MAESTRÍA EN CIBERSEGURIDAD

PROYECTO DE GRADUACIÓN

Sometido al Tribunal Examinador de Postgrados para optar por el grado de Maestría en Ciberseguridad

Título del Proyecto

Diseño de una Propuesta de Manual de Procedimientos de Control Perimetral de Ciberseguridad basado en el Marco NIST en la Sede del Pacífico de la Universidad de Costa Rica

AUTOR
Irwin Leal Elizondo

TUTOR: Randall Artavia Delgado

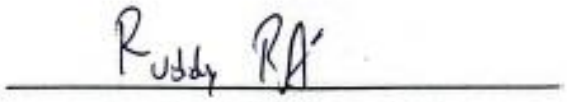
LECTOR: Irvin Argenis Sáenz Córdoba

Perez Zeledón, Costa Rica
Diciembre,2025

UNIVERSIDAD SAN ISIDRO DEL LABRADOR

MAESTRÍA EN CIBERSEGURIDAD

TRIBUNAL EXAMINADOR

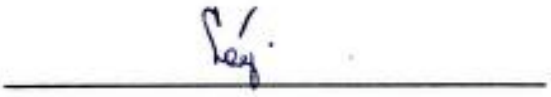


Ing. Ruddy Rodríguez Acuña

Director de Maestría

Msc. Randall Artavia Delgado

Tutor



Msc. Irvin Argenis Sáenz Córdoba

Lector

DECLARACIÓN JURADA

Yo, Irwin Leal Elizondo, mayor, soltero(a), egresado(a) de la carrera de Maestría Profesional en Ciberseguridad de la Universidad San Isidro Labrador, domiciliado en la ciudad de San Mateo, de Alajuela, portador(a) de la cédula de identidad número 6-0405-0541, en este acto, debidamente apercibido y entendido de las penas y consecuencias con las que se castiga, en el Código Penal, el delito del perjurio, ante quienes se constituyen en el Tribunal Examinador de mi Trabajo Final de Graduación para optar por el título de maestría, juro solemnemente que mi trabajo final de graduación titulado "***Diseño de una Propuesta de Manual de Procedimientos de Control Perimetral de Ciberseguridad basado en el Marco NIST en la Sede del Pacífico de la Universidad de Costa Rica***" es una obra original que ha respetado todo lo preceptuado por las Leyes Penales así con la Ley de Derechos de Autor y Derechos Conexos, número 6683 de 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 de 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte: artículo 70°: Es permitido citar a un autor transcribiendo los pasajes pertinentes siempre que estos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor y de la obra original. Asimismo, quedo advertido que la Universidad San Isidro Labrador se reserva el derecho de protocolizar este documento ante Notario Público. En fe de lo anterior firmo en la ciudad de Alajuela, al ser el 16 del mes de Septiembre del año dos mil veinticinco.

Irwin Leal Elizondo

DEDICATORIA

A mi familia y especialmente mis padres Ofelia Elizondo Madrigal y William Leal Calvo por todo el apoyo que me han dado a lo largo de mi carrera académica profesional.

A Dios que me fortalece dándome la sabiduría, perseverancia y tenacidad para completar estes trabajo final para optar por el nivel de Maestría.

A todos mis amigos de trabajo, cursos de maestría y de la vida y en especial a Marcela Benavides Porras que me han dado su apoyo en cada etapa y época de mi vida.

AGRADECIMIENTOS

Expreso mi más sincero agradecimiento a la Universidad Internacional San Isidro Labrador (UISIL) por brindarme la oportunidad de cursar la Maestría en Ciberseguridad, un programa que me permitió fortalecer mis competencias profesionales y comprender la relevancia de la seguridad informática en el contexto actual.

Agradezco profundamente a mi tutor académico por su orientación, paciencia y valiosas observaciones a lo largo del desarrollo de este trabajo final, las cuales fueron determinantes para alcanzar los objetivos propuestos.

Extiendo mi gratitud al personal técnico de la Sede del Pacífico de la Universidad de Costa Rica, por su disposición y colaboración durante la aplicación del cuestionario y por compartir su experiencia y conocimiento en torno a los controles perimetrales.

Finalmente, a mi familia, por su comprensión, apoyo incondicional y motivación constante durante todo este proceso académico y personal.

CARTA DE AUTORIZACIÓN DEL TUTOR

Pérez Zeledón, 06 de diciembre de 2025

Licenciado
Ruddy Rodríguez Acuña
Coordinador de la Escuela de Informática
Universidad Internacional San Isidro Labrador

Estimado señor Coordinador:

Yo, Randall Mauricio Artavia Delgado, mayor, Ingeniero en informática, con domicilio en la Trinidad de Moravia San José, portador de la cédula de identidad número **205740823**, en mi condición de tutor del Proyecto de Graduación titulado Diseño de una Propuesta de Manual de Procedimientos de Control Perimetral de Ciberseguridad basado en el Marco NIST en la Sede del Pacífico de la Universidad de Costa Rica. propuesta por el estudiante Irwin Leal Elizondo, manifiesto lo siguiente:

1. Que el proceso de trabajo final de graduación culmina satisfactoriamente.
2. Que se ha incorporado en el documento final las sugerencias hechas por el Tribunal Examinador.
3. Que he cumplido con el acompañamiento encomendado por la Universidad en forma y fondo.
4. Que considero que el documento final responde a las exigencias académicas establecidas por la Universidad.

Atentamente,

MATI Randall Mauricio Artavia Delgado
Tutor

CARTA DE APROBACIÓN DEL LECTOR

Pérez Zeledón, 06 de diciembre de 2025

Licenciado
Ruddy Rodríguez Acuña
Coordinador de la Escuela de Informática
Universidad Internacional San Isidro Labrador

Estimado señor Coordinador:

Yo, Irvin Argenis Sáenz Córdoba, mayor, Divorciado, Ingeniero en sistemas y docente, vecino de Guápiles, portador de la cédula de identidad número 7-0197-0839, en mi condición de lector del Proyecto de Graduación titulado Diseño de una Propuesta de Manual de Procedimientos de Control Perimetral de Ciberseguridad basado en el Marco NIST en la Sede del Pacífico de la Universidad de Costa Rica propuesta por el estudiante Irwin Leal Elizondo, manifiesto lo siguiente:

1. Que la lectura del trabajo final de graduación concluye satisfactoriamente.
2. Que he leído el documento final y he hecho mis observaciones en el mismo.
3. Que he cumplido con las labores de lector encomendadas por la Universidad en forma y fondo.
4. Que considero que el documento final responde a las exigencias académicas establecidas por la Universidad.

Atentamente,

Máster Irvin Argenis Sáenz Córdoba
Lector

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS Y CUADROS

ÍNDICE DE GRÁFICOS, FIGURAS E ILUSTRACIONES

LISTA DE PALABRAS CLAVES

Ciberseguridad

Control perimetral

Marco NIST

Seguridad de la información

Universidad de Costa Rica

Gestión del riesgo

Infraestructura crítica

Procedimientos de seguridad

Resiliencia tecnológica

Cultura de ciberseguridad

Manual de procedimientos

Continuidad operativa

Modelos de madurez

Monitoreo de red

Autenticación multifactor

RESUMEN EJECUTIVO

El presente Trabajo Final de Graduación desarrolla una propuesta de manual de procedimientos de control perimetral de ciberseguridad, fundamentada en el Marco de Ciberseguridad del NIST, con el fin de fortalecer la protección de los activos tecnológicos y la continuidad operativa de la Sede del Pacífico de la Universidad de Costa Rica.

Para sustentar la propuesta, se realizó un análisis estructurado compuesto por revisión documental, diagnóstico situacional y recopilación de información mediante instrumentos aplicados al personal técnico de TI. Este proceso permitió identificar brechas relacionadas con la ausencia de procedimientos escritos, limitaciones en el monitoreo perimetral, inconsistencias en la gestión de incidentes, carencias en la documentación operativa y oportunidades de mejora en los mecanismos de prevención y detección de amenazas

A partir de estos resultados se diseñó un manual de procedimientos estructurado sobre las cinco funciones del NIST (Identificar, Proteger, Detectar, Responder y Recuperar). Este documento incorpora lineamientos, actividades operativas, roles y responsabilidades, flujos de trabajo, matrices de control, criterios de priorización, protocolos de actuación, documentación de incidentes y mecanismos de mejora continua. Su aplicación permitirá estandarizar los procesos de seguridad perimetral, fortalecer la resiliencia institucional, optimizar la administración del riesgo tecnológico y establecer las bases para futuras auditorías internas, mejoras de infraestructura o ampliaciones del modelo de seguridad institucional.

En conjunto, esta propuesta constituye un instrumento estratégico y operativo que busca mejorar la gestión de ciberseguridad en la Sede del Pacífico, aportando un marco claro, práctico y adaptable para la protección del perímetro tecnológico, la reducción de vulnerabilidades y el cumplimiento de buenas prácticas internacionales, contribuyendo así a la consolidación de una cultura institucional orientada a la seguridad digital y la continuidad del servicio académico y administrativo.

CAPITULO I. INTRODUCCIÓN

1.1 Planteamiento del tema de estudio

La presente propuesta corresponde a la fase inicial del Trabajo Final de Graduación del programa de Maestría en Ciberseguridad de la Universidad Internacional San Isidro Labrador. El proyecto tiene como objetivo principal diseñar un manual de procedimientos para el control perimetral de ciberseguridad en la Sede del Pacífico de la Universidad de Costa Rica, utilizando como referencia el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST).

Este manual se enmarca como una solución práctica a los vacíos existentes en la gestión de controles perimetrales, en una institución pública de educación superior que presenta alta dependencia tecnológica. Actualmente, la Sede del Pacífico enfrenta amenazas constantes asociadas al aumento de servicios expuestos a redes externas, escaneos maliciosos y ataques dirigidos, que pueden comprometer la integridad, disponibilidad y confidencialidad de los servicios institucionales.

La propuesta busca sistematizar procedimientos y estandarizar la actuación técnica y administrativa mediante una guía clara, documentada y alineada con marcos internacionales reconocidos. Al estructurar la defensa perimetral mediante un enfoque metodológico, se pretende fortalecer la resiliencia de los sistemas de información de la sede, permitiendo una mejor capacidad de respuesta ante incidentes de seguridad, así como una mayor preparación preventiva.

El enfoque adoptado es el de investigación práctica aplicada, lo cual permite abordar un problema real mediante el diseño de un producto concreto, aprovechando tanto la revisión bibliográfica como el trabajo de campo. La propuesta contempla la participación activa del personal técnico de la sede, garantizando la contextualización de los procedimientos y su viabilidad de aplicación.

Esta iniciativa también responde a recomendaciones nacionales y regionales sobre la necesidad de robustecer las capacidades de ciberseguridad en las universidades, como lo ha manifestado el Consejo Nacional de Rectores (CONARE, 2022) y la Organización de Estados Iberoamericanos (OEI, 2020). La carencia de

un enfoque sistemático en la protección del perímetro de red ha sido una constante en varias instituciones, y este trabajo se plantea como una alternativa concreta para superar dichas deficiencias.

El resultado del proyecto pretende servir como insumo replicable en otras sedes universitarias, promoviendo una cultura de seguridad informática y cumplimiento normativo. Se espera que el manual se convierta en una herramienta de consulta permanente para el personal de tecnología, así como un documento base para auditorías internas y futuras estrategias de seguridad.

1.2 Antecedentes del tema

La expansión de las tecnologías de la información y la comunicación ha incrementado la complejidad de los entornos tecnológicos en instituciones académicas. La Universidad de Costa Rica, como referente nacional en educación superior, cuenta con múltiples sedes que dependen de infraestructuras de red para sus actividades académicas, administrativas y de investigación. Sin embargo, el crecimiento de los servicios conectados a Internet ha implicado una mayor exposición a riesgos cibernéticos (Villanueva, 2022).

A nivel global, las universidades son objetivos frecuentes de ataques informáticos debido al volumen y sensibilidad de la información que resguardan. De acuerdo con un informe de Check Point (2023), el sector educativo es el segundo más atacado por amenazas como ransomware, escaneo de puertos, ataques de denegación de servicio (DDoS) y vulnerabilidades de perímetro no gestionadas. En Costa Rica, diversas instituciones públicas han sido afectadas por ciberataques, siendo uno de los más mediáticos el perpetrado contra la Caja Costarricense de Seguro Social en 2022, el cual expuso debilidades estructurales en los controles perimetrales (Mora, 2022).

El Marco de Ciberseguridad del NIST (2018) ha sido adoptado en múltiples sectores por su enfoque estructurado y adaptable, siendo recomendado para entidades públicas en Latinoamérica (OEI, 2020). En este contexto, la Sede del

Pacífico de la Universidad de Costa Rica enfrenta retos particulares relacionados con la administración de su perímetro de red, la ausencia de documentación técnica unificada y procedimientos para la prevención y respuesta ante incidentes.

Los controles de seguridad tradicionales, en su mayoría centrados en software antivirus y medidas de usuario final, han demostrado ser insuficientes ante ataques más sofisticados como el ransomware, la suplantación de identidad, y los escaneos no autorizados de puertos perimetrales. A pesar de avances en materia de concienciación digital, no se cuenta actualmente con un manual estructurado ni procedimientos específicos para la defensa del perímetro de red de la sede.

Investigaciones recientes destacan la relevancia de contar con manuales de procedimientos que permitan sistematizar la defensa perimetral (García & Herrera, 2021; López et al., 2020). A pesar de algunos esfuerzos institucionales en materia de concienciación y medidas reactivas, no se ha identificado la existencia de una guía estratégica operativa basada en marcos internacionales como el NIST que se adapte al contexto universitario costarricense. Esta situación plantea una necesidad urgente de intervenir desde un enfoque disciplinar de ciberseguridad.

1.3 Justificación

En el contexto actual de ciberamenazas crecientes, la protección del perímetro de red en instituciones académicas representa un componente esencial de la defensa institucional. La Sede del Pacífico de la Universidad de Costa Rica, al igual que otras entidades públicas de educación superior, gestiona múltiples sistemas digitales que soportan servicios críticos. Sin embargo, la inexistencia de un enfoque estructurado para la protección perimetral plantea riesgos que pueden comprometer la continuidad operativa y la protección de datos sensibles.

La importancia del presente trabajo radica en la necesidad de transformar las prácticas reactivas actuales en una estrategia preventiva, proactiva y documentada, que esté alineada con marcos reconocidos como el Framework del Instituto Nacional de Estándares y Tecnología (NIST). La adopción de dicho marco

permitirá definir procesos de identificación de activos, implementación de controles, monitoreo de eventos y respuesta ante incidentes.

Los beneficiarios directos de esta propuesta serán los administradores de red y personal técnico, quienes contarán con una guía clara para implementar controles perimetrales. Los beneficiarios indirectos incluyen a toda la comunidad universitaria, cuya experiencia con los sistemas institucionales se verá fortalecida al mejorar la disponibilidad y confiabilidad de los servicios digitales. A nivel institucional, se fortalece la capacidad de cumplimiento normativo y la protección de la reputación.

Lo que se prevé cambiar con la investigación es la actual fragmentación en las prácticas de seguridad perimetral, promoviendo una estandarización de procedimientos, asignación clara de responsabilidades y definición de criterios de medición y mejora continua. Esto aportará una solución replicable en otras sedes universitarias, aumentando el nivel de madurez en ciberseguridad del sistema universitario público costarricense.

Según datos de Check Point (2023), el sector educativo experimenta un promedio de más de 2,300 ciberataques semanales por institución. En la región latinoamericana, las universidades han sido blanco frecuente de campañas de ransomware y espionaje digital, lo cual hace evidente la urgencia de contar con políticas claras y procedimientos adaptados a este tipo de amenazas.

Tabla 1.

Promedio de ciberataques semanales por sector (2023)

Sector	Promedio de ataques/semana
Educación e investigación	2,314
Gobierno	1,564
Salud	1,427

Nota. Esta tabla muestra por sector cual es el promedio de ataque a la semana.

Finalmente, desde una perspectiva académica, esta propuesta representa una aplicación concreta del conocimiento adquirido en la Maestría en Ciberseguridad, y un aporte significativo a la construcción de capacidades institucionales en materia de seguridad digital. El diseño de este manual no solo busca proteger infraestructura, sino consolidar una cultura organizacional orientada a la gestión del riesgo, el cumplimiento normativo y la sostenibilidad de los sistemas tecnológicos.

1.4 Objetivos

1.4.1 Objetivo general

Diseñar un manual de procedimientos de control perimetral de ciberseguridad para la Sede del Pacífico de la Universidad de Costa Rica, basado en el Marco NIST, con el fin de fortalecer la gestión de riesgos y la continuidad operativa de los servicios institucionales.

1.4.2 Objetivos específicos

1. Analizar los referentes teóricos y normativos en materia de control perimetral y marcos de ciberseguridad, con énfasis en el enfoque del Framework NIST.

2. Diagnosticar el estado actual de los controles perimetrales en la Sede del Pacífico de la Universidad de Costa Rica, identificando vulnerabilidades y brechas organizacionales.

3. Diseñar un manual de procedimientos técnicos y administrativos orientado a la identificación, protección, detección, respuesta y recuperación de incidentes perimetrales, según lineamientos del NIST.

1.5 Alcances

El presente trabajo tiene como alcance el diseño de un manual de procedimientos de control perimetral de ciberseguridad, centrado exclusivamente en la infraestructura de red de la Sede del Pacífico de la Universidad de Costa Rica. El enfoque se limita a establecer lineamientos para la identificación de activos, aplicación de controles de protección, mecanismos de detección de amenazas,

respuestas a incidentes y planes de recuperación, enmarcados en las cinco funciones del Marco NIST.

El alcance abarca tanto aspectos técnicos como administrativos, incluyendo procedimientos operativos estándar, roles y responsabilidades del personal de TI, flujos de acción ante incidentes y mecanismos de mejora continua. También contempla la elaboración de un plan de implementación escalonado y validación del manual con los actores institucionales pertinentes.

No se incluye la implementación directa de dispositivos o soluciones tecnológicas específicas, ni auditorías de cumplimiento formal. Tampoco se consideran aspectos de seguridad física ni gestión de dispositivos endpoint ajenos al alcance del perímetro de red.

Se espera que este manual pueda ser utilizado como insumo de referencia por otras sedes universitarias, así como por el área central de tecnología de la UCR, y que contribuya a la estandarización de buenas prácticas de ciberseguridad en el ámbito educativo público costarricense.

Figura 1.

Alcance del trabajo final de graduación

Nota: Imagen de fuente propia. Muestra el alcance del trabajo final de graduación

1.6 Limitaciones

El presente Trabajo Final de Graduación presenta una serie de limitaciones propias al alcance definido, a las condiciones institucionales y al tipo de investigación desarrollada. En primer lugar, el estudio se ajusta exclusivamente a la infraestructura de red y los procesos administrativos de la Sede del Pacífico de la Universidad de Costa Rica. Por tanto, no se consideran dispositivos, arquitecturas o procedimientos implementados en otras sedes universitarias ni en el Centro de Informática de la UCR, lo que restringe la generalización de los resultados a un contexto institucional más amplio.

Asimismo, la investigación se enfoca en el diseño de un manual de procedimientos y no en la implementación técnica de controles perimetrales específicos. Esto implica que no se realizan configuraciones reales de dispositivos de seguridad, pruebas de penetración, auditorías de cumplimiento ni validaciones técnicas avanzadas, dado que tales actividades exceden el objetivo propuesto y los recursos disponibles.

Otra limitación corresponde al acceso a la información. El diagnóstico se fundamenta en los datos proporcionados por el personal técnico, entrevistas y cuestionarios. La disponibilidad de información puede verse afectada por políticas internas de confidencialidad, así como por la ausencia de documentación histórica completa sobre incidentes, configuraciones previas o registros de seguridad. Esto puede generar vacíos en la reconstrucción de la situación actual de la infraestructura perimetral.

De igual manera, el estudio se realizó en un período de tiempo acotado, lo que puede limitar la profundidad del análisis en áreas que requieren observación prolongada,. El contexto académico influye en esta limitación, al estar sujeto a un cronograma establecido para la elaboración del TFG.

Por último, la rápida evolución de las amenazas cibernéticas y de las tecnologías de seguridad perimetral constituye una limitación transversal. Las recomendaciones y lineamientos propuestos pueden requerir actualizaciones periódicas para mantenerse alineados con las mejores prácticas, los cambios normativos y las innovaciones tecnológicas.

1.7 Cronograma de actividades

NOMBRE DE LA TAREA	DURACIÓN	INICIO	FINAL
Trabajo de investigación final			
Planeación del trabajo			
Definición del título	1 día	01/07/2025	01/07/2025
Definición de objetivos	2 días	02/07/2025	03/07/2025
Creación del cronograma	2 días	04/07/2025	05/07/2025
Creación bitácora de trabajo	2 días	06/07/2025	07/07/2025
Entrega del plan de trabajo al tutor	1 día	08/07/2025	08/07/2025
Desarrollo			
Desarrollo del Capítulo I	1 semana	09/07/2025	15/07/2025
Creación de estructura del TFG	3 días	16/07/2025	18/07/2025
Planteamiento del tema	3 días	19/07/2025	21/07/2025
Justificación del trabajo	3 días	22/07/2025	24/07/2025
Definición de alcances	2 días	25/07/2025	26/07/2025
Definición de limitaciones	2 días	27/07/2025	28/07/2025
Definición producto esperado	2 días	29/07/2025	30/07/2025
Envío Capítulo I al tutor	1 día	31/07/2025	31/07/2025
Desarrollo del Capítulo II	2 semanas	01/08/2025	14/08/2025
Desarrollo de marco teórico	1 semana	15/08/2025	21/08/2025
Envío Capítulo II al tutor	1 día	22/08/2025	22/08/2025
Desarrollo del Capítulo III	3 semanas	23/08/2025	12/09/2025
Aplicación de instrumentos	2 semanas	13/09/2025	26/09/2025
Análisis de datos	1 semana	27/09/2025	03/10/2025
Envío Capítulo III al tutor	1 día	04/10/2025	04/10/2025
Desarrollo del Capítulo IV	2 semanas	05/10/2025	18/10/2025
Propuesta	1 semana	19/10/2025	25/10/2025
Envío Capítulo IV al tutor	1 día	26/10/2025	26/10/2025
Desarrollo del Capítulo V	2 semanas	27/10/2025	09/11/2025
Desarrollo conclusiones	2 días	10/11/2025	11/11/2025
Desarrollo recomendaciones	2 días	12/11/2025	13/11/2025
Resumen ejecutivo	2 días	14/11/2025	15/11/2025
Anexos	2 días	16/11/2025	17/11/2025
Envío Capítulo V al tutor	1 día	18/11/2025	18/11/2025
Cierre Trabajo Final			
Revisión por parte del Tutor	3 días	19/11/2025	21/11/2025

Correcciones sugeridas por Tutor	3 días	22/11/2025	24/11/2025
Entrega borrador al Lector	1 día	25/11/2025	25/11/2025
Revisión por parte del Lector	2 días	26/11/2025	27/11/2025
Correcciones sugeridas por Lector	2 días	28/11/2025	29/11/2025
Envío al Filólogo	1 día	30/11/2025	30/11/2025
Revisión del Filólogo	2 días	01/12/2025	02/12/2025
Correcciones Trabajo Final	2 días	03/12/2025	04/12/2025
Empaste documento Final	2 días	05/12/2025	06/12/2025
Entrega documento a Universidad	1 día	07/12/2025	07/12/2025

1.8 Producto esperado del TFG

Objetivos específicos	Entregables	Formato
Analizar los referentes teóricos y normativos en materia de control perimetral y marcos de ciberseguridad.	Matriz comparativa en Excel.	.xlsx
Diagnosticar el estado actual de los controles perimetrales en la Sede del Pacífico de la Universidad de Costa Rica.	Lista de chequeo, entrevistas, cuestionarios digitales.	.docx
Diseñar un manual de procedimientos técnicos y administrativos para la gestión perimetral.	Documento técnico que sistematiza acciones, roles y procedimientos para proteger el perímetro de red	.docx

CAPÍTULO II. MARCO TEÓRICO

1. Introducción al concepto de ciberseguridad institucional

La ciberseguridad ha evolucionado como una necesidad estratégica para proteger los activos de información frente a amenazas cada vez más sofisticadas. En el contexto universitario, esta necesidad se vuelve crítica debido a la gran cantidad de datos académicos, administrativos, financieros y personales que se procesan y almacenan. La protección de estos recursos es vital para garantizar la continuidad operativa, la reputación institucional y el cumplimiento normativo (Villanueva, 2022).

A nivel global, las universidades enfrentan múltiples riesgos cibernéticos, desde ataques dirigidos como ransomware, hasta campañas de phishing o explotación de vulnerabilidades en sus servicios expuestos. En Costa Rica, casos recientes como el ataque a la Caja Costarricense de Seguro Social han evidenciado la importancia de establecer controles estructurados, especialmente en las instituciones del sector público (Mora, 2022).

La ciberseguridad institucional implica el desarrollo de políticas, procesos, controles y tecnologías que permitan proteger los sistemas de información y garantizar su disponibilidad, integridad y confidencialidad. En este contexto, el control perimetral se posiciona como una de las capas fundamentales de defensa, especialmente en organizaciones con estructuras descentralizadas como las universidades.

2. Amenazas cibernéticas en el entorno universitario

Diversos estudios confirman que las universidades son blancos atractivos para los ciberatacantes debido a la naturaleza abierta de sus redes, el valor de la información que resguardan y la multiplicidad de usuarios con distintos niveles de privilegios. De acuerdo con el informe "Cyber Attack Trends" de Check Point (2023), el sector educativo es uno de los más atacados a nivel mundial, registrando un promedio de 2,314 ciberataques semanales por institución.

Entre las amenazas más comunes se encuentran:

- **Ransomware**: Secuestro de información mediante cifrado, solicitando un rescate.

- **Escaneo de puertos**: Actividad de reconocimiento para identificar servicios vulnerables.
- **Ataques DDoS**: Saturación de servicios para interrumpir su disponibilidad.
- **Suplantación de identidad (phishing)**: Obtención fraudulenta de credenciales institucionales.
- **Explotación de vulnerabilidades**: Aprovechamiento de fallos en sistemas no actualizados.

Estos vectores de ataque afectan directamente la operatividad de los servicios digitales y, en muchos casos, generan pérdidas económicas, pérdida de información, interrupción de clases, daño reputacional y exposición de datos personales o de investigación.

3. Control perimetral: concepto y evolución

El control perimetral se refiere al conjunto de mecanismos implementados para proteger el borde de la red institucional frente a accesos no autorizados o tráfico malicioso proveniente del exterior. Tradicionalmente, estos mecanismos incluían firewalls, listas de control de acceso (ACLs), y reglas básicas de filtrado. Sin embargo, la evolución de las amenazas ha requerido una transformación hacia controles más avanzados y dinámicos (García & Herrera, 2021).

El perímetro de red ya no es una línea física clara como en los entornos tradicionales, debido al uso de servicios en la nube, redes inalámbricas, teletrabajo y dispositivos móviles. En este nuevo contexto, el perímetro debe entenderse como una frontera lógica, y su protección requiere mecanismos como:

- **Firewalls de nueva generación (NGFW)**.
- **Sistemas de prevención de intrusos (IPS)**.
- **Segmentación de redes internas (microsegmentación)**.
- **VPN seguras para acceso remoto**.
- **Sistemas de detección y respuesta (NDR, XDR)**.

La implementación de estos controles debe estar guiada por un enfoque de defensa en profundidad, en donde el control perimetral actúe como la primera línea de resistencia ante posibles ataques.

4. El Marco de Ciberseguridad del NIST: Fundamentos y Aplicabilidad

El Framework para mejorar la ciberseguridad de las infraestructuras críticas, desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), se ha convertido en uno de los marcos de referencia más utilizados a nivel global para fortalecer la postura de seguridad de organizaciones públicas y privadas. Su objetivo principal es proporcionar un lenguaje común para identificar riesgos, proteger activos, detectar eventos de seguridad, responder a incidentes y recuperar operaciones normales (NIST, 2018).

El marco está organizado en cinco funciones esenciales:

- **Identificar:** Inventariar activos, roles, riesgos y políticas.
- **Proteger:** Establecer controles de seguridad, conciencia y mecanismos técnicos.
- **Detectar:** Desplegar herramientas y procesos para la identificación de anomalías.
- **Responder:** Activar protocolos ante incidentes, contener y remediar.
- **Recuperar:** Restaurar capacidades y comunicar hallazgos.

Este enfoque flexible permite que organizaciones como universidades adapten sus controles de acuerdo con su nivel de madurez, recursos disponibles y entorno regulatorio. Su uso es especialmente adecuado para instituciones descentralizadas que requieren armonización de esfuerzos técnicos y administrativos para proteger su perímetro de red y garantizar la continuidad de sus servicios críticos.

La aplicabilidad del NIST en universidades latinoamericanas ha sido promovida por organismos internacionales como la OEI (2020), debido a su lenguaje accesible, compatibilidad con normas ISO, y la posibilidad de escalar su implementación por fases. Además, se adapta a diferentes niveles de complejidad, lo que lo hace ideal

para entornos como la Sede del Pacífico de la Universidad de Costa Rica, donde existen múltiples servicios interconectados, pero no siempre recursos avanzados.

5. Normas ISO/IEC y su relación con el control perimetral

Las normas internacionales ISO/IEC 27001 e ISO/IEC 27002 constituyen otro referente esencial para el diseño de políticas y controles de seguridad de la información. Estas normas ofrecen una estructura sistemática para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), que puede complementar el marco NIST a nivel operativo (ISO, 2022).

Específicamente, la norma ISO/IEC 27033 aborda la seguridad en redes, lo que incluye la protección del perímetro de red mediante la gestión segura del tráfico entrante y saliente, el diseño de zonas desmilitarizadas (DMZ), el uso de cortafuegos y mecanismos de inspección profunda de paquetes (DPI). Estas guías pueden ser aplicadas de forma complementaria al diseño del manual que se propone, asegurando que las recomendaciones sigan buenas prácticas ampliamente validadas a nivel internacional.

Además, la ISO/IEC 27035 sobre gestión de incidentes establece pautas claras para la respuesta a eventos de seguridad, lo cual se articula con las fases de “Detectar” y “Responder” del NIST. Al adoptar elementos de ambas familias de normas, el manual de control perimetral podrá alcanzar un mayor grado de madurez y estandarización, facilitando su implementación institucional.

6. Modelos de madurez en ciberseguridad

Evaluar la madurez de los controles de seguridad de una organización es crucial para planificar acciones de mejora continua. Los modelos de madurez permiten clasificar el estado de las capacidades de ciberseguridad según niveles que van desde el inicial (ad hoc) hasta el optimizado (basado en métricas y mejora constante). Uno de los modelos más utilizados es el Cybersecurity Capability Maturity Model (C2M2), promovido por el Departamento de Energía de EE.UU.

En el contexto universitario, estos modelos permiten identificar en qué nivel se encuentra la institución respecto al control perimetral: ¿existe documentación formal? ¿Se monitorean los accesos externos? ¿Hay procedimientos de respuesta

definidos? Según García y Herrera (2021), la mayoría de las universidades públicas latinoamericanas se encuentran entre los niveles 1 y 2 de madurez (reactivo y repetible), lo que implica una urgente necesidad de avanzar hacia modelos más estructurados.

El uso de estos modelos puede integrarse en la propuesta de manual para establecer indicadores de desempeño y monitorear su efectividad, promoviendo así una gestión basada en evidencia y métricas.

7. Arquitectura de red perimetral y segmentación

La arquitectura de red perimetral constituye uno de los pilares fundamentales en la defensa de las infraestructuras informáticas. Su diseño determina la forma en que se controlan los flujos de información entre redes internas confiables y redes externas potencialmente hostiles, como Internet. Una arquitectura de red robusta incluye zonas segmentadas con diferentes niveles de confianza, permitiendo aplicar controles diferenciados según el riesgo asociado (Forrest & Martínez, 2020).

En entornos universitarios, donde se alojan múltiples servicios tale como: correo institucional, bases de datos estudiantiles, aulas virtuales, sistemas administrativos, entre otros, es esencial la separación lógica y física de redes, permitiendo un control granular del tráfico. Esto se logra mediante la implementación de redes VLAN, firewalls internos, DMZs (zonas desmilitarizadas) y políticas de acceso por rol (RBAC).

La segmentación de red también contribuye a limitar el movimiento lateral de posibles atacantes. Si un dispositivo es comprometido, su capacidad para propagarse a otras áreas críticas del sistema se reduce significativamente. Esta práctica es recomendada por marcos como Zero Trust Architecture (ZTA), que promueve el principio de “nunca confiar, siempre verificar”, independientemente de la ubicación de un dispositivo (NIST SP 800-207).

8. Herramientas tecnológicas para el control perimetral

Existen diversas tecnologías diseñadas específicamente para el control perimetral, cada una con funciones complementarias que fortalecen la defensa de los sistemas:

- **Firewalls de nueva generación (NGFW):** Permiten filtrar tráfico por puertos, aplicaciones, usuarios y contenido. Integran funciones como IPS, antivirus, control de aplicaciones y filtrado web.
- **Sistemas de detección y prevención de intrusos (IDS/IPS):** Monitorean el tráfico de red en busca de patrones maliciosos, alertando o bloqueando automáticamente según la configuración.
- **Gateways seguros de correo y navegación (Secure Email/Web Gateways):** Analizan el tráfico de aplicaciones para bloquear amenazas como phishing, malware o enlaces maliciosos.
- **Sistemas de gestión de eventos e información de seguridad (SIEM):** Centralizan y correlacionan logs de seguridad para detectar comportamientos anómalos.
- **Sistemas de control de acceso a la red (NAC):** Evalúan la conformidad de dispositivos antes de conceder acceso a la red.

La selección de estas herramientas debe estar guiada por un análisis de riesgos, presupuesto disponible y nivel de madurez tecnológica. Además, su efectividad depende de una correcta configuración, mantenimiento, monitoreo y respuesta oportuna ante alertas.

9. Rol del factor humano en la seguridad perimetral

Aunque la tecnología es esencial en el control perimetral, el factor humano representa un componente crítico tanto como fortaleza como debilidad. Una parte significativa de los incidentes de ciberseguridad ocurre por errores humanos, mal uso de sistemas o desconocimiento de las políticas institucionales (ENISA, 2022).

Por ello, es indispensable incorporar estrategias de concienciación y capacitación continua, especialmente para el personal técnico encargado de administrar el perímetro de red. La definición de roles claros, procedimientos documentados, simulacros de respuesta a incidentes y revisión periódica de permisos son acciones que fortalecen la postura de seguridad.

Además, la cultura organizacional debe promover la responsabilidad compartida sobre la ciberseguridad, reconociendo que todos los miembros de la institución (docentes, estudiantes, administrativos) interactúan con sistemas expuestos a Internet y, por tanto, deben adoptar buenas prácticas como el uso de contraseñas seguras, la verificación de enlaces y la denuncia de comportamientos sospechosos.

10. Retos en entornos universitarios descentralizados

Las universidades públicas como la Universidad de Costa Rica operan bajo un modelo descentralizado, en el cual cada sede o unidad académica gestiona sus propios recursos tecnológicos. Esta autonomía puede representar un obstáculo para la implementación de controles perimetrales estandarizados, al existir múltiples enfoques, presupuestos, niveles de conocimiento técnico y prioridades (Rodríguez & Chaves, 2021).

Entre los principales retos se encuentran:

- Falta de políticas institucionales unificadas sobre ciberseguridad.
- Limitaciones presupuestarias para adquirir herramientas de protección.
- Infraestructuras heredadas con configuraciones obsoletas.
- Escasa comunicación entre sedes y centros de TI centrales.
- Diferencias en la capacidad técnica del personal responsable.

Superar estos desafíos requiere de liderazgo institucional, marcos normativos comunes, plataformas de colaboración técnica y recursos dedicados a la gestión del cambio. En este contexto, el desarrollo de un manual estandarizado de control perimetral puede servir como catalizador para mejorar la coordinación y establecer una base común sobre la cual construir una defensa integral.

11. Buenas prácticas en la implementación de controles perimetrales

La implementación efectiva de controles perimetrales requiere no solo el uso adecuado de herramientas tecnológicas, sino también la adopción de buenas

prácticas que aseguren su correcta operación y sostenibilidad en el tiempo. Algunas de las recomendaciones ampliamente aceptadas por expertos y organismos como SANS Institute (2023) incluyen:

- **Documentar procedimientos estándar:** Toda acción relacionada con la administración del perímetro debe estar respaldada por procedimientos formalizados que especifiquen qué hacer, quién lo hace y cómo.
- **Aplicar el principio de menor privilegio:** Los accesos a recursos deben otorgarse únicamente en función de las responsabilidades del usuario y su necesidad operativa.
- **Actualizar y parchear sistemas regularmente:** La mayoría de los ataques exitosos explotan vulnerabilidades conocidas y no corregidas.
- **Auditar los registros de actividad:** Revisar logs del firewall, del SIEM y otros sistemas ayuda a detectar anomalías tempranas.
- **Monitorear continuamente la red:** La visibilidad en tiempo real es esencial para identificar actividades inusuales o intentos de intrusión.

Estas prácticas deben integrarse dentro de una estrategia institucional que permita su ejecución constante y no ocasional, estableciendo mecanismos de control, seguimiento y retroalimentación.

12. Ejemplos de manuales de ciberseguridad aplicados en universidades

Diversas universidades en América Latina han comenzado a implementar manuales y guías de ciberseguridad específicos para su contexto. Por ejemplo, la Universidad Nacional Autónoma de México (UNAM) cuenta con un manual de políticas de seguridad informática que incluye un apartado específico sobre protección del perímetro de red. En Colombia, la Universidad del Rosario ha desarrollado un plan de continuidad de servicios digitales con componentes perimetrales.

En Costa Rica, si bien existen iniciativas de concientización y lineamientos generales, no se han identificado manuales específicos sobre control perimetral en

el contexto de sedes regionales universitarias. Esto refuerza la pertinencia de la presente propuesta como una solución contextualizada, capaz de convertirse en modelo para otras unidades académicas del país.

Según López, Pérez y Mendoza (2020), la clave del éxito de estos manuales reside en su claridad, aplicabilidad, alineamiento con normativas y el involucramiento del personal técnico desde su diseño hasta su aplicación.

13. El marco legal y normativo costarricense

En Costa Rica, la legislación vigente reconoce la importancia de proteger los activos digitales institucionales. La Ley N.º 8968 sobre Protección de la Persona frente al Tratamiento de sus Datos Personales establece la responsabilidad de las instituciones públicas sobre la custodia de los datos. A su vez, la Ley N.º 8220 obliga a garantizar la continuidad y disponibilidad de los servicios públicos digitales.

En el ámbito universitario, el CONARE ha promovido lineamientos estratégicos para la ciberseguridad en universidades públicas (2022), en los que se sugiere implementar controles estructurados, incluyendo medidas perimetrales. Sin embargo, estos documentos aún no se traducen en procedimientos operativos concretos, dejando un vacío que puede ser abordado mediante la elaboración de manuales específicos como el que se propone en este trabajo.

La presente propuesta se alinea con dichos marcos regulatorios, contribuyendo no solo al cumplimiento normativo, sino también a la estandarización de prácticas en el sector universitario público.

14. Impacto de la falta de controles perimetrales estructurados

La ausencia de procedimientos claros para la protección del perímetro puede desencadenar múltiples consecuencias negativas. Entre ellas destacan:

- **Pérdida de confidencialidad:** Acceso no autorizado a información sensible de estudiantes, docentes o investigadores.
- **Interrupción del servicio:** Ataques de denegación de servicio (DDoS) pueden afectar plataformas de matrícula, aulas virtuales o servicios administrativos.

- **Pérdida económica:** Desde costos por recuperación hasta sanciones legales por incumplimiento normativo.
- **Daño reputacional:** Incidentes públicos pueden afectar la confianza de la comunidad y los stakeholders.

García y Herrera (2021) sostienen que muchas universidades subestiman estos riesgos hasta que experimentan un evento grave. Contar con un manual permite anticiparse, reaccionar de forma estructurada y mitigar el impacto ante un incidente.

15. Consideraciones para el diseño de un manual contextualizado

El diseño de un manual de procedimientos debe partir del análisis de la realidad institucional. Es decir, no se trata de copiar modelos genéricos, sino de adaptar las mejores prácticas a las capacidades, cultura organizacional y estructura tecnológica específica de la sede.

Para garantizar su éxito, el manual debe cumplir con los siguientes criterios:

- **Relevancia:** Abordar necesidades reales del contexto.
- **Simplicidad:** Redactado en lenguaje técnico pero accesible.
- **Flexibilidad:** Que permita su ajuste en función de la evolución tecnológica.
- **Integración:** Debe articularse con otras políticas institucionales.
- **Evaluación:** Debe incluir métricas para su revisión y mejora continua.

En este sentido, la propuesta presentada busca generar un documento base sólido, construido con participación técnica y validado por actores clave de la Sede del Pacífico de la Universidad de Costa Rica.

16. Gestión del cambio organizacional en la implementación de manuales

Uno de los principales desafíos al implementar un manual de control perimetral es la resistencia al cambio. La gestión del cambio organizacional es un proceso estructurado que busca facilitar la transición de una situación actual a una futura deseada. En términos prácticos, implica movilizar a las personas, los

procesos y la tecnología hacia una nueva forma de operar. Según Kotter (2012), los cambios sostenibles en las organizaciones requieren más que nuevas herramientas: requieren transformación cultural.

Kotter plantea ocho etapas fundamentales para un cambio exitoso: (1) establecer un sentido de urgencia; (2) formar una coalición poderosa; (3) desarrollar una visión clara; (4) comunicar la visión; (5) facultar a otros para actuar según la visión; (6) generar logros a corto plazo; (7) consolidar las mejoras y producir más cambios; y (8) anclar los nuevos enfoques en la cultura institucional. En el contexto universitario, estas etapas pueden adaptarse a procesos como la adopción de normativas nuevas o la implementación de herramientas de ciberseguridad.

Por ejemplo, en la Sede del Pacífico de la Universidad de Costa Rica, la introducción del manual debe comenzar por demostrar los riesgos actuales y la necesidad de proteger los activos digitales. Luego, se deben identificar aliados estratégicos dentro de la administración, el personal técnico y académico que faciliten el proceso. La capacitación, la comunicación efectiva y la disponibilidad de recursos serán clave.

Además, se recomienda establecer una unidad o comité de implementación que se encargue de velar por el cumplimiento del manual, la resolución de dudas y la recolección de retroalimentación. Las universidades que han logrado implementar con éxito políticas de seguridad informática han destacado la importancia de involucrar a todos los niveles organizacionales (López & Salas, 2021).

La sostenibilidad del cambio dependerá en última instancia de su integración en la cultura institucional. Por eso, se debe trabajar no solo en los aspectos técnicos del manual, sino también en generar conciencia sobre su valor, ofrecer incentivos para el cumplimiento y establecer mecanismos de monitoreo y mejora continua. La gestión del cambio, en este contexto, no es una tarea puntual, sino un proceso cíclico y adaptativo que acompaña el desarrollo tecnológico y organizativo de la institución.

17. Evaluación de riesgos y activos críticos

Antes de definir cualquier medida de protección perimetral, es imprescindible realizar una evaluación exhaustiva de riesgos. Esta etapa permite identificar los activos críticos de la organización, analizar las amenazas potenciales y valorar las vulnerabilidades existentes. En términos de ciberseguridad, un activo crítico es cualquier recurso —físico o digital— cuya pérdida o compromiso pueda afectar la confidencialidad, integridad o disponibilidad de los servicios (ISO/IEC 27005, 2018).

En el entorno universitario, los activos críticos pueden incluir bases de datos de estudiantes y docentes, sistemas de matrícula, plataformas de aprendizaje virtual, servidores de correo electrónico institucional y repositorios de investigación. Para cada uno de estos activos debe determinarse su valor, el nivel de exposición a amenazas (internas y externas) y la probabilidad de ocurrencia de eventos adversos.

Las metodologías más utilizadas para este tipo de análisis incluyen MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) e ISO/IEC 27005. Estas ofrecen esquemas estructurados para identificar, clasificar y evaluar riesgos de forma cualitativa y cuantitativa.

En el caso de la Sede del Pacífico, sería fundamental realizar talleres con personal técnico y administrativo para identificar conjuntamente los sistemas más sensibles y las amenazas más probables. Esta información permitirá no solo diseñar controles perimetrales más adecuados, sino también priorizar recursos y esfuerzos. Además, contar con un inventario de activos y un mapa de riesgos actualizado será clave para la evolución del manual y su adaptación a futuros escenarios tecnológicos o institucionales.

La evaluación de riesgos debe ser entendida como un proceso continuo, no como una actividad puntual. La naturaleza dinámica de las amenazas cibernéticas obliga a revisar periódicamente los análisis realizados, adaptando las medidas de seguridad a nuevas vulnerabilidades, cambios tecnológicos o modificaciones en la operativa institucional.

18. Integración del manual con políticas institucionales existentes

Para que un manual de control perimetral sea efectivo y aplicable, debe integrarse armónicamente dentro del conjunto normativo y de políticas institucionales ya existentes en la organización. Esta integración no solo legitima el documento, sino que asegura su coherencia con otras iniciativas de gobernanza tecnológica y facilita su implementación al no generar duplicidades ni contradicciones (Pino & Cárdenas, 2020).

En el caso de la Universidad de Costa Rica y específicamente su Sede del Pacífico, es necesario vincular el manual con:

- La política institucional de tecnologías de información y comunicación (TIC), que establece lineamientos generales sobre el uso de la infraestructura tecnológica.
- El reglamento interno sobre la protección de datos personales, en concordancia con la Ley 8968.
- Las políticas de uso aceptable de la red y servicios informáticos, que orientan el comportamiento de los usuarios dentro del entorno digital institucional.
- Las normativas de seguridad emitidas por el CONARE o el Centro de Informática (CI), si están disponibles.

Una correcta integración implica mapear los apartados del manual con los lineamientos ya existentes, para identificar dónde se refuerzan, complementan o requieren ajustes. Esto puede hacerse mediante una matriz de alineamiento normativo que permita visualizar las relaciones entre documentos y evidenciar cualquier vacío legal o procedimental que deba ser subsanado.

Asimismo, es importante que la aplicación del manual esté respaldada por órganos institucionales como el consejo académico, la administración de la sede o el comité de tecnología, de modo que se garantice su vigencia formal. En esta línea, el manual debe establecer mecanismos de actualización periódica, en coordinación con los cambios que puedan surgir en otras políticas.

Otro aspecto clave es que las recomendaciones y procedimientos establecidos en el manual se traduzcan en acciones concretas dentro del entorno de trabajo cotidiano. Por ejemplo, las configuraciones sugeridas en los firewalls, las responsabilidades del personal técnico o los protocolos de respuesta a incidentes deben estar alineados con las capacidades reales y los roles establecidos en la institución.

Finalmente, se recomienda incluir en el manual un apartado específico de articulación normativa, donde se indiquen explícitamente los documentos con los cuales se relaciona, su jerarquía dentro del marco institucional y las dependencias administrativas responsables de su supervisión y cumplimiento.

19. Indicadores de desempeño y métricas de evaluación

Para garantizar que la implementación del manual de control perimetral tenga un impacto real y medible, es necesario establecer indicadores de desempeño que permitan monitorear su cumplimiento y eficacia a lo largo del tiempo. Estos indicadores deben estar alineados con los objetivos estratégicos de la institución, así como con las mejores prácticas internacionales en gestión de la ciberseguridad (ISACA, 2021).

Un buen indicador debe ser específico, medible, alcanzable, relevante y temporal (modelo SMART). Algunos ejemplos de métricas aplicables al control perimetral en entornos universitarios son:

- **Número de intentos de acceso no autorizado bloqueados por el firewall.**
- **Porcentaje de sistemas actualizados con los últimos parches de seguridad.**
- **Tiempo promedio de respuesta ante incidentes detectados en el perímetro.**
- **Frecuencia de revisiones de configuraciones de equipos perimetrales.**
- **Nivel de cumplimiento de los procedimientos descritos en el manual (auditado).**

- **Resultados de auditorías internas o externas sobre controles perimetrales.**

Además, estos indicadores pueden organizarse en categorías según su propósito: prevención, detección, respuesta y recuperación. Esta clasificación permite establecer un tablero de control integral que brinde una visión global del estado de la ciberseguridad perimetral.

Es recomendable que las métricas sean recogidas por un sistema automatizado o mediante reportes periódicos elaborados por el personal técnico responsable. Asimismo, los resultados deben presentarse ante la administración y el comité de tecnología de la sede, acompañados de análisis comparativos, tendencias históricas y recomendaciones.

La implementación de indicadores también debe estar acompañada por una cultura de mejora continua. En este sentido, los datos recogidos deben usarse no solo para evaluar el desempeño, sino también para ajustar procedimientos, identificar necesidades de capacitación, justificar inversiones o redefinir prioridades.

Un manual que incluye indicadores claros no solo facilita su evaluación, sino que también lo convierte en una herramienta dinámica y viva, capaz de adaptarse a la evolución del contexto tecnológico e institucional. Esta orientación hacia la evidencia es clave para construir una gestión de la ciberseguridad basada en resultados y no solo en intenciones.

20. Propuesta de estructura del manual de control perimetral

Para facilitar la implementación efectiva del control perimetral en la Sede del Pacífico de la Universidad de Costa Rica, se propone una estructura estandarizada para el manual que contemple los aspectos técnicos, organizacionales y normativos necesarios. Esta estructura debe ser clara, comprensible y adaptable a futuros cambios tecnológicos o regulatorios.

Una posible organización del manual podría incluir los siguientes apartados:

1. **Introducción y objetivos:** Define el propósito del manual, su justificación y los objetivos generales y específicos que persigue.

2. **Alcance y aplicabilidad:** Establece las unidades organizativas, sistemas, infraestructuras y personal a los que aplica el manual, delimitando responsabilidades y escenarios.
3. **Marco normativo y referencias:** Compila las leyes, reglamentos, políticas institucionales y estándares internacionales (como NIST, ISO/IEC 27001 y 27005) que sustentan el contenido del manual.
4. **Roles y responsabilidades:** Especifica los actores involucrados en la implementación de los controles perimetrales, sus funciones, responsabilidades y niveles de autoridad.
5. **Diagnóstico de infraestructura y riesgos:** Resume los resultados del análisis de riesgos y activos críticos, identificando vulnerabilidades relevantes.
6. **Diseño de la arquitectura perimetral:** Describe los elementos físicos y lógicos que componen el perímetro de red, incluyendo diagramas de red, segmentación, ubicaciones de firewalls, etc.
7. **Herramientas tecnológicas:** Enumera los sistemas, plataformas y equipos utilizados para proteger el perímetro (firewalls, IDS, SIEM, VPN, entre otros) y sus configuraciones básicas.
8. **Procedimientos técnicos estándar:** Detalla los pasos operativos para la administración del perímetro, incluyendo configuraciones, reglas, monitoreo, mantenimiento y actualización.
9. **Gestión de incidentes:** Define el protocolo a seguir ante la detección de un incidente de seguridad en el perímetro, incluyendo mecanismos de escalamiento y comunicación.
10. **Indicadores y métricas:** Presenta los KPI definidos para monitorear la eficacia de los controles, así como los formatos de reporte y revisión.

11. **Capacitación y concientización:** Propone un plan básico de formación para los usuarios y el personal técnico respecto a la aplicación del manual y los riesgos asociados.

12. **Mecanismos de revisión y actualización:** Establece la periodicidad de revisión del manual, los criterios para su modificación y los responsables de dicho proceso.

13. **Anexos:** Incluye glosarios, diagramas, formatos, plantillas y cualquier otro material complementario.

Esta estructura no es rígida, y puede ajustarse según las características específicas de cada sede o de la evolución institucional. Lo importante es que el manual proporcione una guía práctica, verificable y contextualizada, que facilite la toma de decisiones técnicas, promueva la mejora continua y contribuya a la cultura de ciberseguridad de la institución.

21. Lecciones aprendidas de experiencias internacionales en controles perimetrales

La implementación de controles perimetrales en instituciones de educación superior no es un fenómeno aislado, sino una tendencia consolidada en universidades de diversos países que buscan fortalecer su postura frente a los crecientes riesgos cibernéticos. Analizar estas experiencias permite extraer aprendizajes valiosos que pueden adaptarse al contexto de la Universidad de Costa Rica.

En Estados Unidos, por ejemplo, universidades como Stanford y MIT han desarrollado centros de operaciones de seguridad (SOC) internos que monitorean constantemente su perímetro digital. Han demostrado que la centralización del monitoreo, el uso de plataformas SIEM y la capacitación continua son pilares fundamentales para la eficacia operativa. En Europa, la Universidad de Cambridge ha adoptado arquitecturas de microsegmentación y principios de “zero trust” para reducir la superficie de ataque.

En América Latina, la Universidad de São Paulo y la Universidad de los Andes en Colombia han publicado políticas específicas sobre control perimetral, destacando la importancia de contar con manuales operativos, equipos multidisciplinarios y participación activa de los usuarios. Estas instituciones han resaltado que una barrera frecuente es la fragmentación organizacional y la resistencia al cambio cultural.

De estas experiencias se pueden extraer lecciones como: la necesidad de contar con liderazgo institucional fuerte, la importancia de visibilizar los riesgos mediante métricas claras, la integración del control perimetral en los planes estratégicos de TIC y la promoción de alianzas con organismos especializados para capacitar y auditar.

22. El papel de la concientización institucional en la protección del perímetro

Además de la tecnología, un componente esencial para el éxito de un esquema de control perimetral es la cultura organizacional. La concientización en ciberseguridad se refiere a la capacidad de los miembros de una institución para reconocer, prevenir y responder adecuadamente a las amenazas informáticas (ENISA, 2021).

En las universidades, donde conviven perfiles diversos —estudiantes, investigadores, personal técnico y administrativo—, los programas de concientización deben ser inclusivos, periódicos y contextualizados. Esto incluye desde campañas educativas sobre el uso responsable del correo institucional hasta simulaciones de incidentes como phishing o accesos no autorizados.

El manual propuesto debe incorporar directrices para el diseño e implementación de programas de concientización adaptados a los riesgos perimetrales, como la protección de contraseñas, la identificación de dispositivos desconocidos conectados a la red o el reporte de actividades anómalas.

Asimismo, se deben generar materiales como infografías, cápsulas informativas, talleres presenciales o virtuales y pruebas de conocimiento que refuercen las prácticas seguras. Estos esfuerzos deben ser coordinados por la

administración y ejecutados en alianza con unidades de tecnología y recursos humanos.

La concientización no es un evento único, sino un proceso continuo que debe alinearse con la evolución de las amenazas, las lecciones aprendidas y los cambios institucionales. Un entorno en el que los usuarios están informados y comprometidos constituye la primera línea de defensa del perímetro digital.

23. Interoperabilidad del manual con otras sedes universitarias

Si bien el presente manual está diseñado para responder a las particularidades de la Sede del Pacífico, su estructura, enfoque metodológico y principios fundamentales pueden ser replicables en otras sedes de la Universidad de Costa Rica. Este potencial de escalabilidad depende de su capacidad para integrarse a una visión institucional más amplia de la ciberseguridad.

La interoperabilidad del manual se refiere a su capacidad para adaptarse a diferentes contextos organizativos y técnicos dentro de la misma universidad. Esto implica que debe utilizar lenguaje estandarizado, buenas prácticas reconocidas y una estructura modular que permita ajustes según los recursos, infraestructura y prioridades de cada sede.

Además, se recomienda que el manual incluya mecanismos de documentación que faciliten la adaptación, como formularios editables, listas de verificación, instructivos y lineamientos que puedan ser reutilizados o modificados. También es deseable promover espacios intersede para compartir experiencias, resolver dudas comunes y fomentar una cultura colaborativa de seguridad digital.

El objetivo no es imponer un modelo único, sino construir una base sólida sobre la cual cada sede pueda edificar su propio sistema de control perimetral. Este enfoque fomenta la autonomía, pero al mismo tiempo asegura coherencia institucional y cumplimiento normativo.

24. Vinculación con políticas nacionales de ciberseguridad

La propuesta de este manual no se construye en un vacío normativo, sino que se alinea con los lineamientos y metas definidas en las políticas nacionales de

ciberseguridad. En Costa Rica, el “Plan Nacional de Ciberseguridad 2023–2027” establece como prioridad la protección de infraestructuras críticas, la creación de capacidades técnicas y el fortalecimiento de la cultura de seguridad digital.

Dicho plan, liderado por el MICITT, sugiere explícitamente la adopción de estándares internacionales como NIST y la implementación de procedimientos estructurados en instituciones públicas. El manual propuesto responde a esta directriz al ofrecer una herramienta práctica para la protección del perímetro, una de las áreas más vulnerables en el ecosistema universitario.

Asimismo, el documento puede contribuir al cumplimiento de marcos internacionales como el Convenio de Budapest sobre Ciberdelincuencia, al establecer mecanismos claros para la trazabilidad, el registro de eventos y la respuesta ante incidentes.

La vinculación con políticas nacionales también refuerza el argumento institucional para priorizar recursos, capacitar personal y justificar la adquisición de tecnología específica. Un manual que responda a los objetivos del país no solo fortalece la postura de la universidad, sino que contribuye a la seguridad digital nacional.

25. Tendencias emergentes en el control perimetral y su impacto en entornos académicos

El control perimetral ha evolucionado de manera significativa durante la última década, impulsado por tendencias tecnológicas globales y el incremento de amenazas cibernéticas dirigidas a instituciones educativas. El perímetro tradicional, basado exclusivamente en firewalls y segmentación estática, ha dado paso a enfoques más dinámicos, inteligentes y orientados al contexto. Según Gartner (2023), las tendencias emergentes en seguridad perimetral se concentran en la integración de analítica avanzada, la automatización y la adopción de arquitecturas distribuidas.

Una de las tendencias más relevantes es el Secure Access Service Edge (SASE), un modelo que combina capacidades de red y seguridad en un servicio basado en la nube. Este enfoque resulta especialmente útil para universidades que

operan sedes descentralizadas, campus distribuidos y modalidades híbridas de trabajo y estudio. SASE integra funciones como firewall en la nube, Zero Trust Network Access (ZTNA) y sistemas de inspección de tráfico cifrado, ofreciendo protección incluso fuera del perímetro físico tradicional (Chandramouli & Rose, 2021).

Otra tendencia clave es el uso de inteligencia artificial aplicada al análisis perimetral. Plataformas modernas combinan machine learning y big data para identificar patrones anómalos en tráfico de red, reducir falsos positivos y predecir comportamientos maliciosos. En entornos universitarios, donde el tráfico es elevado, variado y difícil de clasificar, estas herramientas permiten una gestión más efectiva del perímetro sin aumentar la carga operativa sobre el personal técnico.

Asimismo, se observa una creciente adopción de TLS Inspection y Deep Packet Inspection (DPI) para inspeccionar tráfico cifrado, dado que más del 80% del tráfico malicioso circula mediante HTTPS (ENISA, 2023). Su implementación debe considerar tanto la capacidad tecnológica como las implicaciones legales respecto a privacidad y manejo de datos.

En conjunto, estas tendencias emergentes representan oportunidades para fortalecer los controles perimetrales en instituciones como la Sede del Pacífico de la UCR, siempre que se integren de manera contextualizada, gradual y bajo lineamientos normativos vigentes.

26. Arquitecturas Zero Trust y su relación con el control perimetral

El paradigma Zero Trust se ha consolidado como un enfoque indispensable en estrategias modernas de ciberseguridad. A diferencia de los modelos tradicionales, que confiaban en usuarios y dispositivos una vez dentro del perímetro, Zero Trust se basa en el principio de “nunca confiar, siempre verificar”, independientemente de la ubicación o el origen del acceso (NIST SP 800-207).

Este modelo redefine el control perimetral al desplazar parte de la seguridad desde el borde de la red hacia cada usuario, dispositivo, aplicación y flujo de datos. En universidades, donde existe una alta rotación de usuarios, dispositivos

personales y redes abiertas, Zero Trust puede reducir riesgos asociados al acceso lateral, la suplantación de identidad y la explotación de vulnerabilidades internas.

Los elementos centrales del enfoque Zero Trust incluyen:

- Autenticación multifactor reforzada (MFA): Verificación continua de identidad.
- Microsegmentación avanzada: Limitación del movimiento lateral incluso dentro de subredes internas.
- Validación continua del estado de los dispositivos: Acceso condicionado a nivel de parcheo, antivirus o postura de seguridad.
- Políticas de acceso basadas en contexto: Consideración de variables como ubicación, horario, reputación del tráfico y nivel de riesgo.

La adopción de Zero Trust no implica eliminar el perímetro, sino ampliarlo hacia un modelo distribuido, en el que cada componente se convierte en un microperímetro. De acuerdo con Moreira y Santana (2022), este enfoque ha sido especialmente efectivo en instituciones de educación superior que enfrentan amenazas internas y externas simultáneas.

Integrar principios Zero Trust en el manual de control perimetral permitirá armonizar las prácticas tradicionales con estrategias modernas, creando un entorno más seguro, resiliente y adaptable para la UCR.

27. Automatización y orquestación de la seguridad perimetral

La automatización, a través de plataformas SOAR (Security Orchestration, Automation and Response), se ha posicionado como un componente clave para mejorar la eficiencia operacional en la gestión perimetral. La creciente cantidad de alertas, eventos y registros generados por herramientas como firewalls, IDS/IPS, SIEM y gateways hace que la supervisión humana exclusiva resulte insuficiente y propensa a errores (ISACA, 2021).

- SOAR permite automatizar tareas como:
- Bloqueo automático de direcciones IP maliciosas.
- Actualización de listas negras y reglas de firewall.

- Respuestas rápidas ante eventos repetitivos.
- Correlación de alertas entre diversas fuentes.
- Generación automática de reportes e indicadores.

Para universidades con recursos técnicos limitados, como la Sede del Pacífico, la automatización puede mejorar significativamente los tiempos de respuesta y reducir la fatiga de alerta del personal técnico. Además, plataformas de orquestación pueden estandarizar procedimientos, alineándolos con los lineamientos del manual y garantizando su cumplimiento cotidiano.

La automatización también favorece la trazabilidad y la auditoría, al documentar cada evento y acción tomada. Esto contribuye al cumplimiento normativo y a la mejora continua, elementos esenciales de la propuesta metodológica basada en NIST**.**

28. Conclusión del marco teórico

A lo largo de este marco teórico se ha argumentado la importancia de contar con un manual de control perimetral contextualizado, técnico y alineado con buenas prácticas internacionales. Se han abordado los conceptos fundamentales de ciberseguridad institucional, los marcos normativos más relevantes, las metodologías de análisis de riesgos, la gestión del cambio y la estructura sugerida del documento.

También se ha profundizado en aspectos clave como la concientización, la interoperabilidad entre sedes, la alineación con políticas nacionales y la evaluación mediante indicadores. Todo esto con el objetivo de construir una herramienta práctica que contribuya no solo a la protección tecnológica, sino a una cultura universitaria más resiliente frente a los desafíos del entorno digital.

Este marco teórico sirve como base conceptual y técnica para el desarrollo del manual en fases posteriores del proyecto, orientando las decisiones de diseño, implementación y evaluación. Representa un esfuerzo por vincular la teoría con la práctica, la academia con la gestión institucional, y la seguridad con el servicio educativo de calidad.

CAPITULO III. MARCO METODOLÓGICO

3.1 Tipo de investigación

3.1.1 Finalidad

La finalidad de una investigación puede clasificarse en teórica o aplicada. Según Bernal (2016), una investigación teórica busca ampliar el conocimiento existente sin una aplicación inmediata, concentrándose en el desarrollo conceptual. Por su parte, una investigación aplicada tiene como propósito resolver problemas concretos mediante el uso del conocimiento, generando productos o soluciones específicas para un contexto determinado.

En este TFG, la finalidad es aplicada, ya que se orienta a resolver un problema real en la Sede del Pacífico de la Universidad de Costa Rica: la ausencia de procedimientos estandarizados para el control perimetral de ciberseguridad. El producto final será un manual operativo que podrá implementarse directamente, siguiendo lineamientos del Marco NIST.

3.1.2 Enfoque sistemático

El enfoque sistemático se puede clasificar en macro, meta, meso o micro. De acuerdo con Hernández, Fernández y Baptista (2022), un enfoque macro abarca un ámbito amplio nacional o internacional, un enfoque meta se centra en sectores o áreas específicas, el enfoque meso analiza unidades organizacionales intermedias, por ejemplo, una institución o sede, y el enfoque micro estudia procesos o unidades muy específicas y delimitadas.

En este TFG, el enfoque es meso, porque se dirige a una unidad organizacional específica (la Sede del Pacífico de la UCR) pero con la posibilidad de que el manual sea replicado en otras sedes universitarias.

3.1.3 Naturaleza

La naturaleza de la investigación puede ser cuantitativa, cualitativa o mixta. Hernández et al. (2022) definen la investigación cuantitativa como aquella que recolecta y analiza datos numéricos para probar hipótesis o responder preguntas, mientras que la cualitativa se centra en comprender fenómenos a partir de

información no numérica, interpretando experiencias, percepciones y contextos. Una naturaleza mixta combina ambos enfoques.

Este TFG tiene una naturaleza cualitativa con elementos cuantitativos. Predomina lo cualitativo porque se realizará un análisis profundo de procedimientos, configuraciones y percepciones del personal técnico; sin embargo, se incorporarán métricas e indicadores de seguridad perimetral para complementar el diagnóstico

3.1.4 Carácter

El carácter de una investigación describe la manera en que aborda el problema.

Según Sampieri et al. (2022), puede ser descriptivo caracteriza fenómenos o situaciones, explicativo que busca causas y relaciones, causal que determina la relación causa-efecto, comprensivo que interpreta significados o una combinación de estos.

En este TFG, el carácter es descriptivo y propositivo. Es descriptivo porque documentará el estado actual de la seguridad perimetral en la sede, y propositivo porque generará una solución concreta, el manual de procedimientos que mejore la gestión y protección del perímetro de red.

3.2 Administración y abordaje del proyecto objeto

3.2.1 Descripción de supuestos

Según Kerzner (2022), la administración de un proyecto consiste en planificar, organizar y supervisar los recursos, tiempos y actividades necesarias para cumplir con los objetivos, considerando supuestos, restricciones y riesgos. El abordaje del proyecto define la estrategia de ejecución, las fases de trabajo y la coordinación entre los actores involucrados.

En este TFG, la administración y el abordaje contemplan:

- **Supuestos:**

    1. El personal técnico de la Sede del Pacífico colaborará activamente en entrevistas y validaciones.

2. No habrá cambios significativos en la infraestructura de red durante el desarrollo del TFG.
3. Se permitirá el acceso a documentación interna relevante para el diagnóstico.

3.2.2 Restricciones y riesgos

- **Restricciones:**
    1. El estudio se limita a la ciberseguridad perimetral, excluyendo seguridad física y de dispositivos endpoint.
    2. Los recursos disponibles serán únicamente los que posee actualmente la sede.
    3. El trabajo de campo estará supeditado al calendario académico y disponibilidad de los actores clave.
- **Riesgos:**
    1. Posible resistencia al cambio organizacional por parte de personal técnico o administrativo.
    2. Cambios en las políticas institucionales que modifiquen el alcance del manual.
    3. Limitaciones para la recolección de datos debido a restricciones de confidencialidad.

Este abordaje se estructurará en tres fases: diagnóstico, diseño y validación del manual, con revisiones periódicas junto al tutor y el personal técnico de la sede.

3.3 Sujetos y fuentes de información

3.3.1 Sujetos de Información

De acuerdo con Hernández, Fernández y Baptista (2022), los sujetos de información son las personas, organizaciones o unidades de estudio de las que se

obtienen los datos necesarios para la investigación.
En este TFG, los sujetos de información serán:

- Personal técnico de TI de la Sede del Pacífico de la UCR.
- Administradores de red y encargados de seguridad informática.
- Representantes administrativos con funciones relacionadas a TIC y ciberseguridad.

Estos sujetos se seleccionan por su conocimiento directo de la gestión del perímetro de red y su papel en la implementación de políticas de seguridad.

3.3.2 Fuentes de información

Según Bernal (2016), las fuentes se clasifican en:

- **Primarias:** información obtenida directamente por el investigador, como entrevistas, encuestas y observaciones.
- **Secundarias:** datos recopilados por otros autores o instituciones, como informes, normativas y literatura académica.
- **Terciarias:** compilaciones o índices que resumen información proveniente de fuentes primarias y secundarias.

En este TFG:

- **Primarias:** entrevistas semiestructuradas y cuestionarios aplicados al personal técnico y administrativo.
- **Secundarias:** políticas institucionales, reportes de incidentes, configuraciones de red, y literatura técnica sobre NIST e ISO.
- **Terciarias:** bases de datos académicas y repositorios de organismos especializados (NIST, ENISA, CONARE, MICITT).

3.4 Muestreo

3.4.1 Población y muestreo

Según Sampieri et al. (2022), el muestreo es el proceso de selección de un conjunto representativo de la población para obtener información relevante en un estudio. Puede ser probabilístico cuando todos los elementos de la población tienen la misma probabilidad de ser seleccionados o no probabilístico cuando la selección se basa en criterios del investigador.

3.4.2 Tipo de muestreo

En este TFG se aplicará un muestreo no probabilístico por criterio (o intencional), eligiendo participantes que tengan experiencia directa en la gestión del perímetro de red en la Sede del Pacífico. Esto garantiza que la información provenga de actores con conocimiento técnico y experiencia en el área.

3.5 Diseño de técnicas e instrumentos para recolectar información

3.5.1 Detalle de técnica e instrumentos de aplicación

- Entrevistas semiestructuradas para obtener información detallada sobre los procedimientos y configuraciones actuales.
- Cuestionarios con preguntas cerradas y abiertas para complementar los datos cualitativos con métricas cuantificables.
- Listas de chequeo para evaluar configuraciones y cumplimiento de buenas prácticas de seguridad perimetral.

3.5.2 Detalle de la aplicación de técnicas e instrumentos

- Guías de entrevista validadas por el tutor.
- Formularios digitales para el registro y análisis de datos.

3.6 Determinación de variables

3.6.1 Clasificación

Las variables pueden clasificarse en:

- Conceptuales: Definición teórica basada en literatura especializada.

- Operacionales: Forma en que será aplicada o medida en el contexto del TFG.
- Instrumentales: Herramienta o instrumento utilizado para recolectar o gestionar la información de la variable.

3.6.2 Definición

La identificación de variables es fundamental para precisar lo que se observará y medirá en el desarrollo del TFG. De acuerdo con Hernández, Fernández y Baptista (2022), una variable es "una propiedad que puede adquirir diferentes valores y cuya variación es objeto de análisis en una investigación".

3.6.3 Cuadro o matriz de las variables

En el presente trabajo se identifican las siguientes variables relacionadas con los objetivos específicos del TFG:

Objetivos	Variable	Conceptualmente	Operacional	Instrumental
Analizar los referentes teóricos y normativos en materia de control perimetral y marcos de ciberseguridad.	Marco normativo de ciberseguridad	Conjunto de normas, estándares y buenas prácticas que orientan la protección de la infraestructura tecnológica.	Identificar y clasificar fuentes normativas (NIST, ISO, CONARE, entre otros).	Revisión documental, matriz comparativa en Excel.
Diagnosticar el estado actual de los controles perimetrales en la Sede del Pacífico de la Universidad de Costa Rica.	Diagnostico estado actual	Grado en que una organización ha implementado prácticas estructuradas de protección del perímetro de red.	Evaluación de prácticas existentes, configuraciones, roles y procedimientos, mediante un cuestionario en word	Lista de chequeo, entrevistas, cuestionarios digitales.
Diseñar un manual de procedimientos técnicos y administrativos para la gestión perimetral.	Manual de procedimiento	Documento técnico que sistematiza acciones, roles y procedimientos para proteger el perímetro de red	Redacción del manual con base en el diagnóstico, el marco teórico y el marco NIST.	Documento Word

CAPÍTULO IV. ANÁLISIS DE RESULTADOS

4.1 Resultados de la aplicación del cuestionario

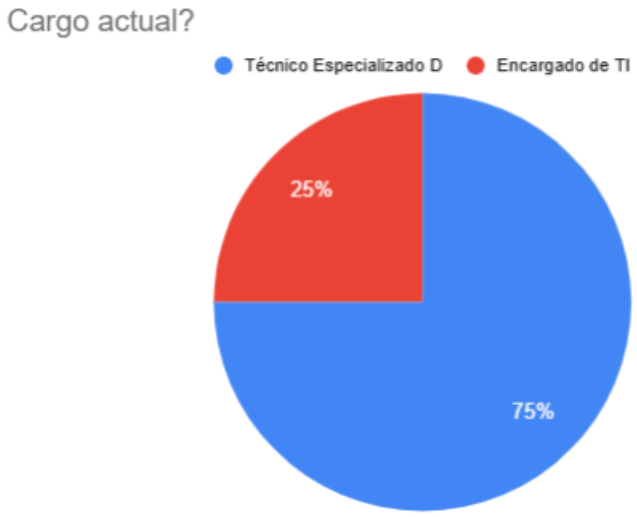
En este capítulo se presentan y analizan los resultados del Cuestionario para Diagnóstico de Controles Perimetrales de Ciberseguridad aplicado al personal técnico de la Sede del Pacífico de la Universidad de Costa Rica. El propósito del análisis es diagnosticar el estado actual de los controles perimetrales, identificar fortalezas y brechas y generar insumos directos para el diseño del Manual de Procedimientos de Control Perimetral de Ciberseguridad basado en el Marco NIST, en coherencia con los objetivos del Trabajo Final de Graduación.

Dado que la población encuestada corresponde a personal con responsabilidades directas en infraestructura y seguridad, los resultados constituyen una fuente cualitativa y cuantitativa confiable para comprender la madurez actual del perímetro de red en las funciones de Identificar, Proteger, Detectar, Responder y Recuperar, establecidas por el NIST.

A continuación, se presenta el análisis pregunta por pregunta, acompañado de la referencia a la figura correspondiente, sugerida en formato de gráfico circular o de barras según la naturaleza de las respuestas.

Figura 2.

Distribución del cargo del personal encuestado

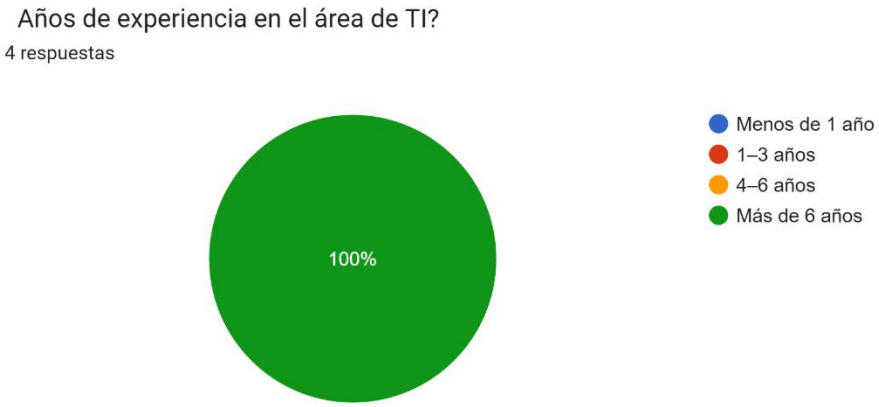


Nota: Imagen de fuente propia. Que representa la familiaridad de los colaboradores con los objetivos de la Auditoria de Tecnologías de Información en la UCR sede del Pacífico.

El 75% de las personas encuestadas ocupa el puesto de Técnico Especializado D, mientras que el 25% corresponde al Encargado de TI. Esta composición evidencia que las respuestas provienen directamente de los perfiles responsables de la operación y administración de la infraestructura tecnológica de la sede, lo que otorga pertinencia técnica al diagnóstico y lo alinea con la realidad operativa del perímetro de red.

Figura 3.

Años de experiencia en TI del personal encuestado.

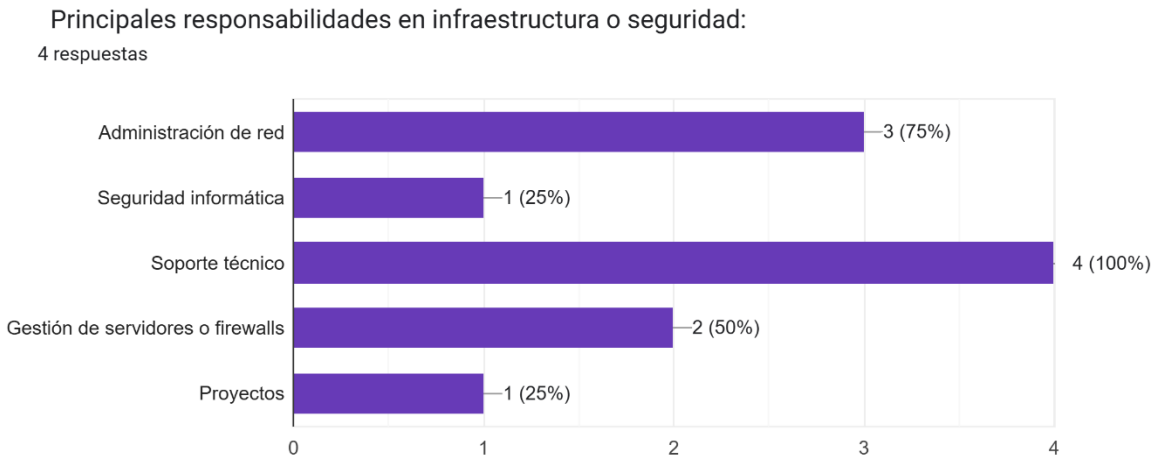


Nota: Imagen de fuente propia. Muestra la cantidad de años de experiencia profesional del personal técnico participante.

El 100% del personal reporta más de 6 años de experiencia en el área de TI. Este hallazgo confirma que la percepción recogida proviene de personal con trayectoria consolidada, capaz de identificar riesgos, fortalezas y debilidades de los controles perimetrales, reforzando la validez de los insumos para el diseño del manual.

Figura 4.

Responsabilidades principales del personal encuestado.



Nota: Imagen de fuente propia. Representa las responsabilidades operativas y de infraestructura reportadas por los funcionarios encuestados**.**

Las respuestas muestran responsabilidades distribuidas entre soporte técnico, administración de red, gestión de servidores y seguridad informática, en algunos casos combinadas. Esto indica que el mismo grupo atiende funciones operativas y estratégicas, lo que puede generar sobrecarga, pero también facilita la implementación de un manual que integre procedimientos técnicos y administrativos en un solo instrumento.

Figura 5.

Inventario de activos tecnológicos perimetrales.

Nota: Imagen de fuente propia. Describe la percepción del personal sobre la existencia de inventarios actualizados de activos perimetrales.

El 100% de los encuestados indica que existe un inventario completo y actualizado de los activos conectados al perímetro de red. Este resultado representa una fortaleza clave alineada con la función Identificar del NIST, ya que disponer de un inventario actualizado es la base para gestionar riesgos y asignar controles adecuados sobre los activos críticos.

Figura 6.

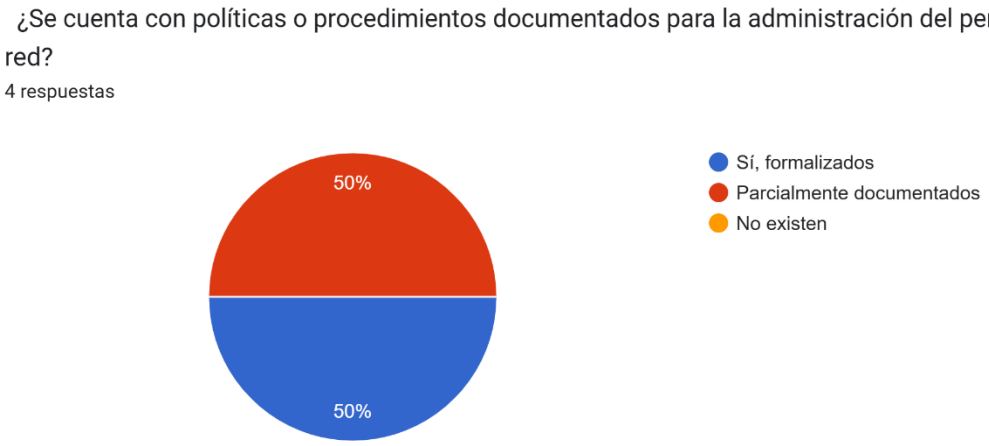
Clasificación de activos por criticidad.

Nota: Imagen de fuente propia. Expone si los activos tecnológicos de la sede cuentan con clasificación de riesgo o criticidad

El 50% señala que el inventario no incluye clasificación de criticidad, un 25% indica que sí se realiza y un 25% que se encuentra en proceso. Aunque se cuenta con inventario, la ausencia o parcialidad en la clasificación limita la priorización de controles y la alineación formal con metodologías de gestión de riesgos como ISO/IEC 27005 y el propio NIST. Esto evidencia una primera brecha que el manual debe subsanar mediante lineamientos claros de categorización de activos.

Figura 7.

Grado de documentación de políticas perimetrales.

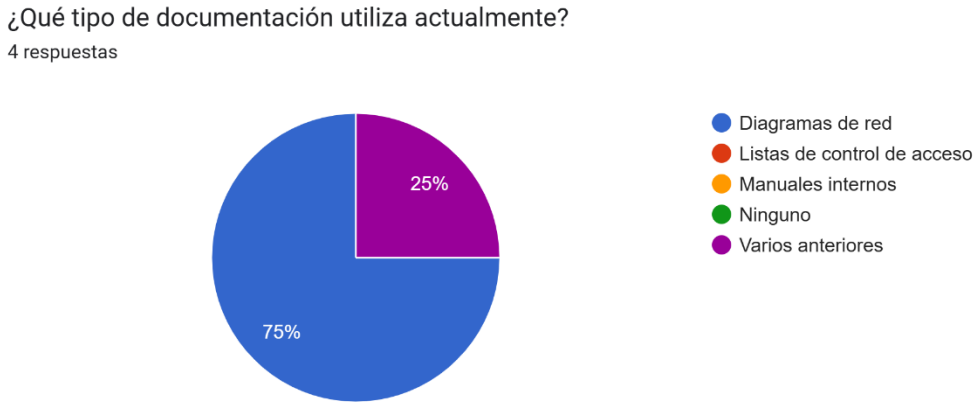


Nota: Imagen de fuente propia. Resume el grado en que el personal reconoce la existencia de documentación formal de procedimientos perimetrales.

El 50% de los participantes indica que existen políticas o procedimientos formalizados, mientras que el otro 50% reporta documentación solo parcial. Esto refleja la existencia de esfuerzos previos, pero también una falta de estandarización y consolidación institucional. El manual propuesto se vuelve necesario para unificar criterios, formalizar procesos y reducir la dependencia de prácticas informales.

Figura 8.

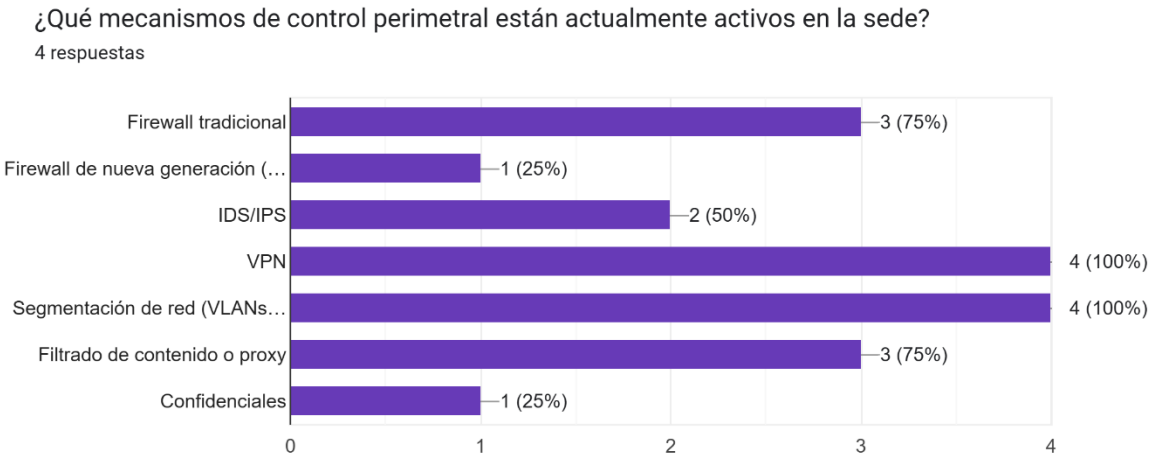
Tipos de documentación vigente.



Nota: Imagen de fuente propia. Señala los tipos de documentación utilizados por el personal técnico para gestionar el perímetro de red.

El 75% menciona principalmente diagramas de red, mientras que el 25% alude a una combinación de documentación técnica más amplia. La predominancia de diagramas indica la presencia de insumos visuales útiles, pero también sugiere que estos deben integrarse en un marco procedimental más robusto, que describa responsabilidades, flujos de aprobación, cambios y controles, como se plantea en la propuesta de manual.

Figura 9. Controles perimetrales implementados.

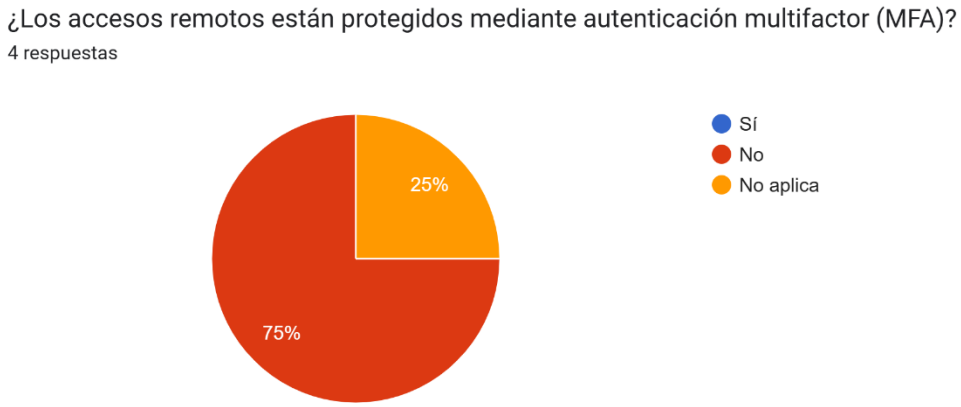


Nota: Imagen de fuente propia. Presenta los controles de seguridad perimetral actualmente implementados en la sede.

Todas las respuestas señalan la existencia de firewall, VPN y segmentación de red (VLAN/DMZ); algunos encuestados mencionan también IDS/IPS, filtrado de contenido y, en un caso, firewall de nueva generación. Esto evidencia una base tecnológica adecuada, coherente con prácticas recomendadas, pero sin un nivel uniforme de madurez. El manual deberá estandarizar el uso, configuración mínima y monitoreo de estos controles para asegurar su efectividad.

Figura 10.

Protección de accesos remotos con MFA.

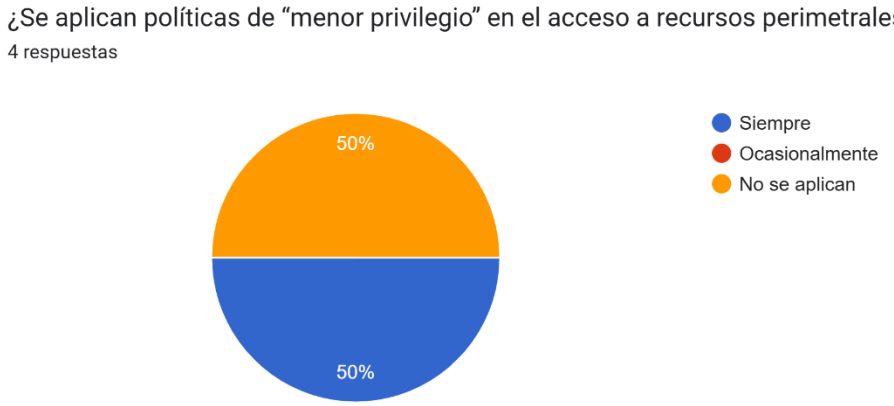


Nota: Imagen de fuente propia. Indica la implementación o ausencia de mecanismos MFA en accesos remotos al entorno institucional.

El 75% indica que no se utiliza MFA en accesos remotos y el 25% señala que no aplica. En la práctica, el resultado evidencia una ausencia de autenticación multifactor como control obligatorio, lo cual representa una brecha crítica frente a lineamientos actuales de seguridad, Zero Trust y funciones de Proteger del NIST. Este hallazgo justifica que el manual incluya la implementación progresiva de MFA como control prioritario.

Figura 11.

Aplicación del principio de menor privilegio.

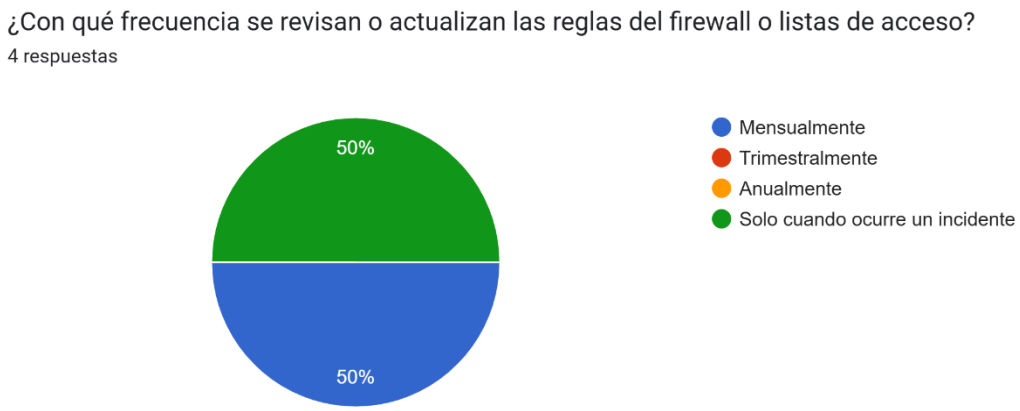


Nota: Imagen de fuente propia. Refleja el grado de aplicación del principio de menor privilegio en la administración de accesos.

El 50% afirma que el principio de menor privilegio se aplica siempre, mientras que el 50% indica que no se aplica. Esta disparidad muestra inconsistencia en la gestión de permisos sobre recursos perimetrales y sugiere la necesidad de procedimientos formales para la asignación, revisión y revocación de accesos, en concordancia con buenas prácticas NIST e ISO/IEC 27001.

Figura 12.

Frecuencia de revisión de reglas de firewall.

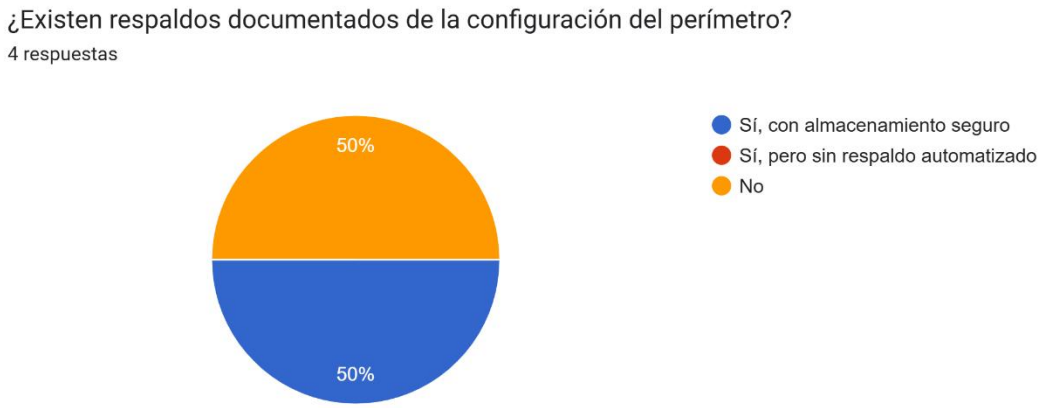


Nota: Imagen de fuente propia. Muestra la periodicidad con la que el personal revisa y actualiza las reglas del firewall perimetral.

El 50% reporta revisiones mensuales, mientras que el otro 50% únicamente lo hace cuando ocurre un incidente. Esto refleja coexistencia de un enfoque preventivo y otro marcadamente reactivo. El manual debe definir una frecuencia mínima obligatoria, basada en el nivel de criticidad de los servicios, para asegurar la actualización oportuna de reglas.

Figura 13.

Existencia de respaldos de configuración.

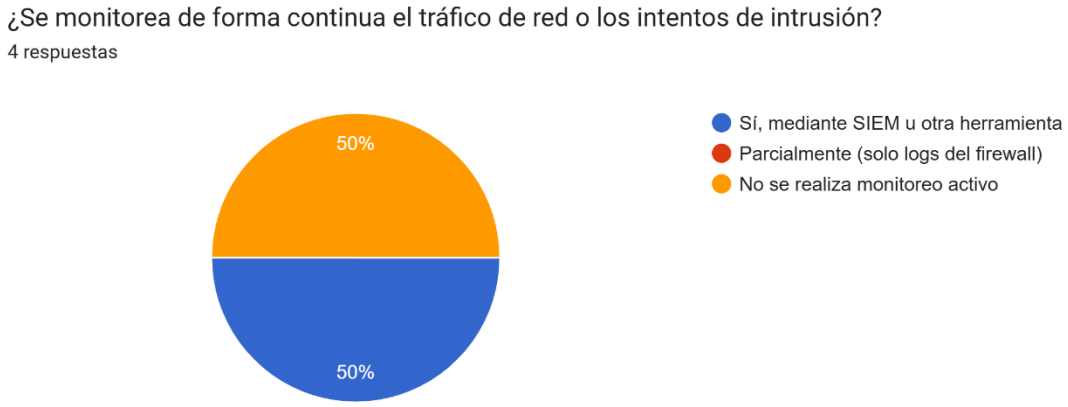


Nota: Imagen de fuente propia. Informa si los respaldos de configuraciones críticas del perímetro se realizan y almacenan adecuadamente.

El 50% indica que sí existen respaldos con almacenamiento seguro, mientras que el 50% señala que no se cuenta con ellos. Esta situación plantea un riesgo directo para la función de Recuperar, ya que un incidente en equipos perimetrales podría prolongarse por falta de configuraciones respaldadas. El manual deberá establecer la obligación de generar y resguardar respaldos periódicos verificados.

Figura 14.

Monitoreo del tráfico perimetral.

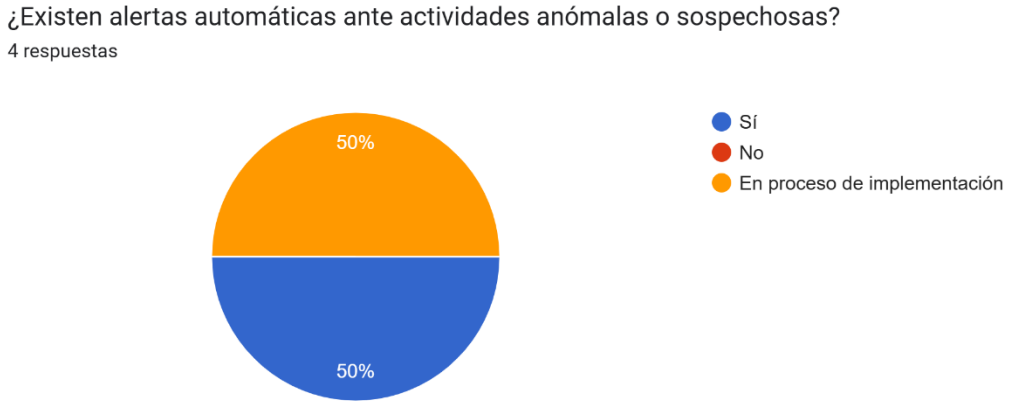


Nota: Imagen de fuente propia. Describe si la sede cuenta con monitoreo y análisis continuo del tráfico en el perímetro

El 50% señala que se realiza monitoreo mediante herramientas como SIEM u otras, mientras que el 50% indica que no se realiza monitoreo activo. Esta dualidad evidencia una implementación parcial de la función Detectar, con dependencia de prácticas individuales. El manual deberá formalizar el monitoreo continuo y la centralización de eventos relevantes.

Figura 15.

Implementación de alertas automáticas.

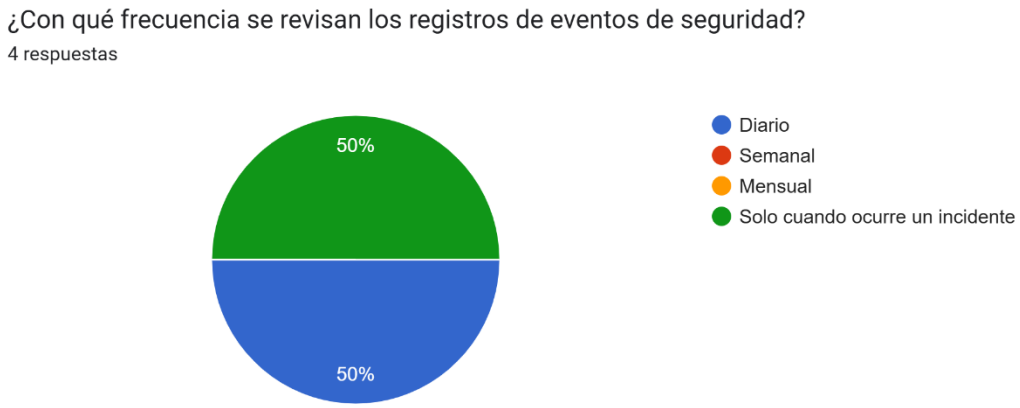


Nota: Imagen de fuente propia. Representa la existencia de alertas automáticas ante actividades anómalas en el entorno perimetral

El 50% reporta que sí existen alertas automáticas, y el 50% indica que estas están en proceso de implementación. El resultado es positivo, pero muestra una etapa de transición, por lo que el manual debe incorporar lineamientos específicos sobre umbrales, responsables de atención y tiempos de respuesta ante alertas.

Figura 16.

Revisión de registros de seguridad.

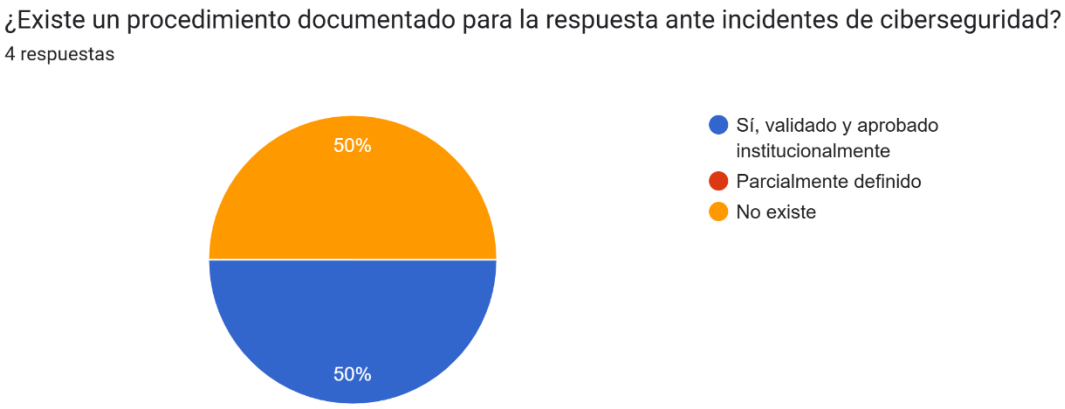


Nota: Imagen de fuente propia. Expone cada cuánto tiempo el personal revisa los registros de eventos de seguridad.

El 50% revisa los registros a diario, mientras que el 50% lo hace solo cuando ocurre un incidente. De nuevo se evidencia la coexistencia de prácticas maduras con otras reactivas. El manual deberá establecer una rutina formal de revisión, con evidencia documental y criterios de priorización.

Figura 17.

Procedimientos de respuesta a incidentes.



Nota: Imagen de fuente propia. Indica si la organización cuenta con procedimientos formalizados para la atención de incidentes de ciberseguridad.

El 50% indica que no existe procedimiento documentado, mientras que el 50% señala que sí existe y está validado institucionalmente. Esta diferencia refleja falta de conocimiento homogéneo o aplicación desigual del procedimiento. El manual propuesto debe articularse con los lineamientos institucionales existentes y clarificar roles, flujos de escalamiento y pasos mínimos a seguir ante incidentes perimetrales.

Figura 18.

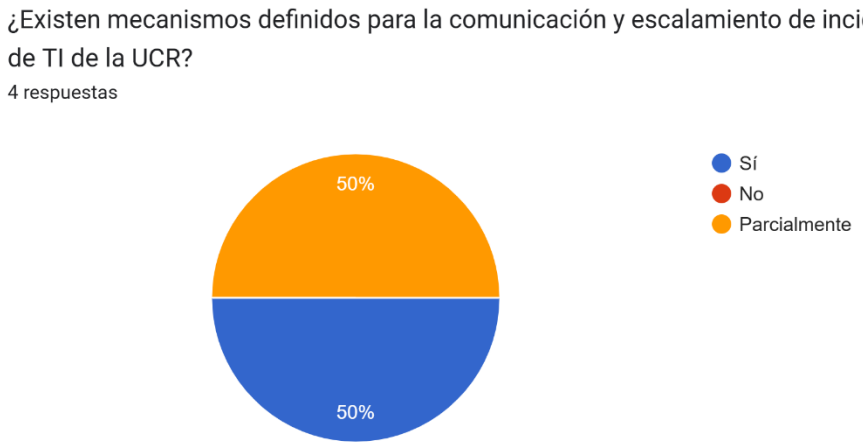
Simulacros de respuesta a incidentes.

Nota: Imagen de fuente propia. Señala si el personal técnico participa en ejercicios o simulacros de respuesta a incidentes.

El 75% del personal técnico nunca ha participado en simulacros de respuesta a incidentes, mientras que solo el 25% indica haber participado recientemente. Esto muestra una debilidad importante en la función Responder, ya que la efectividad de los protocolos depende de la práctica. El manual deberá incluir la planificación periódica de simulacros y su documentación.

Figura 19.

Mecanismos de comunicación y escalamiento.

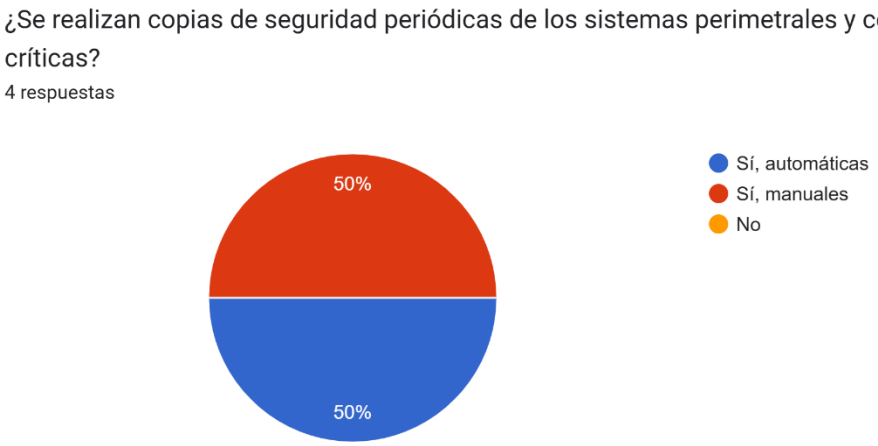


Nota: Imagen de fuente propia. Muestra la percepción del personal respecto a la claridad de los mecanismos de comunicación con TI central.

El 50% considera que existen mecanismos parcialmente definidos, mientras que el 50% indica que sí están definidos. Aunque ningún encuestado señala ausencia total, la percepción de parcialidad evidencia oportunidades para formalizar canales, responsables y tiempos de respuesta conjuntos con el nivel central, aspecto que debe quedar claramente descrito en el manual.

Figura 20.

Copias de seguridad perimetrales.

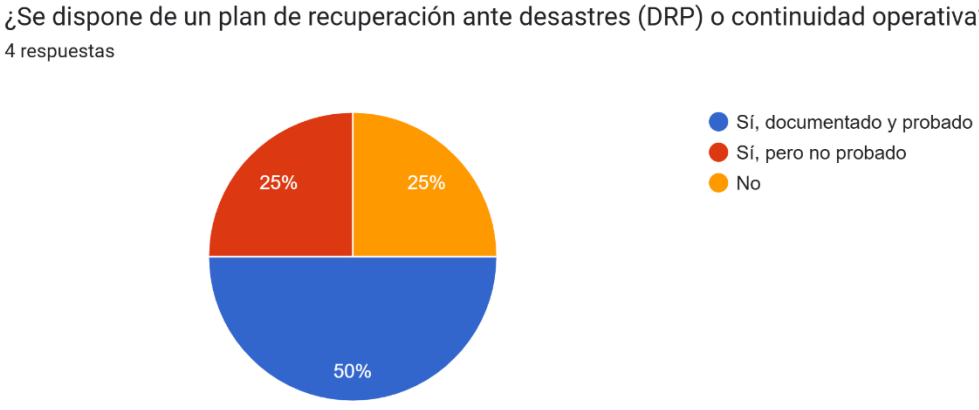


Nota: Imagen de fuente propia. Expone si la sede realiza copias de seguridad de los sistemas y configuraciones del perímetro

El 100% indica que sí se realizan copias de seguridad, distribuidas entre esquemas manuales (50%) y automáticos (50%). Este resultado es una fortaleza asociada a la función Recuperar, aunque se requiere estandarizar periodicidad, verificación y resguardo de dichas copias dentro de los procedimientos formales.

Figura 21.

Disponibilidad de DRP/continuidad operativa.

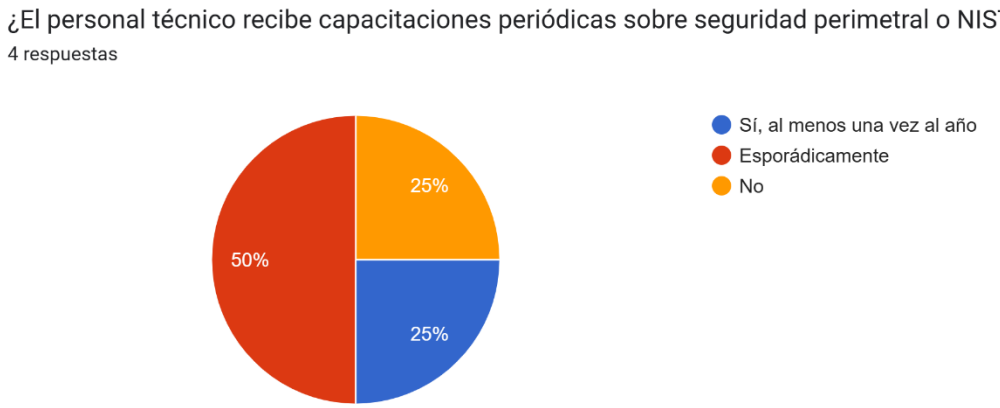


Nota: Imagen de fuente propia. Representa la percepción del personal sobre la existencia y grado de aplicación del DRP institucional.

El 50% señala que existe un plan documentado y probado, el 25% que existe, pero no ha sido probado, y el 25% que no cuenta con plan. Esto indica avances relevantes, pero con brechas en validación y cobertura, por lo que el manual deberá integrar la relación entre controles perimetrales y el DRP, asegurando pruebas periódicas y claridad en responsabilidades.

Figura 22.

Capacitaciones en seguridad perimetral.



Nota: Imagen de fuente propia. Indica la frecuencia con la que el personal recibe capacitación formal en temas de ciberseguridad perimetral.

El 25% indica recibir capacitación al menos una vez al año, el 50% señala capacitaciones esporádicas y el 25% no recibe capacitación. La tendencia muestra que la formación no es sistemática, lo cual impacta directamente la correcta operación de controles perimetrales. El manual deberá ir acompañado de un plan de capacitación continua, alineado con el marco NIST y políticas institucionales.

Figura 23.

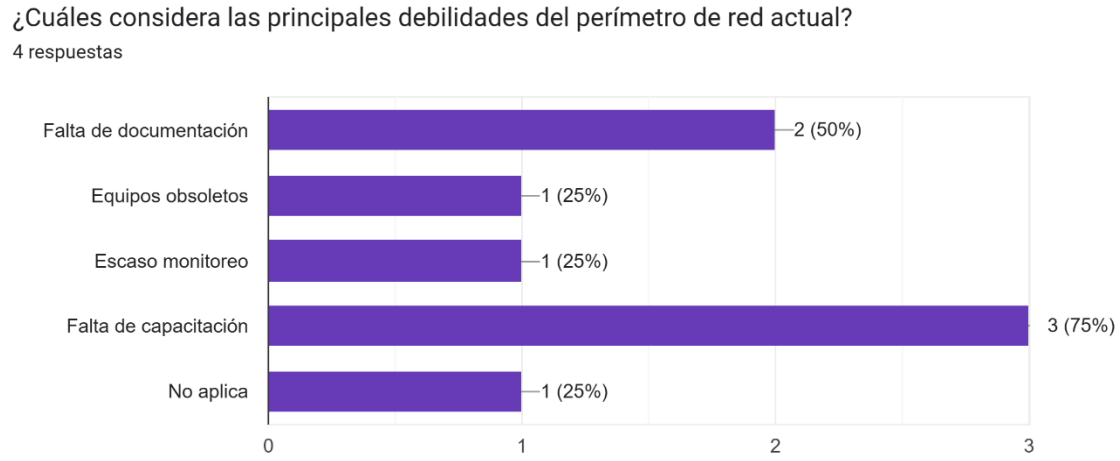
Nivel percibido de cultura de ciberseguridad.

Nota: Imagen de fuente propia. Describe el nivel de cultura de ciberseguridad percibido dentro de la sede.

El 50% percibe una cultura de ciberseguridad media, el 25% alta y el 25% baja. La distribución sugiere una cultura en desarrollo, con esfuerzos visibles, pero aún heterogéneos. El manual de procedimientos se configura como herramienta clave para consolidar prácticas, estandarizar criterios y fortalecer dicha cultura en toda la sede.

Figura 24.

Principales debilidades del perímetro de red actual



Nota: Imagen de fuente propia. Resume las debilidades principales identificadas mediante las respuestas abiertas del cuestionario.

Dos de los encuestados señalan explícitamente la falta de documentación, y tres hacen referencia directa a la necesidad de mayor capacitación. Estos hallazgos confirman la urgencia de contar con un manual estructurado, acompañado de procesos de actualización y formación continua.

Síntesis de las preguntas abiertas mejoras priorizadas para fortalecer el perímetro y sobre los Comentarios o recomendaciones adicionales

Las respuestas se concentran en tres líneas principales, capacitación técnica sistemática del personal, implementación de autenticación multifactor (MFA)y auditorías periódicas sobre configuración y cumplimiento. La coincidencia entre debilidades y mejoras propuestas refuerza la necesidad de que el manual incluya apartados específicos sobre: requisitos de MFA, programa de capacitación, auditorías internas y revisión periódica de controles.

Los comentarios finales insisten en reforzar el uso de MFA en accesos críticos, fortalecer la capacitación del personal técnico. Este énfasis reiterado valida que la propuesta de manual no solo debe ser normativa, sino acompañarse de un plan de implementación práctica, que incluya actualizaciones tecnológicas y desarrollo de competencias.

Síntesis del análisis de resultados obtenidos

El análisis de los resultados obtenidos a partir del cuestionario aplicado al personal técnico de la Sede del Pacífico de la Universidad de Costa Rica permite evidenciar un panorama mixto en relación con la gestión del control perimetral de ciberseguridad. Por un lado, se identifican avances significativos en la infraestructura tecnológica y la adopción de ciertos controles básicos, tales como la existencia de firewalls, segmentación de red, uso de VPN y realización de respaldos de información. Estos elementos constituyen un punto de partida sólido y demuestran que la sede cuenta con una base técnica favorable para fortalecer su postura de seguridad.

Sin embargo, los resultados también revelan brechas relevantes que limitan la madurez institucional en materia de ciberseguridad perimetral. En particular, se observa la ausencia de una clasificación formal de activos según su nivel de criticidad, lo cual dificulta la priorización de esfuerzos de protección y la gestión efectiva de riesgos. Este aspecto resulta crucial dentro de la función Identificar del marco NIST, que establece como requisito fundamental el conocimiento detallado de los activos, su valor para la organización y su nivel de exposición a amenazas.

Asimismo, la documentación de políticas y procedimientos operativos se presenta de manera parcial o informal, dependiente en gran medida de la experiencia del personal técnico. Esta situación genera vulnerabilidades asociadas a la falta de estandarización y a la dependencia del conocimiento individual. En este sentido, el desarrollo del Manual de Procedimientos de Control Perimetral se justifica como un instrumento indispensable para formalizar las prácticas existentes, establecer responsabilidades claras y garantizar la continuidad operativa ante cambios de personal o incidentes imprevistos.

Otro hallazgo de relevancia se relaciona con la protección de los accesos remotos. La ausencia de mecanismos de autenticación multifactor (MFA) representa una debilidad crítica frente a los estándares actuales de seguridad y a la función Proteger del NIST, que enfatiza la necesidad de controles robustos de acceso y autenticación. La implementación progresiva de este tipo de mecanismos debe ser prioritaria dentro del manual, dado que permitiría reducir la superficie de exposición a ataques externos.

En cuanto a las funciones de Detección y Respuesta, los datos reflejan que, aunque existe cierto monitoreo del tráfico y generación de alertas, estas prácticas no se aplican de forma uniforme ni continua. La revisión de registros de eventos y las pruebas de respuesta ante incidentes se realizan de manera reactiva, generalmente posterior a la ocurrencia de un evento. Esto sugiere la necesidad de establecer rutinas formales de supervisión, análisis de logs y simulacros de incidentes que fortalezcan la capacidad institucional para detectar y responder de forma oportuna.

El componente humano emerge como un eje transversal del diagnóstico. La mayoría de los encuestados manifiesta la necesidad de fortalecer la capacitación técnica y la cultura de ciberseguridad entre los funcionarios de la sede. Este hallazgo reafirma que la ciberseguridad no depende únicamente de la infraestructura tecnológica, sino también del compromiso y la concientización de las personas que operan los sistemas. En correspondencia con lo planteado por ENISA (2021) y García & Herrera (2021), el manual deberá incorporar estrategias de formación continua y programas de sensibilización que promuevan buenas prácticas y fomenten una cultura institucional sólida en torno a la seguridad digital.

En conjunto, los hallazgos evidencian que la Sede del Pacífico cuenta con los recursos técnicos mínimos necesarios para implementar controles perimetrales efectivos, pero requiere avanzar hacia una madurez organizacional y procedimental más alta. El manual propuesto surge, por tanto, como una herramienta estratégica para consolidar las funciones del NIST Identificar, Proteger, Detectar, Responder y Recuperar, dentro de un marco de gobernanza coherente, documentado y sostenible. Su implementación permitirá no solo estandarizar las prácticas operativas, sino también integrar la gestión del perímetro a la planificación institucional, contribuyendo al fortalecimiento de la resiliencia tecnológica de la sede y, en última instancia, de toda la Universidad de Costa Rica.

4.2 Introducción a la propuesta

Con base en los hallazgos obtenidos, se propone el diseño de un Manual de Procedimientos de Control Perimetral de Ciberseguridad, destinado a la Sede del Pacífico de la Universidad de Costa Rica. Este instrumento busca establecer lineamientos claros, estandarizar prácticas, definir responsabilidades y fortalecer la capacidad institucional para prevenir, detectar y responder ante incidentes de seguridad en la red perimetral.

La propuesta se fundamenta en el Marco de Ciberseguridad del NIST (2018) y en las normas ISO/IEC 27005:2018 e ISO/IEC 27002:2022, adaptadas al contexto universitario. Su objetivo es consolidar la gobernanza de la seguridad perimetral

bajo un enfoque de mejora continua, en consonancia con las políticas institucionales y la misión académica de la UCR

4.3 Propuesta

4.3.1 Introducción

Con base en los hallazgos obtenidos, se propone el diseño de un Manual de Procedimientos de Control Perimetral de Ciberseguridad, destinado a la Sede del Pacífico de la Universidad de Costa Rica. Este instrumento busca establecer lineamientos claros, estandarizar prácticas, definir responsabilidades y fortalecer la capacidad institucional para prevenir, detectar y responder ante incidentes de seguridad en la red perimetral.

La propuesta se fundamenta en el Marco de Ciberseguridad del NIST (2018) y en las normas ISO/IEC 27005:2018 e ISO/IEC 27002:2022, adaptadas al contexto universitario. Su objetivo es consolidar la gobernanza de la seguridad perimetral bajo un enfoque de mejora continua, en consonancia con las políticas institucionales y la misión académica de la UCR.

4.3.2 Objetivo General

Diseñar un manual que establezca los procedimientos, controles, roles y responsabilidades necesarios para la gestión eficiente y segura del perímetro tecnológico de la Sede del Pacífico, alineado con el Marco NIST y las buenas prácticas internacionales de ciberseguridad.

4.3.3 Objetivos específicos

- Estandarizar los procedimientos de control y monitoreo del perímetro de red institucional.
- Definir los roles, responsabilidades y flujos de comunicación en la gestión de incidentes.
- Fortalecer las capacidades de detección, respuesta y recuperación ante amenazas.

- Promover la cultura de ciberseguridad y la capacitación continua del personal técnico.
- Incorporar métricas y mecanismos de seguimiento que permitan evaluar la efectividad de los controles implementados.

4.3.4 Alcance

El manual está dirigido al personal técnico de TI de la Sede del Pacífico de la UCR, abarcando las infraestructuras de red, servidores, dispositivos de borde, servicios de acceso remoto, políticas de autenticación y mecanismos de monitoreo asociados al perímetro institucional.

Su aplicación contempla los procesos operativos y administrativos relacionados con la seguridad perimetral, incluyendo la gestión de incidentes, la administración de accesos y la recuperación ante desastres

4.3.5 Estructura propuesta del manual

El Manual de Procedimientos de Control Perimetral de Ciberseguridad se propone con la siguiente estructura:

1. **Introducción general**
    - Propósito del manual
    - Alcance institucional
    - Normativa y marcos de referencia (NIST, ISO, UCR)
2. **Marco conceptual y normativo**
    - Conceptos clave de seguridad perimetral
    - Relación con el Marco NIST y normas ISO
    - Políticas y lineamientos internos de la UCR
3. **Roles y responsabilidades**
    - Encargado de TI
    - Técnicos de infraestructura
    - Coordinador de seguridad

- Usuarios autorizados y terceros

4. **Gestión de activos y configuración del perímetro**
    - Inventario y clasificación por criticidad
    - Registro de dispositivos conectados
    - Control de cambios y respaldos de configuración
    - Procedimientos operativos de control perimetral
    - Configuración segura de firewalls y routers
    - Segmentación de red y zonas de seguridad
    - Implementación de VPN y MFA
    - Control de acceso basado en roles
    - Monitoreo y detección de amenazas
    - Uso de sistemas IDS/IPS
    - Revisión de logs y eventos de seguridad
    - Alertas automáticas y respuesta inicial
    - Coordinación con el centro de TI central
    - Gestión de incidentes de seguridad
    - Clasificación de incidentes
    - Flujo de respuesta y escalamiento
    - Registro y análisis posterior al incidente
5. **Plan de respaldo y recuperación**
    - Políticas de copias de seguridad
    - Restauración de configuraciones perimetrales
    - Vinculación con el plan de continuidad operativa
6. **Capacitación y cultura de ciberseguridad**
    - Programas de formación periódica
    - Campañas de sensibilización
    - Evaluación de competencias
7. **Evaluación, métricas y mejora continua**

- Indicadores de desempeño (KPIs)
- Auditorías internas
- Revisión anual del manual

4.3.6 Fundamentación de la propuesta

El diseño de esta estructura responde a la necesidad de integrar las funciones definidas por el NIST CSF: Identificar, Proteger, Detectar, Responder y Recuperar, dentro de un marco operativo adaptado a las condiciones reales de la sede. Cada sección contribuye al cumplimiento de una o más de estas funciones, garantizando un enfoque integral de la seguridad perimetral.

Asimismo, la propuesta se alinea con los principios de mejora continua establecidos por CMMI Institute (2020) y las recomendaciones de ENISA (2021) sobre la creación de una cultura institucional de seguridad. De esta forma, el manual se constituye en una herramienta dinámica, orientada no solo a la corrección de debilidades actuales, sino también al fortalecimiento permanente de las capacidades institucionales ante un entorno de amenazas cada vez más complejo.

En conclusión, el desarrollo del Manual de Procedimientos de Control Perimetral de Ciberseguridad representa una respuesta directa a las necesidades detectadas en la Sede del Pacífico de la Universidad de Costa Rica. Su implementación permitirá establecer un marco unificado de actuación, promover la estandarización de procesos y consolidar una cultura organizacional orientada a la protección, detección y respuesta efectiva frente a incidentes.

De este modo, se fortalecerá la postura de ciberseguridad institucional bajo los lineamientos del Marco NIST y las buenas prácticas internacionales, contribuyendo a una gestión más eficiente, segura y resiliente del entorno tecnológico universitario.

4.3.7 Propuesta de plantillas para la seguridad perimetral de acuerdo con la estructura planteada

El presente apartado ofrece una serie de plantillas estructuradas, diseñadas para servir como base del futuro Manual de Procedimientos de Control Perimetral de Ciberseguridad. Su propósito es proporcionar una estructura formal que permita organizar la información, estandarizar la documentación y facilitar el proceso de recolección de datos, definición de responsabilidades y redacción final del manual.

Estas plantillas están alineadas con la estructura propuesta en 4.3.5 y con las funciones del Marco NIST (Identificar, Proteger, Detectar, Responder y Recuperar).

Las tablas y estructuras presentadas en este apartado tienen un carácter exclusivamente demostrativo. Su contenido es ilustrativo y no representa datos reales ni procedimientos definitivos. El propósito de dichas plantillas es servir como base estructural para la construcción del Manual de Procedimientos de Control Perimetral de Ciberseguridad, facilitando la organización del contenido y la documentación futura. Cada plantilla deberá completarse posteriormente con información oficial, validada y contextualizada por el personal técnico de la Sede del Pacífico de la Universidad de Costa Rica

4.3.7.1 Portada del Manual

Manual de Procedimientos de Control Perimetral de Ciberseguridad Sede del Pacífico – Universidad de Costa Rica

Versión: _____
Fecha de emisión: _____
Responsable de la actualización: _____
Aprobado por: _____

4.3.7.2 Introducción general

4.3.7.2.1 Propósito del manual

“Aquí se debe colocar la descripción detallada del propósito del manual, su razón de ser y objetivo general.”

4.3.7.2.2 Alcance institucional

“Aquí se debe especificar el alcance del manual, las unidades, sistemas, infraestructura y procesos que cubre.”

4.3.7.2.3 Normativa y marcos de referencia (NIST, ISO, UCR)

“Aquí se debe incluir el listado y la descripción de las principales normas, marcos y políticas institucionales que fundamentan el manual.”

4.3.7.3 Marco conceptual y normativo

4.3.7.3.1 Conceptos clave de seguridad perimetral

“Aquí se deben definir los conceptos esenciales que serán utilizados a lo largo del manual (por ejemplo: firewall, VLAN, IDS/IPS, VPN, MFA)”

4.3.7.3.2 Relación con el Marco NIST y normas ISO

“Aquí se debe explicar cómo el manual se alinea con las funciones del NIST (Identificar, Proteger, Detectar, Responder, Recuperar) y con los controles de ISO 27001/27002.”

4.3.7.3.3 Políticas y lineamientos internos de la UCR

“Aquí se deben mencionar las políticas internas institucionales que aplican al control perimetral.”

4.3.7.4 Control de Versiones

Tabla 2

Control de versiones del manual

Versión	Fecha	Descripción del cambio	Elaboró	Revisó	Aprobó
1.0	dd/mm/aaaa	Versión inicial del manual	Irwin	Irvin	Randal

Nota: Esta tabla permite registrar las versiones del manual y los responsables de cada actualización.

4.3.7.4 Roles y Responsabilidades

Tabla 3

Distribución de roles y responsabilidades operativas

Rol	Unidad / Puesto	Responsabilidades	Nivel de autoridad	Firma
Encargado de TI	Dirección Sede	Supervisión general, aprobación de cambios, coordinación con TI central	Alta	
Administrador de Red	TI – Sede del Pacífico	Configuración de firewall, gestión de VPN, segmentación	Alta	
Técnico Especializado	TI	Ejecución de procedimientos, monitoreo, documentación	Media	
Usuario autorizado	Todas las unidades	Uso adecuado de servicios, reporte de incidentes	Baja	

Nota. La tabla define los roles formales requeridos para la gestión perimetral.

4.3.7.5 Inventario y Clasificación de Activos

Tabla 4

Activos tecnológicos relacionados con la frontera perimetral

Clasificación por criticidad y ubicación					
ID	**Activo**	**Descripción**	**Ubicación**	**Responsable**	**Criticidad**
FW-01	Firewall NGFW	Dispositivo perimetral principal	Cuarto de comunicaciones	Admin Red	Alta
SRV-02	Servidor de autenticación	Maneja MFA y accesos	Data center	Encargado TI	Alta
SW-03	Switch capa 3	Segmentación interna	Oficina TI	Técnico	Media

Nota. Esta tabla resume los activos perimetrales que serán analizados, incluyendo responsable, ubicación y criticidad.

4.3.7.6 Clasificación y Valoración del Riesgo

Tabla 5

Clasificación de activo y riesgo asociado

Activo	**Impacto Confidencialidad**	**Impacto Integridad**	**Impacto Disponibilidad**	**Nivel de riesgo**	**Controles asociados**
Firewall NGFW	Alto	Alto	Alto	Crítico	Segmentación, monitoreo, respaldos
Servidor VPN	Medio	Alto	Alto	Alto	MFA, control de acceso

Nota. Esta tabla permite valorar el riesgo conforme a marcos NIST e ISO 27005.

4.3.7.7 Mapa del Perímetro de Red (Esquema vacío)

Título mayor: Arquitectura perimetral de la sede

(espacio reservado para insertar diagrama institucional)

4.3.7.8 Procedimiento Técnico Estándar (PTE)

Tabla 6

Estructura del procedimiento técnico

Paso	Descripción	Responsable	Evidencia
1	Validar identidad del solicitante	Técnico	Ticket
2	Aplicar cambio o regla	Admin Red	Captura config
3	Registrar modificación	Técnico	Bitácora

Nota. Este formato define la estructura de los Procedimientos Técnicos Estándar.

4.3.7.9 Gestión de Incidentes Perimetrales

Tabla 7

Flujo de gestión de incidentes

Fase	Descripción	Responsable	Tiempo máximo
Detección	Identificación del evento	Técnico TI	15 min
Análisis	Validación de incidentes	Admin TI	30 min
Contención	Bloqueo o aislamiento	Admin Red	1 hora
Recuperación	Restauración del servicio	TI	Variable

Nota. La tabla describe el flujo base para gestionar eventos de ciberseguridad.

4.3.7.10 Lista de Verificación de Configuraciones

Tabla 8

Checklist de configuración perimetral

Ítem	Cumple (Sí/No)	Evidencia	Responsable	Observaciones
MFA habilitado				
Reglas actualizadas				
VLAN aplicadas				
Respaldo exportado				

Nota. Esta lista permite validar controles mínimos requeridos.

4.3.7.11 Registro de Cambios en Firewall

Tabla 9

Control de cambios aplicados al firewall

Fecha	Área afectada	Cambio aplicado	Motivo	Solicita	Aprueba	Evidencia
dd/mm	VLAN Académica	Nueva regla	Solicitud docente	Nombre	Jefe TI	Adjuntar

Nota. Los cambios deben documentarse con evidencia adjunta.

4.3.7.12 Indicadores y Métricas (KPIs)

Tabla 10

Indicadores operativos perimetrales

Indicador	Fórmula	Frecuencia	Responsable	Meta	Estado
Intentos bloqueados	Log SIEM / mes	Mensual	TI	Reducción	
Tiempo de respuesta	(TR – TD)	Por incidente	TI	< 30 min	
Sistemas actualizados	Actualizados / total	Mensual	Técnico	100%	

Nota. Los indicadores deben revisarse periódicamente.

4.3.7.13 Plan de Respaldo y Recuperación

Tabla 11

Plan base de recuperación perimetral

Servicio	Responsable	Procedimiento	Recursos	RTO	Estado
Firewall	Encargado TI	Importar configuración	Backup	2 h	A
VPN	Admin Red	Restaurar perfiles	Servidor auth	1 h	A

Nota. La tabla establece procesos mínimos de restauración.

4.3.7.14 Capacitación y Concientización

Tabla 12

Programa de formación y sensibilización

Tema	Público objetivo	Modalidad	Responsable	Frecuencia	Evidencia
Uso de VPN	Funcionarios	Taller	TI	Semestral	Lista firma
Seguridad perimetral	Técnicos	Capacitación	TI	Anual	Informe

Nota. Esta plantilla estructura el plan formativo.

4.3.7.15 Alineamiento Normativo (NIST – ISO – UCR)

Tabla 13

Matriz de alineamiento normativo

Sección	NIST	ISO	Política UCR	Observaciones
Incidentes	RS	A.16	Seguridad TIC	
Accesos	PR	A.9	Reglamento TIC	

Nota. Esta matriz permite rastrear cumplimiento y fundamentos normativos.

4.3.7.16 Auditoría y Revisión Anual

Tabla 14

Auditoría interna del control perimetral

Actividad	Frecuencia	Responsable	Evidencia	Resultado
Auditoría firewall	Trimestral	TI	Informe	
Auditoría logs	Mensual	Técnico	Capturas	
Revisión del manual	Anual	Encargado TI	Acta	

Nota. Todas las actividades deben documentarse para evaluación continua.

El desarrollo de esta propuesta constituye un paso fundamental para la creación del Manual de Procedimientos de Control Perimetral de Ciberseguridad. A partir de los hallazgos del diagnóstico y del análisis normativo, se generó una estructura sólida, alineada con buenas prácticas internacionales como el Marco NIST y normas ISO, pero adaptada a la realidad operativa de la Sede del Pacífico.

Las plantillas presentadas permiten estandarizar la documentación, clarificar roles, formalizar procesos y facilitar la futura implementación institucional del manual. De esta manera, el apartado de propuesta sienta las bases para fortalecer la gestión perimetral, contribuir a la continuidad operativa, reducir brechas de seguridad y consolidar una cultura organizacional orientada a la protección del perímetro digital.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

El desarrollo del presente Trabajo Final de Graduación permitió abordar integralmente la problemática relacionada con la ausencia de procedimientos formalizados para el control perimetral de ciberseguridad en la Sede del Pacífico de la Universidad de Costa Rica. A partir del análisis teórico, el diagnóstico institucional y el diseño del manual de procedimientos, se logró generar una propuesta sustentada y funcional. Las conclusiones que se presentan a continuación responden directamente a los objetivos específicos definidos al inicio del proyecto.

Objetivo 1:

Estandarizar los procedimientos de control y monitoreo del perímetro de red institucional.

El análisis de referentes teóricos y normativos confirmó que el control perimetral constituye una de las capas esenciales dentro de un modelo de defensa en profundidad, especialmente en instituciones académicas que operan con infraestructuras digitales críticas y exposición constante a amenazas cibernéticas. El estudio del Marco NIST, las normas ISO/IEC 27001 y 27005, así como las guías emitidas por el CONARE y organismos como ENISA, permitió determinar su alta pertinencia para el contexto universitario costarricense.

Este análisis evidenció que la ausencia de referencia formal a estos marcos en la Sede del Pacífico ha limitado la estandarización de prácticas técnicas y administrativas, generando brechas en la gestión del riesgo y en la capacidad de respuesta ante incidentes. Asimismo, se concluye que los marcos estudiados no solo brindan lineamientos técnicos, sino que favorecen la cultura organizacional, la gobernanza tecnológica y la madurez institucional. Por tanto, su adopción representa una oportunidad valiosa para fortalecer la postura de ciberseguridad de la sede y alinearse con estándares internacionales que son ampliamente reconocidos y replicables.

Objetivo 2:

Definir los roles, responsabilidades y flujos de comunicación en la gestión de incidentes.

El diagnóstico realizado mediante cuestionarios, análisis documental y observación permitió identificar que, aunque la Sede del Pacífico cuenta con equipamiento base adecuado, incluyendo firewall, VPN, segmentación lógica de la red y, en algunos casos, IDS/IPS, persisten vacíos significativos en materia de formalización, documentación y estandarización de procedimientos perimetrales.

Entre los principales hallazgos destaca la existencia de un inventario actualizado de activos tecnológicos, lo cual constituye una fortaleza alineada con la función “Identificar” del NIST; sin embargo, la falta de clasificación por criticidad y el uso de documentación técnica fragmentada limita la efectividad del análisis de riesgo y de la toma de decisiones operativas.

Asimismo, se constató que muchas de las tareas relacionadas con el perímetro se ejecutan mediante buenas prácticas adoptadas empíricamente por el personal técnico, pero sin un soporte procedimental formal que garantice su continuidad, trazabilidad y mejora continua. Esta situación aumenta la dependencia del conocimiento individual, dificulta la auditoría interna y expone a la sede a riesgos innecesarios ante incidentes de seguridad o cambios de personal.

En síntesis, el diagnóstico permitió determinar con claridad que la institución posee capacidades tecnológicas iniciales, pero requiere urgentemente un instrumento operativo que consolide roles, responsabilidades, procesos, métricas y lineamientos uniformes.

Objetivo 3:

Fortalecer las capacidades de detección, respuesta y recuperación ante amenazas.

A partir del análisis de resultados y de la revisión normativa, fue posible diseñar una propuesta de manual alineado con las funciones del Marco NIST: Identificar, Proteger, Detectar, Responder y Recuperar. El diseño incorpora

plantillas, roles, responsabilidades, procedimientos y métricas que permiten sistematizar la gestión perimetral. El manual responde directamente a las brechas identificadas, aportando una estructura práctica, escalable y replicable para futuras implementaciones en otras sedes universitarias. Se concluye que el manual constituye un instrumento base que fortalece la continuidad operativa, la gestión del riesgo y la cultura de ciberseguridad institucional.

5.2 Recomendaciones

A partir de los hallazgos obtenidos durante el análisis del estado actual del control perimetral, así como del proceso de diseño del manual propuesto, se establecen a continuación una serie de recomendaciones orientadas a fortalecer la gestión de la ciberseguridad en la Sede del Pacífico de la Universidad de Costa Rica. Estas recomendaciones derivan directamente de las conclusiones alcanzadas y buscan garantizar la aplicabilidad, sostenibilidad y mejora continua del manual diseñado. Además, pretenden orientar a la institución hacia un modelo más maduro, coherente con buenas prácticas internacionales, y ajustado a las capacidades y necesidades propias de la sede.

En primer lugar, se recomienda que el Encargado de TI, en coordinación con la Administración de la Sede, impulse la adopción formal del manual de procedimientos diseñado. Este proceso debería completarse en un plazo de tres meses posteriores a su aprobación, asegurando que el documento se incorpore dentro de las políticas institucionales de TIC y se alinee plenamente con marcos internacionales como NIST e ISO. La formalización del manual permitirá superar la actual fragmentación de prácticas y establecer una guía unificada para la operación, documentación y toma de decisiones en materia de seguridad perimetral.

Asimismo, se aconseja que el personal técnico de TI desarrolle, en un periodo aproximado de uno a dos meses, una clasificación de criticidad de los activos tecnológicos que forman parte del perímetro de red. Esta acción es indispensable para fortalecer la gestión del riesgo, priorizar esfuerzos y orientar adecuadamente la asignación de controles. La existencia de un inventario

actualizado representa un avance significativo; no obstante, su efectividad se ve limitada si no se acompaña de una categorización basada en impacto y probabilidad.

De igual modo, se recomienda avanzar en la consolidación y formalización de toda la documentación asociada al perímetro de red. En un plazo de tres a cuatro meses, los técnicos responsables deberían integrar los diagramas, configuraciones, registros y procedimientos actualmente dispersos dentro del esquema estructurado que proporciona el manual. Esta estandarización contribuirá a la trazabilidad de las acciones, facilitará auditorías internas y reducirá la dependencia del conocimiento tácito del personal.

Por otra parte, se sugiere la implementación de un programa de capacitación continúa dirigido tanto al personal técnico como a los funcionarios que interactúan con sistemas expuestos al perímetro. Este programa, coordinado entre el Encargado de TI y la Oficina de Recursos Humanos, podría iniciarse en un plazo de dos meses, con sesiones periódicas a lo largo del año. Su objetivo principal es fortalecer la cultura de ciberseguridad, garantizar el uso adecuado de las herramientas perimetrales y mejorar la capacidad institucional para prevenir, detectar y responder a incidentes.

Adicionalmente, resulta fundamental que el equipo de TI incorpore un sistema de indicadores y métricas que permita evaluar de manera objetiva el desempeño de los controles perimetrales. Esta implementación debería concretarse en un lapso de tres meses, con ciclos de medición mensual. La utilización de indicadores como intentos de intrusión bloqueados, tiempos de respuesta o frecuencia de revisión del firewall contribuirá a una gestión más proactiva, basada en evidencia y enfocada en la mejora continua.

Finalmente, se recomienda establecer auditorías internas trimestrales, lideradas por el Encargado de TI y con apoyo de la Auditoría Interna cuando corresponda. Estas auditorías deberán revisar configuraciones, registros, cumplimiento de procedimientos y la vigencia del manual, con el fin de garantizar su aplicación sostenida en el tiempo. De igual manera, se sugiere promover la articulación del manual con otras sedes de la UCR, proceso que podría desarrollarse en un plazo de seis a doce meses, generando sinergias institucionales

y favoreciendo la estandarización de prácticas de ciberseguridad a nivel universitario.

En conjunto, estas recomendaciones constituyen una ruta clara y coherente para avanzar hacia una gestión perimetral más sólida, estructurada y alineada con las nuevas exigencias tecnológicas y normativas. Su implementación permitirá no solo resguardar de manera más eficiente la infraestructura de la Sede del Pacífico, sino también consolidar una cultura institucional orientada a la seguridad, la continuidad operativa y la mejora continua.

BIBLIOGRAFÍA

- Bernal, C. A. (2016). *Metodología de la investigación: Administración, economía, humanidades y ciencias sociales* (4.ª ed.). Pearson Educación.
- Check Point Software Technologies. (2023). *Cyber Attack Trends: 2023 Mid-Year Report*. https://www.checkpoint.com/downloads
- Chandramouli, R., & Rose, S. (2021). Secure Access Service Edge (SASE) and Zero Trust Architecture (ZTA). NIST Special Publication 1800.
- CONARE. (2022). *Lineamientos estratégicos para la ciberseguridad en las universidades públicas*. Consejo Nacional de Rectores.
- European Union Agency for Cybersecurity. (2022). ENISA Threat Landscape 2022. https://www.enisa.europa.eu/publications
- ENISA. (2021). *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines
- ENISA. (2023). Cyber Threat Landscape Report 2023. European Union Agency for Cybersecurity.
- Forrest, J., & Martínez, L. (2020). Arquitecturas perimetrales modernas para redes académicas. *Journal of Network Security*, 12(3), 55–72.
- García, D., & Herrera, M. (2021). Propuesta de manual de seguridad perimetral para instituciones académicas. *Revista Seguridad Informática*, 39(4), 22–35.
- Gartner. (2023). Market Guide for Zero Trust Network Access. Gartner Research.
- Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2022). *Metodología de la investigación* (7.ª ed.). McGraw-Hill Education.
- IBM Security. (2023). *Cost of a Data Breach Report 2023*. https://www.ibm.com/security/data-breach
- Instituto Nacional de Estándares y Tecnología (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- International Organization for Standardization. (2013). *ISO/IEC 27001:2013 – Information security management systems — Requirements*. ISO.

- International Organization for Standardization. (2018). *ISO/IEC 27005:2018 – Information technology — Security techniques — Information security risk management*. ISO.
- ISACA. (2021). *COBIT 2019 Framework: Introduction and Methodology*. Information Systems Audit and Control Association. https://www.isaca.org/resources/cobit
- Kerzner, H. (2022). *Project management: A systems approach to planning, scheduling, and controlling* (13th ed.). John Wiley & Sons.
- Kotter, J. P. (2012). *Leading change*. Harvard Business Review Press.
- López, J., & Salas, C. (2021). Gestión del cambio y cultura organizacional en la implementación de políticas TIC en universidades públicas. *Revista de Administración Digital*, 7(2), 45–60.
- López, R., Pérez, C., & Mendoza, J. (2020). Estrategias de ciberdefensa para entornos universitarios. *Revista Latinoamericana de Tecnología Educativa*, 19(2), 77–91.
- MICITT. (2023). *Plan Nacional de Ciberseguridad 2023–2027*. Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica. https://www.micitt.go.cr
- Mora, J. (2022). Lecciones del ciberataque a la Caja Costarricense: análisis desde la ciberseguridad institucional. *Revista Jurídica UCR*, 36(1), 55–70.
- Moreira, L., & Santana, J. (2022). Zero Trust aplicado a instituciones académicas: Retos y oportunidades. Revista Iberoamericana de Seguridad Digital, 8(1), 45–67.
- OEI. (2020). *Ciberseguridad en América Latina: Retos y oportunidades*. Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura.
- Pino, J., & Cárdenas, A. (2020). Integración normativa en entornos tecnológicos universitarios. *Revista Iberoamericana de Derecho Informático*, 6(1), 75–92.
- Sampieri, R., Collado, C. F., & Lucio, P. B. (2022). *Metodología de la investigación* (7.ª ed.). McGraw-Hill Education.
- SANS Institute. (2023). Best Practices for Network Perimeter Security. https://www.sans.org/white-paper
- Universidad de Cambridge. (2021). *Cybersecurity Strategy 2021–2025*. IT Services, University of Cambridge. https://www.it.cam.ac.uk
- Universidad de los Andes. (2019). *Política de seguridad de la información y control perimetral*. Facultad de Ingeniería, Bogotá, Colombia.

- Universidad de São Paulo. (2020). Manual de segurança perimetral para redes acadêmicas. Departamento de TIC.
- Universidad del Rosario. (2020). *Política de seguridad de la información y control perimetral*. Facultad de Ingeniería, Bogotá, Colombia.
- Universidad Nacional Autónoma de México. (2021). *Manual de políticas de seguridad informática*. Dirección General de Cómputo y TIC.
- Villanueva, P. (2022). Riesgos cibernéticos en entornos académicos costarricenses: una revisión crítica. *Revista de Tecnología e Innovación Educativa*, 14(2), 101–115.

ANEXOS

Anexo 1. Cuestionario aplicado al personal técnico de TI

Instrucciones:

Marque la opción que mejor describa la situación actual o responda brevemente según corresponda.

La información será utilizada únicamente con fines académicos y de mejora institucional.

Sección 1. Identificación general

1. Cargo actual: _____
2. Años de experiencia en el área de TI:
   ☐ Menos de 1 año ☐ 1–3 años ☐ 4–6 años ☐ Más de 6 años
3. Principales responsabilidades en infraestructura o seguridad:
   ☐ Administración de red
   ☐ Seguridad informática
   ☐ Soporte técnico
   ☐ Gestión de servidores o firewalls
   ☐ Otro: _____

Sección 2. Identificación y gestión de activos (Función "Identificar" – NIST)

4. ¿Existe un inventario actualizado de los activos tecnológicos conectados al perímetro de red?
   ☐ Sí, completo y actualizado
   ☐ Parcial
   ☐ No existe
5. ¿El inventario incluye clasificación por criticidad o nivel de riesgo?
   ☐ Sí ☐ No ☐ En proceso
6. ¿Se cuenta con políticas o procedimientos documentados para la administración del perímetro de red?
   ☐ Sí, formalizados

☐ Parcialmente documentados

☐ No existen

7. ¿Qué tipo de documentación utiliza actualmente?

   ☐ Diagramas de red

   ☐ Listas de control de acceso

   ☐ Manuales internos

   ☐ Ninguno

   ☐ Otro: _____

Sección 3. Protección y controles implementados (Función “Proteger”)

8. ¿Qué mecanismos de control perimetral están actualmente activos en la sede?

   ☐ Firewall tradicional

   ☐ Firewall de nueva generación (NGFW)

   ☐ IDS/IPS

   ☐ VPN

   ☐ Segmentación de red (VLANs o DMZs)

   ☐ Filtrado de contenido o proxy

   ☐ Otro: _____

9. ¿Los accesos remotos están protegidos mediante autenticación multifactor (MFA)?

   ☐ Sí ☐ No ☐ No aplica

10. ¿Se aplican políticas de “menor privilegio” en el acceso a recursos perimetrales?

    ☐ Siempre ☐ Ocasionalmente ☐ No se aplican

11. ¿Con qué frecuencia se revisan o actualizan las reglas del firewall o listas de acceso?

☐ Mensualmente ☐ Trimestralmente ☐ Anualmente ☐ Solo cuando ocurre un incidente

12. ¿Existen respaldos documentados de la configuración del perímetro?
    ☐ Sí, con almacenamiento seguro
    ☐ Sí, pero sin respaldo automatizado
    ☐ No

Sección 4. Detección y monitoreo (Función "Detectar")

13. ¿Se monitorea de forma continua el tráfico de red o los intentos de intrusión?
    ☐ Sí, mediante SIEM u otra herramienta
    ☐ Parcialmente (solo logs del firewall)
    ☐ No se realiza monitoreo activo
14. ¿Existen alertas automáticas ante actividades anómalas o sospechosas?
    ☐ Sí ☐ No ☐ En proceso de implementación
15. ¿Con qué frecuencia se revisan los registros de eventos de seguridad?
    ☐ Diario ☐ Semanal ☐ Mensual ☐ Solo cuando ocurre un incidente

Sección 5. Respuesta y recuperación (Funciones "Responder" y "Recuperar")

16. ¿Existe un procedimiento documentado para la respuesta ante incidentes de ciberseguridad?
    ☐ Sí, validado y aprobado institucionalmente
    ☐ Parcialmente definido
    ☐ No existe
17. ¿El personal técnico ha participado en simulacros o ejercicios de respuesta a incidentes?
    ☐ Sí, recientemente ☐ Hace más de un año ☐ Nunca

18. ¿Existen mecanismos definidos para la comunicación y escalamiento de incidentes al nivel central de TI de la UCR?
    ☐ Sí ☐ Parcialmente ☐ No

19. ¿Se realizan copias de seguridad periódicas de los sistemas perimetrales y configuraciones críticas?
    ☐ Sí, automáticas
    ☐ Sí, manuales
    ☐ No

20. ¿Se dispone de un plan de recuperación ante desastres (DRP) o continuidad operativa?
    ☐ Sí, documentado y probado
    ☐ Sí, pero no probado
    ☐ No

Sección 6. Cultura, capacitación y madurez institucional

21. ¿El personal técnico recibe capacitaciones periódicas sobre seguridad perimetral o NIST?
    ☐ Sí, al menos una vez al año
    ☐ Esporádicamente
    ☐ No

22. ¿Considera que existe una cultura de ciberseguridad consolidada en la sede?
    ☐ Alta ☐ Media ☐ Baja

23. ¿Cuáles considera las principales debilidades del perímetro de red actual?
    ☐ Falta de documentación
    ☐ Equipos obsoletos
    ☐ Escaso monitoreo
    ☐ Falta de capacitación
    ☐ Otro: _____

24. ¿Qué mejoras priorizaría para fortalecer el perímetro de red?

25. ¿Tiene comentarios o recomendaciones adicionales sobre la gestión perimetral en la sede?

Anexo 2. Resultados completos del cuestionario

Tabla 1

Cargo actual?	Años de experiencia en el área de TI?	Principales responsabilidades en infraestructura o seguridad:	¿Existe un inventario actualizado de los activos tecnológicos conectados al perímetro de red?	¿El inventario incluye clasificación por criticidad o nivel de riesgo?
Técnico Especializado D	Más de 6 años	Soporte técnico	Sí, completo y actualizado	No
Técnico Especializado D	Más de 6 años	Administración de red, Soporte técnico, Gestión de servidores o firewalls	Sí, completo y actualizado	Sí
Encargado de TI	Más de 6 años	Administración de red, Seguridad informática, Soporte técnico, Gestión de servidores o firewalls, Proyectos	Sí, completo y actualizado	En proceso
Técnico Especializado D	Más de 6 años	Administración de red, Soporte técnico	Sí, completo y actualizado	No

Tabla 2

¿Se cuenta con políticas o procedimientos documentados para la administración del perímetro de red?	¿Qué tipo de documentación utiliza actualmente?	¿Qué mecanismos de control perimetral están actualmente activos en la sede?	¿Los accesos remotos están protegidos mediante autenticación multifactor	¿Se aplican políticas de "menor privilegio" en el acceso a recursos perimetrales?
Parcialmente documentados	Diagramas de red	Firewall tradicional, VPN, Segmentación de red (VLANs o DMZs), Filtrado de contenido o proxy	No	No se aplican
Sí, formalizados	Diagramas de red	Firewall tradicional, IDS/IPS, VPN, Segmentación de red (VLANs o DMZs)	No	Siempre
Sí, formalizados	Varios anteriores	Firewall de nueva generación (NGFW), IDS/IPS, VPN, Segmentación de red (VLANs o DMZs), Filtrado de contenido o proxy, Confidenciales	No aplica	Siempre
Parcialmente documentados	Diagramas de red	Firewall tradicional, VPN, Segmentación de red (VLANs o DMZs), Filtrado de contenido o proxy	No	No se aplican

Tabla 3

¿Con qué frecuencia se revisan o actualizan las reglas del firewall o listas de acceso?	¿Existen respaldos documentados de la configuración del perímetro?	¿Se monitorea de forma continua el tráfico de red o los intentos de intrusión?	¿Existen alertas automáticas ante actividades anómalas o sospechosas?	¿Con qué frecuencia se revisan los registros de eventos de seguridad?
Solo cuando ocurre un incidente	No	No se realiza monitoreo activo	En proceso de implementación	Solo cuando ocurre un incidente
Mensualmente	Sí, con almacenamiento seguro	Sí, mediante SIEM u otra herramienta	Sí	Diario
Mensualmente	Sí, con almacenamiento seguro	Sí, mediante SIEM u otra herramienta	Sí	Diario
Solo cuando ocurre un incidente	No	No se realiza monitoreo activo	En proceso de implementación	Solo cuando ocurre un incidente

Tabla 4

¿Existe un procedimiento documentado para la respuesta ante incidentes de ciberseguridad?	¿El personal técnico ha participado en simulacros o ejercicios de respuesta a incidentes?	¿Existen mecanismos definidos para la comunicación y escalamiento de incidentes al nivel central de TI de la UCR?	¿Se realizan copias de seguridad periódicas de los sistemas perimetrales y configuraciones críticas?	¿Se dispone de un plan de recuperación ante desastres (DRP) o continuidad operativa?
No existe	Nunca	Parcialmente	Sí, manuales	No
Sí, validado y aprobado institucionalmente	Nunca	Sí	Sí, automáticas	Sí, documentado y probado
Sí, validado y aprobado institucionalmente	Sí, recientemente	Sí	Sí, automáticas	Sí, documentado y probado
No existe	Nunca	Parcialmente	Sí, manuales	Sí, pero no probado

Tabla 5

¿El personal técnico recibe capacitaciones periódicas sobre seguridad perimetral o NIST?	¿Considera que existe una cultura de ciberseguridad consolidada en la sede?	¿Cuáles considera las principales debilidades del perímetro de red actual?	¿Qué mejoras priorizaría para fortalecer el perímetro de red?	¿Tiene comentarios o recomendaciones adicionales sobre la gestión perimetral en la sede?
No	Baja	Falta de documentación, Equipos obsoletos, Escaso monitoreo, Falta de capacitación	capacitacion	Capacitacion
Esporádicamente	Media	Falta de capacitación	Implementar la autenticación multifactor (MFA) y auditorias periódicas.	Reforzar el acceso con MFA
Sí, al menos una vez al año	Alta	No aplica	NA	NA
Esporádicamente	Media	Falta de documentación, Falta de capacitación	Capacitación y auditorías	Reforzar el acceso con Autenticación Multifactor