administradores. Utiliza un almacén de datos estructurado como base para una organización jerárquica lógica de la información del directorio.
Ciberdefensa	Conjunto de medidas, estrategias y acciones dirigidas a proteger los sistemas de información, detectar amenazas cibernéticas y responder rápidamente ante incidentes de seguridad.
Ciberseguridad	Conjunto de medidas y acciones adoptadas para proteger los sistemas de información, redes y datos de accesos no autorizados, alteración, destrucción o interrupción.
Ciberresilencia	Capacidad de las entidades financieras para prevenir, mitigar, responder y recuperarse de incidentes

	relacionados con riesgos tecnológicos o cibernéticos, asegurando la continuidad y confiabilidad de sus operaciones críticas.
Cibervigilancia	La cibervigilancia es un mecanismo de vigilancia de personas, objetos o procesos basado en las nuevas tecnologías y funciona a partir de redes de datos, como Internet, y tiene por objeto facilitar la vigilancia en función de la cantidad, la rapidez o la complejidad de los datos que se han de tratar.
Ransomware	El ransomware se define como un tipo de ataque en el que los actores de amenazas toman el control de los activos de un objetivo y exigen un rescate a cambio de la devolución de la disponibilidad del activo o de exponer públicamente los datos del objetivo.
Servicio TIC	Los servicios digitales y de datos prestados a través de los sistemas de TIC a uno o varios usuarios internos o externos de forma continua, incluidos el hardware como servicio y los servicios de hardware que incluyen la prestación de asistencia técnica a través de actualizaciones de software o firmware por parte del proveedor de hardware y excluidos los servicios telefónicos analógicos tradicionales.
Canal digital	Medio a través del cual una entidad brinda servicios usando plataformas tecnológicas como aplicaciones móviles, banca por internet, billeteras digitales, cajeros automáticos, etc. Toda la información se transmite, procesa y almacena en formato digital.

Nota. Elaboración propia

Anexos

Anexo A. Cuestionario de Diagnóstico de Ciberresiliencia

Instrumento de autoevaluación basado en cinco bloques temáticos:

1. Controles técnicos sobre el AD
2. Gestión de identidades privilegiadas
3. Detección y respuesta a incidentes
4. Recuperación y continuidad operativa
5. Cumplimiento normativo y gobernanza

Cada ítem es valorado en una escala del 1 al 5. La sumatoria permite medir el nivel de madurez y establecer líneas base y metas de mejora. En la Tabla 13, Tabla 14, Tabla 15, Tabla 16 y Tabla 17 definimos las encuestas descritas:

ENCUESTA

Tabla 13

Bloque A. Controles Técnicos sobre el AD

N.º	Pregunta	Escala (1 a 5)
A1	¿Se cuenta con autenticación multifactor (MFA) para cuentas administrativas del AD?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
A2	¿Está configurado el monitoreo de cambios críticos en el AD (alta de cuentas, cambios de GPO, etc.)?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
A3	¿Se ha implementado segmentación de dominios o separación entre entornos críticos y no críticos?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
A4	¿Se revisan periódicamente las cuentas con privilegios elevados?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
A5	¿Se realiza hardening de los controladores de dominio según buenas prácticas (CIS, Microsoft)?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

N.º	Pregunta	Escala (1 a 5)
A6	¿Se emplean logs centralizados para registrar eventos del AD?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Nota. Elaboración propia

Tabla 14

Bloque B. Gestión de Identidades Privilegiadas

N.º	Pregunta	Escala (1 a 5)
B1	¿Se utiliza una solución PAM (Privileged Access Management) para controlar accesos privilegiados?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
B2	¿Se establecen cuentas administrativas temporales con vencimiento automático?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
B3	¿Se tiene un proceso formal de revisión de privilegios excesivos o heredados?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Nota. Elaboración propia

Tabla 15

Bloque C. Detección y Respuesta ante Incidentes

N.º	Pregunta	Escala (1 a 5)
C1	¿Existen alertas configuradas para detectar actividades anómalas en el AD (p. ej. replicación no autorizada)?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
C2	¿Se han definido procedimientos específicos para responder a incidentes que comprometan el AD?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
C3	¿Se cuenta con simulacros de respuesta ante ataques dirigidos al AD (ransomware, exfiltración de datos, etc.)?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Nota. Elaboración propia

Tabla 16

Bloque D. Recuperación y Continuidad

N.º	Pregunta	Escala (1 a 5)
D1	¿Se realizan respaldos frecuentes y seguros del AD?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
D2	¿Se han probado recientemente los procedimientos de restauración del AD?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
D3	¿La organización cuenta con una estrategia de recuperación ante desastres que contemple específicamente el AD?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Nota. Elaboración propia

Tabla 17

Bloque E. Cumplimiento Normativo y Gobierno

N.º	Pregunta	Escala (1 a 5)
E1	¿Se encuentra la organización alineada con algún marco de referencia (DORA, NIST CSF v2.0), ISO/IEC 27001:2022) para su resiliencia operativa?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
E2	¿Se realiza revisión periódica de políticas y procedimientos relacionados al AD?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
E3	¿Existe una cultura organizacional que promueva la resiliencia digital y la mejora continua?	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Nota. Elaboración propia