UNIVERSIDAD HISPANOAMERICANA

Escuela de Ingeniería informática

Tesis para optar por el grado de bachillerato

TÍTULO DEL PROYECTO

Propuesta para el fortalecimiento de la seguridad de la información, basados en la metodología ISO27001 e ISO27002, para reducir brechas de seguridad y cumplir normativas, en el departamento de IT de Procter & Gamble en la sede de Costa Rica para el tercer cuatrimestre del 2025

Estudiante

Christopher Jesus Rivera Steller

Cedula 1-1710-0608

Tutor:

Marco Vinicio Soto Monge

Octubre, 2025

Tabla de Contenido

Table of Contents

DECLARACIÓN JURADA

Yo Christopher Jesús Rivera Steller, mayor de edad, portador de la cédula de identidad número 117100608 egresado de la carrera de Ingeniería Informática de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Bachillerato, juro solemnemente que mi trabajo de investigación titulado: Propuesta para el fortalecimiento de la seguridad de la información, basados en la metodología ISO27001 e ISO27002, para reducir brechas de seguridad y cumplir normativas, en el departamento de IT de Procter & Gamble en la sede de Costa Rica para el tercer cuatrimestre del 2025 , es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público.

En fe de lo anterior, firmo en la ciudad de San José, a los 7 días del mes de Julio del año dos mil veinti seis.

Firma del estudiante 

Cédula: 117100608

CARTA DEL TUTOR

San José, 08 de Mayo de 2026

Esteban José Gonzalez Vargas
Director
Ingeniería Informática
Universidad Hispanoamericana
Sede Llorente

Estimado señor:

El estudiante **Christopher Rivera Steller**, cédula de identidad número **1-1710-0608**, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado **"Propuesta para el fortalecimiento de la seguridad de la información, basados en la metodología ISO27001 e ISO27002, para reducir brechas de seguridad y cumplir normativas, en el departamento de IT de Procter & Gamble en la sede de Costa Rica para el tercer cuatrimestre del 2025",** el cual ha elaborado para optar por el grado académico de Bachiller en Ingeniería Informática.

En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

a) Original del tema	10%	10%
b) Cumplimiento de entrega de avances	20%	20%
c) Coherencia entre los objetivos, los instrumentos aplicados y los resultados de la investigación	30%	30%
d) Relevancia de las conclusiones y recomendaciones	20%	20%
e) Calidad, detalle del marco teórico	20%	20%
TOTAL		**100%**

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente, MARCO VINICIO SOTO MONGE (FIRMA)
Firmado digitalmente por MARCO VINICIO SOTO MONGE (FIRMA)
Fecha: 2026.05.08 21:30:41 -06'00'

Marco Vinicio Soto Monge

Cédula 110360428

CARTA DE LECTOR

Heredia, 20 de Junio de 2026.

Universidad Hispanoamericana
Sede Heredia
Carrera

Estimado señor

El estudiante Rivera Steller Christopher Jesús, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado "***Propuesta para el fortalecimiento de la seguridad de la información, basados en la metodología ISO27001 e ISO27002, para reducir brechas de seguridad y cumplir normativas, en el departamento de IT de Procter & Gamble en la sede de Costa Rica para el tercer cuatrimestre del 2025***", el cual ha elaborado para obtener su grado de Bachiller.

Se la han realizado varias correcciones durante el proceso, he revisado y ha hecho las ultimas observaciones relativas al contenido analizado, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, propuesta y formato del documento, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación. He verificado que se han hecho las modificaciones correspondientes a las observaciones indicadas.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.

Atte

Erick López Chavarría
Firmado digitalmente por Erick López Chavarría
Fecha: 2026.06.20 09:58:00 -06'00'

Ing. Erick López Ch, M.R.I.

UNIVERSIDAD HISPANOAMERICANA

CENTRO DE INFORMACION TECNOLOGICO (CENIT)

CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA

DE LOS TRABAJOS FINALES DE GRADUACION

San José, Julio 7 del 2026

Señores:

Universidad Hispanoamericana

Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Christopher Jesus Rivera Steller con número de identificación 117100608 autor (a) del trabajo de graduación titulado Propuesta para el fortalecimiento de la seguridad de la información, basados en la metodología ISO27001 e ISO27002, para reducir brechas de seguridad y cumplir normativas, en el departamento de IT de Procter & Gamble en la sede de Costa Rica para el tercer cuatrimestre del 2025 presentado y aprobado en el año 2026 como requisito para optar por el título de Bachillerato en Ingeniería informática; (SI) autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,

_____

Firma y Documento de Identidad

ANEXO 1 (Versión en línea dentro del Repositorio)
LICENCIA Y AUTORIZACIÓN DE LOS AUTORES PARA PUBLICAR Y PERMITIR LA CONSULTA Y USO

Parte 1. Términos de la licencia general para publicación de obras en el repositorio institucional

Como titular del derecho de autor, confiero al Centro de Información Tecnológico (CENIT) una licencia no exclusiva, limitada y gratuita sobre la obra que se integrará en el Repositorio Institucional, que se ajusta a las siguientes características:

a) Estará vigente a partir de la fecha de inclusión en el repositorio, el autor podrá dar por terminada la licencia solicitándolo a la Universidad por escrito.

b) Autoriza al Centro de Información Tecnológico (CENIT) a publicar la obra en digital, los usuarios puedan consultar el contenido de su Trabajo Final de Graduación en la página Web de la Biblioteca Digital de la Universidad Hispanoamericana

c) Los autores aceptan que la autorización se hace a título gratuito, por lo tanto, renuncian a recibir beneficio alguno por la publicación, distribución, comunicación pública y cualquier otro uso que se haga en los términos de la presente licencia y de la licencia de uso con que se publica.

d) Los autores manifiestan que se trata de una obra original sobre la que tienen los derechos que autorizan y que son ellos quienes asumen total responsabilidad por el contenido de su obra ante el Centro de Información Tecnológico (CENIT) y ante terceros. En todo caso el Centro de Información Tecnológico (CENIT) se compromete a indicar siempre la autoría incluyendo el nombre del autor y la fecha de publicación.

e) Autorizo al Centro de Información Tecnológica (CENIT) para incluir la obra en los índices y buscadores que estimen necesarios para promover su difusión.

f) Acepto que el Centro de Información Tecnológico (CENIT) pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

g) Autorizo que la obra sea puesta a disposición de la comunidad universitaria en los términos autorizados en los literales anteriores bajo los límites definidos por la universidad en las "Condiciones de uso de estricto cumplimiento" de los recursos publicados en Repositorio Institucional.

SI EL DOCUMENTO SE BASA EN UN TRABAJO QUE HA SIDO PATROCINADO O APOYADO POR UNA AGENCIA O UNA ORGANIZACIÓN, CON EXCEPCIÓN DEL CENTRO DE INFORMACIÓN TECNOLÓGICO (CENIT), EL AUTOR GARANTIZA QUE SE HA CUMPLIDO CON LOS DERECHOS Y OBLIGACIONES REQUERIDOS POR EL RESPECTIVO CONTRATO O ACUERDO.

Dedicatoria

A Dios, primeramente.

Por haberme permitido llegar a esta gran etapa de mi vida, haberme dado salud, sabiduría y entendimiento para lograr todos mis objetivos.

A mi madre Amalia.

Por ser mi apoyo incondicional en todo momento, por los consejos, valores, paciencia, cariño, amor y las fuerzas infinitas que me das para siempre salir adelante. Infinitas gracias por absolutamente todo madre, esta victoria también es para usted.

A mi padre Marvin.

Por los ejemplos de perseverancia, constancia y superación que me has enseñado siempre, por creer en mí y motivarme a alcanzar mis metas. Gracias por tu guía y por ser un pilar fundamental en mi formación.

A mi hermano Marvin Daniel.

Por siempre estar presente en mi vida, con un momento de alegría y apoyo en cada momento que lo necesité en este proceso. Gracias por tu compañía y por alentarme a seguir adelante.

A mi pareja Alice.

Por tu amor, paciencia y comprensión durante este camino. Gracias por estar a mi lado en los momentos difíciles, por creer en mí y por celebrar cada logro como si fuera tuyo. Este triunfo también te pertenece.

¡Gracias a todos ustedes!

Resumen

En el departamento de Tecnologías de Información de Procter & Gamble en la sede de Costa Rica se ha identificado una problemática crítica relacionada con la obsolescencia y la insuficiente actualización de los protocolos de seguridad de la información. Aunque la empresa cuenta con medidas de seguridad establecidas, estas no han sido revisadas ni adaptadas adecuadamente para enfrentar las nuevas amenazas y vulnerabilidades del panorama cibernético actual, generando una brecha significativa entre las prácticas existentes y las demandas de un entorno empresarial cada vez más sofisticado y propenso a ciberataques. Las causas principales incluyen la falta de actualización e implementación de protocolos basados en las normas internacionales ISO 27001 e ISO 27002, la carencia de recursos técnicos especializados en ciberseguridad, la ausencia de un plan estructurado para la mejora continua y una evaluación insuficiente de la infraestructura tecnológica.

Las consecuencias de esta situación son significativas, ya que existe un alto riesgo de brechas de seguridad que podrían comprometer la confidencialidad, integridad y disponibilidad de la información, ocasionando pérdidas financieras, daño a la reputación empresarial, pérdida de confianza por parte de clientes y socios comerciales, y posibles sanciones legales por incumplimiento normativo.

El problema general se centra en cómo mejorar la implementación de protocolos de seguridad de la información mediante el uso de estándares internacionales para adaptarse al cambiante panorama de amenazas cibernéticas. Se han identificado problemas específicos como las deficiencias de los protocolos actuales, la falta de cobertura frente a nuevas amenazas, el impacto en la eficacia y eficiencia del departamento, y los obstáculos que dificultan la implementación efectiva de soluciones innovadoras. Por ello, el presente proyecto propone diseñar una estrategia integral para el fortalecimiento de la seguridad de la información, fundamentada en las buenas prácticas de las normas ISO 27001 e ISO 27002, que permita reducir las brechas detectadas, proteger los activos informáticos y garantizar el cumplimiento normativo durante el tercer cuatrimestre del año 2025.

CAPÍTULO I: PROBLEMA DEL PROYECTO

1.1 ANTECEDENTES Y JUSTIFICACIÓN DEL PROYECTO

1.1.1 Antecedentes del contexto de la empresa

Procter & Gamble (P&G) es una compañía global de bienes de consumo, se especializa en el desarrollo y la fabricación de productos de alta calidad para el hogar y cuidado personal. La compañía fue fundada en mil ochocientos treinta y siete, tiene su sede en Cincinnati, Ohio. La misión de P&G es proporcionar productos de marca superior que mejoren la vida de los consumidores del mundo.

La empresa comenzó produciendo jabones y velas, ganando rápidamente reputación por la calidad de sus productos. Durante la Guerra Civil estadounidense, P&G suministró productos al ejército, lo que impulsó significativamente su crecimiento. En mil ochocientos setenta y nueve, lanzó Ivory Soap, el primer jabón flotante que se convirtió en un producto icónico.

P&G fue pionera en el uso de la publicidad moderna, siendo una de las primeras en patrocinar programas de radio en la década de mil novecientos treinta. Durante las décadas de mil novecientos cincuenta y sesenta, la compañía revolucionó el mercado con productos como Tide (detergente), Crest (pasta dental con flúor) y Pampers (pañales desechables), que transformaron sus respectivas categorías.

A partir del dos mil veinticuatro, la compañía tiene una fuerza laboral global y opera en más de ciento ochenta países, con presencia en múltiples categorías de productos incluyendo cuidado del hogar, belleza, cuidado personal, salud y cuidado del bebé.

Misión: "Proporcionar productos y servicios de marca superior que mejoren la vida de los consumidores del mundo". Esta declaración de misión representa el compromiso de la compañía de ofrecer productos innovadores de alta calidad en diversas categorías, desde el cuidado personal hasta la limpieza del hogar, con el objetivo de superar las expectativas y satisfacer las necesidades cambiantes de los consumidores a nivel global.

Visión: "Ser reconocida como la mejor empresa de productos de consumo y servicios del mundo". Esta visión enfatiza el compromiso de la compañía para liderar la industria mediante la creación de productos que marquen una diferencia significativa en la vida diaria de las personas.

Procter & Gamble tiene como objetivo lograr su visión siendo reconocida por su innovación, sostenibilidad, responsabilidad social y construcción de relaciones de confianza con consumidores y socios comerciales.

Valores: Integridad, liderazgo, responsabilidad, pasión por ganar y confianza. Estos valores sirven como base de la cultura de la compañía y reflejan su compromiso de ofrecer productos y servicios excepcionales a los consumidores. Los valores fundamentales de la compañía se basan en los principios de honestidad, colaboración e innovación, que ayudan a fomentar un entorno de trabajo que impulse el crecimiento y inspire a los empleados a desempeñar su máximo potencial.

Procter & Gamble es una de las compañías líderes en la industria de bienes de consumo. Sus innovadores productos han sido reconocidos por su calidad y eficacia a nivel mundial. Por ejemplo, marcas como Tide, Pampers, Gillette y Oral-B dominan sus respectivos segmentos de mercado. Además de su dedicación a la innovación, P&G se compromete a mejorar la vida de las personas en todo el mundo.

La innovación ha sido una fuerza impulsora detrás de Procter & Gamble desde su inicio. La compañía cree que la innovación no solo es importante para competir en el mercado, sino que también es crucial para abordar las necesidades de los consumidores y mejorar su calidad de vida. La compañía ha realizado importantes inversiones en investigación y desarrollo para llevar soluciones innovadoras al mercado.

Procter & Gamble continúa lanzando innovaciones en sus diferentes líneas de productos, enfocándose en sostenibilidad y responsabilidad ambiental. La empresa ha implementado iniciativas para reducir su huella de carbono y promover el uso de materiales reciclables en sus empaques. Otra innovación importante es su compromiso con la digitalización y el comercio electrónico, adaptándose a las nuevas tendencias de consumo y manteniendo su liderazgo en la industria global de bienes de consumo.

1.1.2 Justificación del proyecto

La ciberseguridad se ha convertido en una preocupación crítica para las organizaciones en un entorno digital cada vez más complejo y amenazante. Procter & Gamble, como líder en el sector de bienes de consumo, enfrenta desafíos significativos en la gestión de su infraestructura tecnológica, donde la seguridad de los datos y la protección de la información son esenciales para mantener la confianza de sus clientes y socios.

La implementación de protocolos de estrategias innovadoras para mejorar enfoques prácticos en la normativa de seguridad de la información en el departamento de la empresa Procter & Gamble en el primer cuatrimestre del 2025 se justifica por las siguientes razones fundamentadas:

Directriz de la empresa

La seguridad de la información es una prioridad para Procter & Gamble, como se refleja en su compromiso con la protección de los activos empresariales y la confidencialidad de los datos. La implementación de protocolos innovadores en este sentido refleja la directriz de la empresa de mantenerse a la vanguardia en materia de seguridad cibernética y protección de datos.

La integridad es un valor central para Procter & Gamble, que ha estado arraigado en la compañía desde su fundación. Mantener altos estándares y principios éticos es crucial para generar confianza entre los clientes, las partes interesadas y los empleados. La compañía ha realizado fuertes medidas para garantizar que se mantengan los más altos estándares de integridad en cada faceta de sus operaciones comerciales.

- Procter & Gamble ha implementado un programa de capacitación ética para todos los empleados.
- La capacitación tiene como objetivo reforzar el compromiso de la compañía con la integridad y educar a los empleados sobre cómo reconocer y responder a los dilemas éticos.

- La compañía ha establecido un código de conducta que detalla los estándares de comportamiento que se esperan de todos los empleados en el entorno laboral e interacciones con los clientes y las partes interesadas.

Cumplimiento legal

La empresa está sujeta a regulaciones y leyes relacionadas con la seguridad de la información, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea como la Ley de Privacidad del Consumidor de California (CCPA) en los Estados Unidos. La implementación de protocolos mejorados garantizará el cumplimiento continuo de estas regulaciones, mitigando así el riesgo de sanciones legales y protegiendo la reputación de la empresa.

El sistema de gestión de calidad de Procter & Gamble incluye múltiples certificaciones reglamentarias que se llevan a cabo en cada una de sus instalaciones.

Oportunidad de negocio

En un entorno empresarial cada vez más digitalizado, la seguridad de la información se ha convertido en un diferenciador competitivo crucial. Mejorar los enfoques prácticos en la normativa de seguridad de la información no solo protegerá a Procter & Gamble contra amenazas cibernéticas, sino que también fortalecerá su reputación como una empresa comprometida con la protección de datos de clientes y socios comerciales, lo que potencialmente generará nuevas oportunidades de negocio.

¿Cómo garantizamos el cumplimiento de la sostenibilidad en nuestra organización? Inicialmente lo hacemos mediante la Gobernanza, estableciendo procesos, procedimientos, prácticas y políticas de negocio responsable que permitan el cumplimiento sostenido de nuestros objetivos de forma ética y transparente. El desarrollo integral y constante de nuestros colaboradores, basado en el crecimiento profesional, social, financiero, físico y mental, es la clave de nuestro pilar Talento. Aseguramos el progreso de nuestros colaboradores gracias a los programas de educación, entrenamiento y salud, los cuales, además de impulsar a nuestros colaboradores, nos han llevado a una cultura de crecimiento social e igualdad de oportunidades.

1.2 DEFINICIÓN DEL PROBLEMA

En la empresa Procter & Gamble se ha identificado una problemática crítica relacionada con la obsolescencia y la insuficiente actualización de los protocolos de seguridad de la información en el departamento de Tecnologías de Información. A pesar de contar con medidas establecidas, estas no han sido revisadas ni adaptadas adecuadamente para enfrentar las nuevas amenazas y vulnerabilidades del panorama cibernético actual, lo que genera una brecha significativa entre las prácticas existentes y las demandas de un entorno empresarial cada vez más sofisticado y propenso a ciberataques. Esta situación se debe principalmente a la falta de actualización e implementación de protocolos y controles basados en las normas internacionales ISO 27001 e ISO 27002, la carencia de recursos técnicos especializados en ciberseguridad, la ausencia de un plan estructurado para la mejora continua, y una evaluación insuficiente de la infraestructura tecnológica y los procedimientos actuales.

1.2.1. Problemática

Se ha identificado una problemática relacionada con la obsolescencia de los protocolos de seguridad existentes. A pesar de contar con medidas de seguridad establecidas, estas no han sido actualizadas para hacer frente a las nuevas amenazas y vulnerabilidades en el panorama cibernético actual. Esta situación ha creado una brecha entre las prácticas actuales y las demandas de un entorno empresarial cada vez más sofisticado y propenso a ciberataques

Estas causas limitan la capacidad del departamento de TI para adaptarse proactivamente a las nuevas amenazas, y afectan la alineación de políticas con las regulaciones vigentes. Como consecuencia, Procter & Gamble enfrenta riesgos significativos de brechas de seguridad que podrían comprometer la confidencialidad, integridad y disponibilidad de la información, ocasionando pérdidas financieras, daño a su reputación, pérdida de confianza por parte de clientes y socios comerciales, y la posibilidad de sanciones legales por incumplimiento normativo. Por ello, resulta imperativo diseñar una propuesta integral para el fortalecimiento de la seguridad de la información, basada en las buenas prácticas de las normas ISO 27001 e ISO 27002, que permita reducir las brechas detectadas, proteger los activos informáticos y garantizar el cumplimiento normativo, enfocándose en el departamento de Tecnologías de Información de Procter & Gamble, con un horizonte de ejecución para el tercer cuatrimestre del año 2025.

1.2.2. Problema General

¿Cómo puede mejorarse la implementación de protocolos de seguridad de la información en el departamento de Tecnologías de Información de Procter & Gamble en la sede de Costa Rica, mediante el uso de estándares internacionales, ante la insuficiente adaptación de las prácticas actuales frente al cambiante panorama de amenazas cibernéticas?

1.2.3. Problemas Específicos

¿Cuáles son las deficiencias específicas de los protocolos actuales de seguridad de la información en el departamento de Procter & Gamble?

¿Qué aspectos del panorama de amenazas cibernéticas no están siendo abordados de manera adecuada por los protocolos existentes en Procter & Gamble?

¿Cómo afecta la falta de adaptación de las prácticas de seguridad de la información a la eficacia y eficiencia del departamento de Procter & Gamble?

¿Cuáles son los obstáculos internos y externos que dificultan la implementación efectiva de protocolos innovadores en seguridad de la información en Procter & Gamble?

1.3 OBJETIVOS DEL PROYECTO

1.3.1 Objetivo general

Diseñar una propuesta para el fortalecimiento de la seguridad de la información, basados en la metodología de las normas ISO 27001 e ISO 27002, en el departamento de Tecnologías de Información de la empresa Procter & Gamble en la sede de Costa Rica, con el fin de reducir brechas de seguridad, proteger los activos informáticos y garantizar el cumplimiento normativo frente a las amenazas cibernéticas actuales durante el tercer cuatrimestre del año 2025.

1.3.2 Objetivos específicos

1) Analizar las políticas y procedimientos actuales de seguridad de la información en el departamento de Tecnologías de Información de Procter & Gamble, basándose en los lineamientos establecidos por la norma ISO 27001, para identificar brechas, debilidades y oportunidades de mejora que permitan orientar acciones correctivas.
2) Evaluar la infraestructura tecnológica existente en el departamento de IT de Procter & Gamble, basándose en los lineamientos establecidos por la norma ISO 27002, con el propósito de detectar vulnerabilidades y riesgos que comprometan la integridad y disponibilidad de los activos de información.

3) Diseñar una propuesta de mejora integral para los procedimientos de seguridad de la información y la infraestructura tecnológica, fundamentada en las buenas prácticas de ISO 27001 e ISO 27002, que permita fortalecer la gestión de la seguridad de la información en el tercer cuatrimestre del año 2025.

1.4 ALCANCES Y LIMITACIONES

1.4.1 Alcances

El alcance de este proyecto comprende el análisis y diseño de una propuesta para el fortalecimiento de la seguridad de la información en el departamento de Tecnologías de Información de Procter & Gamble en la sede de Costa Rica, con base en las normas ISO 27001 e ISO 27002. A continuación, se describen los entregables relacionados con cada uno de los objetivos específicos planteados:

1) **El primer entregable del proyecto es un diagnóstico de las políticas y procedimientos actuales de seguridad de la información,** el cual incluye la recopilación y revisión documental de las normas, lineamientos, procesos y controles implementados actualmente en el departamento de IT. Este diagnóstico permitirá identificar brechas, desviaciones o ausencias respecto a los controles exigidos por las buenas prácticas establecidas en las normas ISO/IEC 27001 e ISO/IEC 27002.
2) **El segundo entregable consiste en una evaluación de la infraestructura tecnológica existente,** considerando los recursos físicos, lógicos y organizacionales que soportan la seguridad de la información en la empresa. La evaluación tomará en cuenta aspectos como la arquitectura de red, servidores, mecanismos de respaldo, control de accesos, gestión de incidentes, y otros elementos críticos, permitiendo identificar puntos vulnerables o áreas de oportunidad dentro del entorno tecnológico actual.
3) **El tercer entregable es una propuesta de mejora integral,** la cual incluye recomendaciones específicas para la actualización de políticas, procedimientos y controles, así como sugerencias de adecuación o fortalecimiento de la infraestructura tecnológica. Esta propuesta se estructurará con base en los lineamientos de las normas ISO 27001 e ISO 27002, y estará orientada a reducir las brechas identificadas, cumplir con los requerimientos normativos, y elevar el nivel de madurez en la gestión de la seguridad de la información dentro del área de IT.

1.4.2 Limitaciones

El desarrollo de este proyecto presenta ciertas limitaciones derivadas del contexto institucional, normativo y operativo en el que se llevará a cabo. Estas limitaciones no impiden su ejecución, pero definen claramente el marco dentro del cual se desarrollará la investigación y la propuesta. A continuación, se detallan:

1) **Acceso restringido a documentación confidencial:** Debido a las políticas de seguridad y confidencialidad de la empresa Procter & Gamble, es posible que no se tenga acceso completo a todos los procedimientos, informes o controles implementados actualmente. Esto limitará el análisis a la información que la organización esté dispuesta a compartir, lo cual puede influir en el nivel de profundidad de ciertos apartados del diagnóstico.
2) **Restricciones normativas internas de la empresa:** El proyecto deberá ajustarse a las normativas, directrices y políticas internas vigentes en Procter & Gamble. Esto significa que cualquier propuesta elaborada deberá estar alineada con los marcos organizacionales ya establecidos, sin poder modificar o proponer elementos que contradigan dichas políticas.
3) **Dependencia del nivel de colaboración del personal interno:** La recopilación de información necesaria para los diagnósticos dependerá de la disponibilidad y disposición del personal del área de TI para participar en entrevistas, encuestas o reuniones. Aunque se procurará obtener la información requerida, la participación limitada de los involucrados podría afectar la amplitud del análisis.

1.5 Cronograma de Actividades

Nivel 1 Etapa 1: Preparación y planificación del proyecto

Nivel 2 Definición de objetivos y alcance.

Nivel 2 Recopilación y revisión de documentos relevantes sobre la situación actual de seguridad de la información en Procter & Gamble.

Nivel 3 Definición de entregables.

Nivel 3 Redacción de objetivos.

Nivel 1 Etapa 2: Diagnóstico de políticas y procedimientos actuales

Nivel 2 Recopilación de datos.

Nivel 2 Recolectar información sobre las políticas y procedimientos de seguridad de la información en el departamento de Tecnologías de Información de Procter & Gamble.

Nivel 3 Análisis de brechas y debilidades.

Nivel 3 Identificar desviaciones respecto a los controles exigidos por las normas ISO 27001 e ISO 27002.

Nivel 3 Documentar los hallazgos y resultados de la evaluación de políticas y procedimientos actuales.

Nivel 1 Etapa 3: Evaluación de la infraestructura tecnológica

Nivel 2 Análisis de recursos físicos y lógicos.

Nivel 2 Evaluar arquitectura de red, servidores, mecanismos de respaldo, control de accesos y gestión de incidentes.

Nivel 3 Identificación de vulnerabilidades.

Nivel 3 Detectar puntos vulnerables que comprometan la integridad y disponibilidad de los activos de información.

Nivel 3 Documentar las áreas de oportunidad dentro del entorno tecnológico actual.

Nivel 1 Etapa 4: Diseño de propuesta de mejora integral

Nivel 2 Desarrollo de recomendaciones específicas.

Nivel 3 Diseñar mejoras para políticas, procedimientos y controles basados en ISO 27001 e ISO 27002.

Nivel 3 Proponer adecuaciones para el fortalecimiento de la infraestructura tecnológica.

Nivel 3 Estructurar la propuesta orientada a reducir brechas identificadas y garantizar cumplimiento normativo.

Nivel 1 Etapa 5: Definición de métricas y plan de monitoreo

Nivel 2 Establecimiento de indicadores clave de desempeño.

Nivel 3 Definir métricas para medir la efectividad de las mejoras propuestas.

Nivel 3 Diseñar mecanismos de seguimiento y control continuo.

Nivel 3 Proponer metodología de análisis y ajuste para mejora continua de la seguridad de la información.

Nivel 1 Etapa 6: Documentación y presentación de resultados

Nivel 2 Elaboración de documentación técnica.

Nivel 3 Consolidar diagnósticos, evaluaciones y propuesta de mejora integral.

Nivel 3 Preparar recomendaciones para capacitación del personal del departamento de TI.

Nivel 3 Documentar lecciones aprendidas y conclusiones del proyecto.

Nivel 1 Etapa 7: Evaluación final y cierre del proyecto

Nivel 2 Evaluación de resultados.

Nivel 2 Verificar el cumplimiento de objetivos específicos planteados.

Nivel 3 Validación de entregables.

Nivel 3 Confirmar que los tres entregables principales han sido completados satisfactoriamente.

Nivel 3 Cierre del proyecto.

Nivel 3 Formalizar el cierre del proyecto y entregar los resultados al equipo de dirección de Procter & Gamble.

CAPÍTULO II: MARCO TEÓRICO

2.1 CONCEPTOS GENERALES

En el desarrollo de este capítulo, se presenta una revisión de los conceptos esenciales que permitirán a los lectores comprender el proyecto de manera integral. El propósito es construir una base de conocimientos sólida que facilite la comprensión de los temas que se abordarán posteriormente.

El contenido se ha estructurado en tres secciones principales: en primer lugar, se expondrán los conceptos generales, que abarcan términos aplicables a cualquier tipo de investigación. A continuación, se desarrollarán los conceptos informáticos, enfocados específicamente en el área de ciberseguridad, dado que este proyecto se enmarca en el campo de la informática. Finalmente, se presentará la sección de conceptos y herramientas técnicas, elementos fundamentales que se aplicarán durante la fase práctica del proyecto.

2.1.1 ¿Qué son los sistemas de información?

Los sistemas de información se componen de diversos procesos y elementos que trabajan coordinadamente para lograr un objetivo específico. Existen múltiples tipos de sistemas y tecnologías asociadas. Según (Laudon, 2016)un sistema de información se define como un "conjunto de componentes interrelacionados que colaboran para reunir, procesar, almacenar y distribuir información que apoya la toma de decisiones, la coordinación, el control, el análisis y la visualización en una organización". Estos componentes incluyen personas, datos, actividades y recursos tecnológicos que operan de manera integrada para satisfacer las necesidades informativas de la organización.

Esta perspectiva resalta el papel fundamental que desempeñan los sistemas de información en la gestión eficaz de los recursos organizacionales y en los procesos de toma de decisiones dentro de empresas como Procter and Gamble. Cada uno de los elementos que conforman estos sistemas opera de forma integrada para procesar y distribuir la información, garantizando así que las necesidades informativas de la organización se cubran de manera óptima.

2.1.2 ¿Qué son estrategias

Según (Mintzberg, 1987)"la estrategia es un patrón en una corriente de decisiones o acciones; específicamente, se refiere a la consistencia en el comportamiento, ya sea intencional o no". Las estrategias en el ámbito tecnológico constituyen planes estructurados que orientan la toma de decisiones y las acciones dentro de entornos digitales, buscando cumplir con propósitos determinados. Estas funcionan como directrices para el desarrollo, la puesta en marcha y la administración de herramientas tecnológicas que mejoren el desempeño, la productividad y la capacidad de innovación en las organizaciones. En síntesis, una estrategia tecnológica representa el plan maestro que establece la manera de aprovechar la tecnología para conseguir objetivos concretos.

De igual manera, se enfatiza el concepto de estrategia en función de los propósitos de este proyecto, en el cual se establecerá un plan innovador orientado a proteger la información y mantener la confidencialidad de la empresa.

2.1.3 ¿Qué son protocolos?

Los protocolos informáticos representan un conjunto estructurado de reglas y convenciones que establecen el formato y la gestión de las interacciones entre dispositivos conectados en una red o sistema de comunicación, facilitando el intercambio de información entre ellos. De esta manera, el protocolo constituye el marco que determina la semántica comunicativa, así como los mecanismos de detección y corrección de errores, especificando de manera precisa la forma en que debe realizarse el intercambio de datos.

Es fundamental adherirse rigurosamente a estas normas, ya que de otro modo un equipo no podrá establecer comunicación con otros dispositivos de la red. Las redes informáticas e Internet emplean diversos protocolos de manera extensiva para ejecutar múltiples funciones comunicativas. (Tanenbaum, 2011)

¿Para qué sirve un protocolo informático?

- Interoperabilidad

La ausencia de protocolos imposibilitaría la interoperabilidad entre sistemas. Por ejemplo, si una página web empleara un protocolo completamente distinto a HTTP para transmitir contenido, el navegador sería incapaz de interpretarlo y el usuario no podría acceder a la información.

- Regular el control de flujo

Permite gestionar la velocidad de transmisión de información entre dos equipos, evitando así que un transmisor de alta velocidad sature a un receptor con menor capacidad de procesamiento.

- Administrar congestiones

Gestiona la saturación en la red, definida como el deterioro en la calidad del servicio de red cuando algún enlace procesa un volumen de datos superior a su capacidad operativa.

- Administrar la verificación de errores

Controla los diversos mecanismos que permiten la entrega correcta de datos cuando se utilizan canales de comunicación con baja confiabilidad.

Es importante destacar que estos protocolos determinan la manera en que los datos deben ser enviados, recibidos y procesados para garantizar una comunicación efectiva y libre de errores. Son fundamentales para el funcionamiento de las redes y los servicios en línea, asegurando la compatibilidad y la protección en la transferencia de datos.

2.1.4 Mitigaciones

La mitigación implica la aplicación de diferentes técnicas y enfoques orientados a reducir los niveles de riesgo hasta rangos tolerables. Mediante la implementación de medidas destinadas a contrarrestar amenazas y contingencias, una organización incrementa su capacidad para prevenir y minimizar eventos adversos.

Diversos autores han señalado lo siguiente:

La mitigación de riesgos constituye una fase fundamental dentro del proceso de gestión de riesgos. Se define como el conjunto de acciones y estrategias diseñadas para identificar, evaluar y reducir la probabilidad de ocurrencia o el impacto potencial de eventos adversos que puedan afectar los objetivos organizacionales.

El propósito de la mitigación no consiste en la eliminación total de las amenazas, sino en desarrollar planes de contingencia ante eventos inevitables y disminuir su repercusión en la operatividad empresarial. Entre los diversos tipos de riesgos potenciales se encuentran las vulnerabilidades tecnológicas, los fenómenos naturales como inundaciones o terremotos, la volatilidad económica, las implicaciones jurídicas, las deficiencias en la planificación estratégica y los incidentes operacionales. (Stoneburner, 2002)

Es fundamental destacar que contar con un programa de mitigación de riesgos adecuadamente estructurado permite a la organización estar mejor preparada para responder ante incidentes de seguridad y reducir significativamente sus consecuencias.

2.2 CONCEPTOS INFORMÁTICOS

Los conceptos informáticos son cruciales para la ejecución y consolidación efectiva de proyectos en el área tecnológica, ya que facilita la comprensión de los términos técnicos utilizados en el campo de las tecnologías de información. De esta manera, profesionales provenientes de otras áreas pueden acceder, entender los mecanismos y valorar la trascendencia de la ciberseguridad en el entorno empresarial.

2.2.1 Seguridad de la información

Según (Whitman, 2018), la seguridad de la información constituye el conjunto de medidas destinadas a salvaguardar los activos informacionales críticos de una entidad (incluyendo registros digitales, documentación física, soportes tangibles e incluso comunicaciones verbales) frente al acceso indebido, la exposición no consentida, el uso inadecuado o la modificación no autorizada. En el contexto actual, la protección de información en formato digital, también conocida como "seguridad de datos", concentra la mayor parte de los esfuerzos de los especialistas en esta disciplina, constituyendo el enfoque central del presente análisis.

Conforme a lo planteado, en la era contemporánea los datos constituyen el motor fundamental de la economía globalizada, representando un activo de valor incalculable para las entidades. Resguardar esta información resulta esencial no únicamente para la integridad operativa de la organización, sino también para preservar la credibilidad ante clientes y aliados estratégicos.

Ante el incremento exponencial de las vulnerabilidades cibernéticas, la protección de activos informacionales digitales se ha posicionado como una prioridad estratégica. Los especialistas en seguridad informática concentran sus esfuerzos en desarrollar estrategias integrales que contemplen tanto la prevención como la gestión efectiva de incidentes de seguridad.

En este escenario, la aplicación de normativas de seguridad estrictas y la incorporación de soluciones tecnológicas de vanguardia resultan indispensables. Las entidades deben garantizar que sus infraestructuras de protección se mantengan actualizadas y posean la capacidad de afrontar amenazas novedosas y en constante transformación. Adicionalmente, resulta imperativo promover una mentalidad organizacional orientada a la seguridad, donde el personal en su totalidad comprenda las directrices óptimas de protección y la trascendencia de salvaguardar los recursos informacionales.

Paralelamente, la administración de riesgos desempeña un rol fundamental. La identificación y valoración de riesgos latentes faculta a las organizaciones para implementar acciones preventivas orientadas a neutralizar estas amenazas antes de que escalen a situaciones críticas. La integración de tecnología avanzada, normativas eficaces y una cultura organizacional sólida en materia de seguridad puede facilitar a las entidades la protección de su información y el mantenimiento de una posición competitiva favorable en el mercado internacional.

En síntesis, la seguridad de la información representa una disciplina dinámica y en permanente transformación, motivada por la necesidad imperante de proteger activos informacionales valiosos en un ecosistema progresivamente digitalizado. Al implementar un enfoque holístico que integre tecnología, políticas organizacionales y capacitación continua, las entidades pueden resguardar eficazmente su información y garantizar su sostenibilidad en un contexto globalizado.

2.2.2 Programas de seguridad de la información

Los especialistas en este campo implementan fundamentos de seguridad en las infraestructuras informacionales mediante el diseño de esquemas destinados a la protección de datos. Estos esquemas comprenden un conjunto de normativas, mecanismos de defensa y estrategias estructuradas para establecer y sostener la seguridad informacional de forma eficaz.

Detección de vulnerabilidades. Una vulnerabilidad representa cualquier punto débil presente en la estructura de tecnologías de información (TI) que los atacantes pueden explotar para conseguir acceso ilegítimo a la información. A modo de ejemplo, los ciberdelincuentes pueden capitalizar fallos en el software para insertar programas maliciosos o código dañino en aplicaciones o servicios auténticos.

Los individuos también pueden constituir fuentes de vulnerabilidad en las infraestructuras informacionales. Por ejemplo, los atacantes pueden engañar a los usuarios para que revelen datos sensibles mediante técnicas de manipulación social como los correos electrónicos fraudulentos.

Frecuentemente, los expertos en seguridad informacional recurren a pruebas de intrusión controlada, simulando ataques contra sus propias plataformas, con el objetivo de descubrir estas debilidades. (Stallings, 2018)

En concordancia con lo expuesto, la detección de vulnerabilidades constituye un componente fundamental en la administración de la seguridad informacional. Estos procedimientos se responsabilizan del análisis exhaustivo de infraestructuras y redes, evaluación de configuraciones, mantenimiento actualizado de plataformas, pruebas de intrusión, supervisión permanente, entre otros mecanismos. Estos métodos conforman el fundamento para el establecimiento de programas robustos de protección informacional. Los programas, que abarcan políticas, salvaguardas y estrategias particulares, están diseñados para aplicar principios de seguridad de forma comprehensiva. Al detectar y atender las vulnerabilidades de manera anticipada, las entidades pueden reforzar sus mecanismos de defensa y resguardarse contra eventuales agresiones, asegurando la protección de sus activos informacionales y la operatividad ininterrumpida de sus procesos.

Identificación de amenazas: una amenaza representa cualquier factor que pueda poner en riesgo la confidencialidad, integridad o accesibilidad de una infraestructura informacional.

Una amenaza digital es aquella que aprovecha una debilidad en el entorno tecnológico. Por ejemplo, un ataque de saturación de servicios (DoS) constituye una amenaza cibernética donde los agresores inundan con solicitudes masivas segmentos del sistema informacional corporativo, ocasionando su colapso.

Las amenazas pueden también manifestarse de forma tangible. Los fenómenos naturales adversos, las agresiones físicas o armadas, e inclusive las averías en componentes físicos se contemplan como amenazas para la infraestructura informacional empresarial. (Stallings, 2018) En conclusión, las amenazas hacia las plataformas informacionales pueden clasificarse como digitales o tangibles, y cada categoría demanda tácticas particulares para su neutralización. Comprender y prever estas amenazas resulta fundamental para resguardar los recursos informacionales y asegurar la continuidad operativa corporativa.

2.2.3 Tipos de seguridad de la información

2.2.3.1 Seguridad en red

Esta capa de protección impide que individuos malintencionados o sin autorización puedan ingresar a la infraestructura de red corporativa. Si un atacante logra penetrar la red organizacional, puede provocar que los usuarios legítimos pierdan acceso a la información almacenada en ella, comprometiendo todos los aspectos operativos de la entidad. Una interrupción en los servicios tecnológicos puede resultar tan perjudicial como la exposición de datos sensibles o el hurto de información económica.

2.2.3.2 Seguridad en internet

Los sistemas de filtrado de tráfico ofrecen protección en línea, resguardando la información procesada mediante navegadores web o programas informáticos. Cualquier software nocivo que intente infiltrarse en el sistema a través de una conexión de red será identificado y bloqueado. Esta medida resulta fundamental considerando el creciente uso de navegadores y aplicaciones para gestionar volúmenes significativos de información confidencial.

2.2.3.3 Seguridad en la nube

La protección de entornos cloud constituye un componente esencial dentro de las soluciones de seguridad tecnológica. Se ha posicionado rápidamente como una de las áreas prioritarias en materia de seguridad digital, dado que gran parte de los datos confidenciales se almacenan actualmente en infraestructuras cloud. Esta protección se logra mediante el aseguramiento de aplicaciones SaaS (Software como Servicio) utilizadas en equipos personales, así como en el empleo de servicios de nube compartida.

2.2.3.3 Seguridad de terminales

La protección de dispositivos finales está diseñada para resguardar equipos individuales como teléfonos inteligentes, computadoras portátiles y tabletas. Esta puede incorporarse dentro del sistema operativo del equipo, previniendo que el dispositivo establezca conexión con redes potencialmente riesgosas. Asimismo, evita que el dispositivo transfiera información directamente desde la red corporativa hacia internet. (Tipton, 2020)

En síntesis, la seguridad tecnológica comprende múltiples capas de protección destinadas a resguardar las infraestructuras y datos organizacionales. De esta manera, previene ingresos indebidos y protege contra interrupciones operativas que pueden resultar tan dañinas como la exposición de información. En el contexto digital, se enfoca en el empleo de sistemas de filtrado para proteger datos procesados mediante navegadores y programas, bloqueando software malicioso. Adicionalmente, la protección cloud se ha transformado en prioridad debido al almacenamiento masivo de información personal, asegurando tanto aplicaciones de software como servicios públicos. Finalmente, la seguridad de dispositivos finales busca proteger equipos personales mediante la integración de software especializado que previene conexiones a redes peligrosas y la transferencia no autorizada de información. Estas capas de protección resultan fundamentales para preservar la integridad, confidencialidad y accesibilidad de la información en el ecosistema digital contemporáneo.

2.2.4 Control de la seguridad de la información

El control de la seguridad informacional constituye un conjunto de medidas y herramientas tecnológicas diseñadas para resguardar los activos de información y las infraestructuras tecnológicas de una entidad frente a accesos ilegítimos, utilización inadecuada, exposición no

autorizada, modificación o eliminación. Estos mecanismos de control resultan fundamentales para asegurar la confidencialidad, integridad y disponibilidad de los recursos informacionales.

Tabla 1

Controles de seguridad de la información

Control	Descripción	Ejemplos
Preventivo	Busca impedir la materialización de eventos no deseados.	Barreras de protección perimetral o sistemas de filtrado antivirus en servidores de correo electrónico.
Detección	Busca identificar eventos no deseados una vez que han sucedido.	Sistemas de detección de intrusiones de red o algoritmos de verificación para identificar modificaciones en archivos del sistema.
Disuasivo	Busca desalentar a los individuos de infringir deliberadamente las normativas o protocolos de seguridad.	Advertencia de terminación laboral por incumplimiento de políticas de seguridad o bloqueo de accesos tras múltiples intentos fallidos de autenticación.
Correctivo	Busca resolver las condiciones que facilitaron la actividad no autorizada o restablecer el sistema a su estado previo al incidente.	Ajuste automático de configuraciones del cortafuegos o eliminación de malware y actualización de sus patrones de detección.
Recuperativo	Busca restituir los recursos comprometidos y asistir a la organización en la recuperación de pérdidas financieras	Sistemas de respaldo de información o estrategias de continuidad operacional y recuperación ante desastres.

	ocasionadas por el incidente de seguridad.	

Nota:Adaptado de Computer and Information Security Handbook *(3rd ed.), por J. R. Vacca, 2017, Morgan Kaufmann Publishers.*

En la tabla uno se puede observar la implementación efectiva de controles, la cual resulta esencial para resguardar los activos digitales organizacionales. Contribuye a prevenir y reducir los riesgos de seguridad, garantiza el cumplimiento de marcos regulatorios y normativos, para preservar la credibilidad ante clientes y aliados estratégicos. Adicionalmente, un esquema sólido de control de seguridad informacional es fundamental para asegurar la operatividad ininterrumpida del negocio y proteger la imagen corporativa en un ecosistema digital progresivamente hostil.

2.2.5 Concepto de la ciberseguridad

La ciberseguridad constituye el conjunto de prácticas orientadas a resguardar infraestructuras tecnológicas, redes de comunicación y aplicaciones informáticas frente a agresiones digitales. Habitualmente, estas ofensivas cibernéticas buscan obtener acceso ilegítimo, alterar o eliminar datos sensibles; coaccionar a los usuarios mediante la interrupción de las operaciones empresariales.

En el contexto actual, la adopción de estrategias de protección digital se justifica debido a que la cantidad de dispositivos interconectados supera el número de personas y los agresores demuestran creciente sofisticación en sus métodos. (Easttom, 2021)

La ciberseguridad representa una disciplina fundamental en el ecosistema digital contemporáneo, puesto que salvaguarda los recursos más críticos tanto de las entidades como de los individuos, garantizando la operatividad sostenida del negocio y la confianza de los usuarios en la utilización de plataformas tecnológicas digitales.

2.2.6 Estándares de ciberseguridad

Se refiere a los marcos normativos y directrices ISO vinculados con la ciberseguridad y la protección de activos informacionales. Los marcos ISO constituyen estándares elaborados y

difundidos por la Organización Internacional de Normalización (ISO). Tanto ISO como IEC (Comisión Electrotécnica Internacional) representan las entidades de referencia en materia de estandarización global. Mediante comités técnicos integrados por representantes de organismos miembros de ambas instituciones, se desarrollan estándares internacionales formulados con el propósito de regular procedimientos específicos en ámbitos como la seguridad informacional.

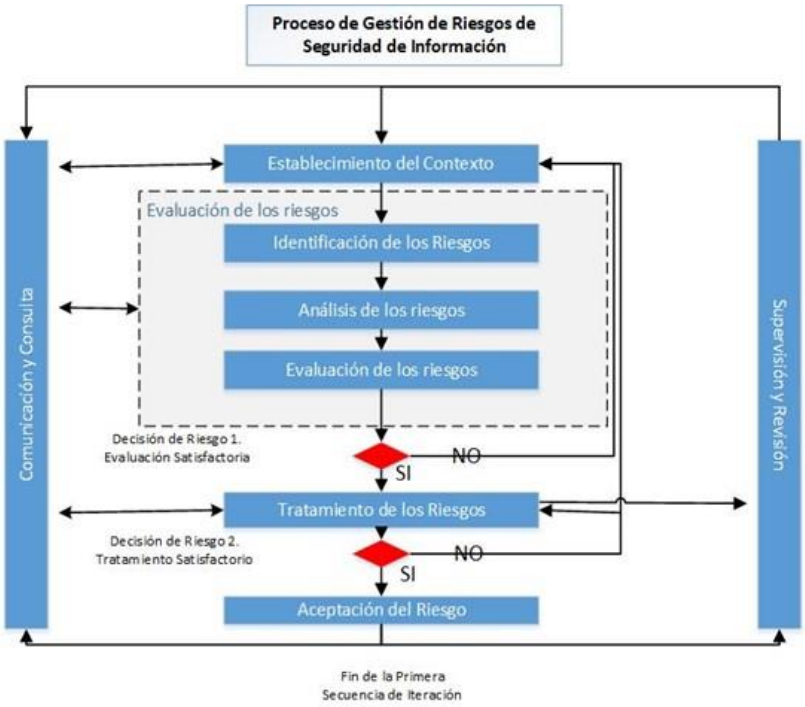
Estos marcos normativos representan, en la actualidad, un componente esencial dentro del sistema de conformidad organizacional, confiriendo prestigio y validación internacional a las entidades. El valor distintivo que proporcionan las implementaciones de estándares ISO a las organizaciones respecto a su competencia se fundamenta en que dichos marcos certificados son sometidos a revisiones y auditorías periódicas para verificar su observancia, generando que la percepción de partes interesadas como clientes o inversores se eleve significativamente.

Los marcos ISO se designan numéricamente de manera progresiva según su finalidad y se clasifican en familias para agrupar aquellos que aborden aspectos de naturaleza similar. El propósito de estos estándares y directrices consiste en identificar metodologías, lineamientos, orientaciones, formación, entre otros elementos, en función de su objetivo (seguridad, continuidad operativa, calidad, entre otros). (Von Solms, 2013)

En concordancia con lo expuesto, los estándares de ciberseguridad resultan fundamentales para establecer un modelo robusto y uniforme en la salvaguarda de información. Implementar y observar estos marcos normativos faculta a las organizaciones para administrar sus vulnerabilidades de ciberseguridad de forma más efectiva y asegurar la protección de sus recursos críticos en un ecosistema digital progresivamente complejo.

El SGSI (Sistema de Gestión de Seguridad de la Información) constituye una herramienta que facilita obtener una perspectiva integral de todas las áreas que requieren supervisión constante. En la mayoría de los casos, estos sistemas se fundamentan en estándares de ciberseguridad.

Ilustración 1 Proceso creación SGSI



Nota: Diagrama de creación del proceso SGSI

Fuente: (Researchgate, 2020)

En la ilustración uno se presenta una diagrama de flujo, donde se identifican las etapas fundamentales para la construcción de un sistema de seguridad informacional, contemplando desde la evaluación inicial hasta la elaboración e implementación operativa de sistemas de resguardo de información.

2.2.6.1 La ciberseguridad y las normas ISO

A continuación, se resaltan algunos de los marcos normativos ISO más significativos en este ámbito:

ISO 27001

Define los lineamientos para un Sistema de Gestión de Seguridad Informacional (SGSI), resguardando los activos de información frente a vulnerabilidades y asegurando su confidencialidad, integridad y accesibilidad.

ISO 27002

Ofrece un compendio de directrices óptimas para la aplicación de mecanismos de protección de información, contemplando aspectos como sensibilización del personal, supervisión de recursos y administración de permisos de acceso.

ISO 27005

Se enfoca en el análisis y administración de vulnerabilidades relacionadas con la seguridad informacional, suministrando orientaciones para la detección, evaluación y mitigación de riesgos.

2.2.7 Pilares de la ciberseguridad

Ante el incremento significativo de ofensivas digitales y criminalidad informática, el resguardo de información se ha posicionado como una necesidad prioritaria para las entidades. No obstante, previo a la adopción de tácticas orientadas a fortalecer la protección informacional, resulta fundamental comprender los fundamentos que la sostienen: confidencialidad, integridad y disponibilidad. Estos tres principios son indispensables para la salvaguarda de datos y representan pilares esenciales dentro de las directrices organizacionales de tecnologías de información, cuya finalidad primordial consiste en facilitar un funcionamiento óptimo de los procedimientos operativos.

Ilustración 2 ¿CIA seguridad de la información

Nota: Importancia de los pilares de la ciberseguridad

Fuente: (Comillas, 2023)

A continuación, se detalla la relevancia de estos fundamentos para la protección de información corporativa y se analiza cómo las tecnologías emergentes pueden potenciar esta seguridad.

2.2.7.1 Confidencialidad

Este principio está vinculado con la privacidad de los activos informacionales, abarcando las medidas implementadas con el propósito de garantizar que la información sensible y reservada se mantenga resguardada y no sea comprometida mediante ataques digitales, actividades de espionaje o cualquier otra modalidad de delito informático. (Stallings, 2018)

La referencia anterior establece que el propósito fundamental consiste en asegurar que los datos sean accesibles exclusivamente para individuos con las credenciales apropiadas. Esto conlleva proteger información crítica y prevenir su exposición no autorizada, ya sea de forma deliberada o involuntaria.

2.2.7.2 Integridad

La integridad constituye el pilar de seguridad informacional que se relaciona con la preservación de la exactitud y coherencia de los datos, así como de las demás plataformas corporativas durante los procesos operativos o el ciclo vital del negocio. Desde la perspectiva de este elemento, resulta fundamental que los datos circulen o se conserven de manera idéntica a su creación, sin que exista manipulación externa que pueda comprometer, deteriorar o alterar la información.

En otras palabras, la integridad asegura la autenticidad de la información, estableciendo que los datos no pueden modificarse sin aprobación previa. Sin embargo, en caso de producirse una modificación indebida, imprevista o no planificada, la información puede verse afectada de manera irreparable. (Stallings, 2018)

Como se señala en la referencia, el objetivo de la integridad es asegurar que los datos permanezcan exactos, íntegros y libres de modificaciones no autorizadas durante su existencia, desde su generación y resguardo hasta su transmisión.

2.2.7.3 Disponibilidad

La disponibilidad implica que todos los componentes de la infraestructura tecnológica y los activos informacionales se encuentren en condiciones operativas óptimas, con la finalidad de que las personas con las credenciales apropiadas tengan acceso a la información cuando la necesiten.

Existen múltiples circunstancias que pueden comprometer la disponibilidad confiable de la información. Se pueden adoptar diversas medidas para mitigarlo, tales como: la implementación de redundancia en redes, servicios y aplicaciones, tolerancia a fallos en los equipos y procedimientos de actualización o mantenimiento de las plataformas tecnológicas.

2.2.8 Amenazas y vulnerabilidades de la seguridad de la información

(Whitman, 2018) señalan que:

Una vulnerabilidad, en el contexto de las tecnologías de información, representa una debilidad o deficiencia en una infraestructura informacional que compromete la protección de los datos, potencialmente permitiendo que un agresor pueda afectar la integridad, disponibilidad o confidencialidad de esta información, además de otras dimensiones de seguridad relevantes para la entidad, tales como la trazabilidad o la autenticidad.

Por esta razón resulta imperativo detectarlas y eliminarlas con la mayor prontitud posible. Estas brechas pueden originarse de diversas fuentes, como defectos en el diseño, configuraciones inadecuadas o ausencia de procedimientos establecidos.

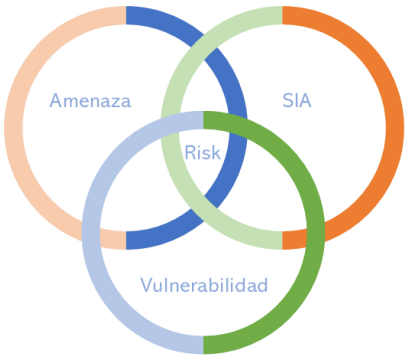
Por otro lado, una amenaza constituye cualquier acción que explota una vulnerabilidad para comprometer la seguridad de una infraestructura informacional. Es decir, representa un evento que podría generar un impacto adverso sobre algún componente del sistema.

Las amenazas pueden derivarse de agresiones digitales (fraude, sustracción de datos, malware), eventos físicos (siniestros, inundaciones) o descuidos y decisiones institucionales (gestión inadecuada de credenciales, ausencia de encriptación). Desde la perspectiva organizacional pueden clasificarse tanto como internas o externas.

Por consiguiente, las vulnerabilidades son las condiciones y características inherentes a los sistemas de una entidad que la tornan susceptible a las amenazas, como debilidades en mecanismos de seguridad o ausencia total de controles protectivos. La problemática radica en que, en el entorno real, si existe una vulnerabilidad, invariablemente habrá alguien que intentará aprovecharla, es decir, beneficiarse de su presencia.

En conclusion, se enfatiza la relevancia de identificar y atender las vulnerabilidades en las infraestructuras informacionales para prevenir que sean explotadas por amenazas, ya sean ataques digitales, sucesos físicos o fallos humanos. La prevención y reducción de vulnerabilidades resultan fundamentales para preservar la seguridad y resguardar los recursos organizacionales.

Ilustración 3 Riesgo de la seguridad de información



En la ilustración número ocho vemos las vulnerabilidades, amenazas y los sistemas informáticos, un cuarto elemento es que tanto impacto puede tener la unión de las vulnerabilidades y las amenazas sobre los sistemas informáticos

Fuente: (INCIB Chile, 2021)

2.2.9 Especialistas y sus roles en ciberseguridad

En el campo de la ciberseguridad, existen múltiples funciones especializadas que colaboran conjuntamente para resguardar las infraestructuras informacionales, redes y activos de datos de una entidad. A continuación, se describen algunas de las funciones más frecuentes y sus atribuciones:

2.2.9.1 Evaluador de seguridad

Un pentester, también denominado Analista de Pruebas de Penetración o Evaluador de Seguridad, es un especialista dedicado a ejecutar evaluaciones de seguridad en plataformas informáticas para detectar vulnerabilidades y debilidades. Su propósito fundamental consiste en replicar las metodologías y tácticas empleadas por agresores para valorar la resistencia de un sistema ante posibles intrusiones y ofensivas. (Engebretson, 2013)

2.2.9.2 Operador de equipo rojo

Los equipos rojos (Red Teams) emulan el comportamiento de atacantes, utilizando herramientas idénticas o equivalentes, aprovechando las vulnerabilidades de seguridad presentes en sistemas y aplicaciones (exploits), técnicas de movimiento lateral (transitar entre equipos comprometidos) y objetivos específicos (sistemas y aplicaciones) de la organización.

2.2.9.3 Equipo azul

Operan en el perfeccionamiento continuo de la protección, monitoreando eventos de seguridad informática, examinando sistemas y aplicaciones para identificar defectos y vulnerabilidades, y validando la eficacia de las medidas defensivas implementadas en la organización.

2.2.9.4 Equipo morado

Los equipos morados (Purple Team) funcionan para garantizar y optimizar la efectividad de los equipos rojo y azul. Logran esto mediante la integración de las estrategias y controles defensivos del equipo azul con las amenazas y vulnerabilidades descubiertas por el equipo rojo. Idealmente, no constituye un equipo independiente, sino una dinámica colaborativa entre ambos equipos. (Engebretson, 2013)

2.2.9.5 Ingeniero de ciberseguridad

Un ingeniero de ciberseguridad representa un profesional que diseña e implementa infraestructuras digitales seguras destinadas a proteger redes, portales web y otros recursos en línea contra agresiones cibernéticas maliciosas. Poseen conocimientos técnicos y experiencia en ingeniería de software, criptografía, protección de redes, administración de sistemas y análisis forense digital.

2.2.9.6 Auditor de ciberseguridad

Un auditor de ciberseguridad constituye un profesional capacitado para evaluar y examinar los sistemas y la infraestructura de protección de una entidad, con el objetivo de detectar posibles vulnerabilidades y riesgos de seguridad.

2.2.9.7 Arquitectos de ciberseguridad

Los arquitectos de seguridad colaboran estrechamente con arquitectos empresariales durante la creación y desarrollo de nuevas infraestructuras de red. En lugar de concentrarse en los procedimientos organizacionales como lo hace un arquitecto empresarial, se requiere que los arquitectos de seguridad supervisen meticulosamente la construcción de redes y aplicaciones. Conjuntamente, la red y las aplicaciones representan las fuentes primarias de riesgo de seguridad informacional. Los arquitectos de seguridad garantizan que se establezcan las medidas protectivas adecuadas desde las etapas iniciales.

2.2.9.8 Consultor de ciberseguridad

Un consultor de ciberseguridad es un especialista en la materia dedicado a implementar técnicas necesarias para ofrecer un rendimiento optimizado en el flujo informacional hacia las entidades, además de proporcionarles una protección reforzada. (Casey, 2011)

En su conjunto, estas funciones operan para construir una defensa integral y adaptable frente a las amenazas cibernéticas, protegiendo los activos digitales y asegurando la continuidad operativa y confianza en las infraestructuras organizacionales.

2.2.10 Estudio y análisis de situación actual

Antes de desarrollar el presente concepto, se debe aclarar que este diagnóstico de la situación actual se gestiona bajo la perspectiva del proyecto, es decir, constituye un diagnóstico

de las condiciones actuales en materia de ciberseguridad. A continuación, la definición del análisis situacional según (Bryson, 2018)

"Representa una valoración de los elementos del contexto interno y externo que probablemente ejercerán la mayor influencia sobre el futuro de la organización"

En síntesis, mediante el diagnóstico de la situación actual examinamos los elementos presentes en la actualidad, que potencialmente pueden constituir problemáticas futuras. Este diagnóstico debe incorporar todos los aspectos críticos para la organización, los cuales serán categorizados según su impacto en las operaciones de la compañía, puesto que sin realizar esta categorización es factible que se obtenga un inventario excesivamente extenso de posibles escenarios.

2.3 CONCEPTOS TÉCNICOS

Estos principios constituyen un cimiento sólido para asimilar las herramientas y técnicas que se utilizarán durante el desarrollo del proyecto de ciberseguridad, resultando apropiados tanto para expertos en la materia como para personas sin formación previa en el ámbito tecnológico.

2.3.1 Firewalls

El cortafuegos, denominado firewall en inglés, constituye un sistema de protección cuya finalidad es impedir accesos no autorizados hacia un sistema, particularmente accesos procedentes de redes externas. Simultáneamente, permite mantener la comunicación del dispositivo con otros servicios y sitios web que sí cuentan con autorización.

El firewall se posiciona en el punto de conexión entre Internet y un equipo o conjunto de equipos en red. Su mecanismo opera mediante el control de toda la información y el flujo de datos que el enrutador (router) transmite desde una red hacia otra. Si el cortafuegos, mediante un análisis rápido, determina que dichos datos cumplen con determinados criterios de seguridad y protocolo establecidos, autorizará su ingreso a la red. Si el firewall detecta alguna anomalía, actuará como una barrera y bloqueará dichos datos para impedir su conexión.

La evaluación de Firewalls representará un elemento fundamental en el desarrollo de este proyecto, debido al monitoreo y análisis mediante el cual se examinará la situación actual de esta herramienta y su implementación.

2.3.2 Backup

(Posey, 2016)señala que, en términos simples, un backup constituye una copia de respaldo de los datos. Esto implica que se genera una réplica de toda la información crítica almacenada en dispositivos, como computadoras o teléfonos móviles.

2.3.2.1 Backup incremental

A diferencia del respaldo completo, el backup incremental únicamente almacena las modificaciones efectuadas desde el último respaldo. En lugar de duplicar todos los archivos nuevamente, solo se respaldan los archivos alterados o incorporados recientemente. Esto convierte al backup incremental en un proceso más veloz que requiere menos capacidad de almacenamiento. No obstante, es fundamental considerar que, durante una restauración, se requerirán tanto el último backup incremental como el respaldo completo más reciente para recuperar la totalidad de los datos.

2.3.2.2 Backup diferencial

Similar al backup incremental, el respaldo diferencial también almacena exclusivamente las modificaciones realizadas desde el último backup. Sin embargo, a diferencia del backup incremental, el respaldo diferencial guarda todos los archivos modificados o añadidos desde el último backup completo. Esto significa que el volumen del backup diferencial aumentará conforme se efectúen más cambios, lo que puede demandar mayor capacidad de almacenamiento. Al igual que con el backup incremental, se necesitará tanto el último backup diferencial como el respaldo completo más reciente para una recuperación integral.

2.3.2.3 Backup continuo

El backup continuo representa un tipo de respaldo en tiempo real que almacena automáticamente las modificaciones realizadas en los archivos a medida que se ejecutan. Emplea tecnología de respaldo instantáneo para garantizar que los datos estén constantemente

respaldados y actualizados. Resulta especialmente útil cuando se trabaja en proyectos activos y se requiere mantener una copia de seguridad permanente sin necesidad de realizar respaldos manuales periódicos.

2.3.2.4 Backup local y en la nube

Se pueden efectuar respaldos o copias de seguridad tanto en dispositivos locales, tales como unidades de almacenamiento externas o servidores de red, como en servicios de almacenamiento cloud. Los backups locales proporcionan control directo sobre los datos y no dependen de conectividad a Internet. Por otra parte, los servicios de almacenamiento en la nube ofrecen la ventaja de poder acceder a los respaldos desde cualquier ubicación y dispositivo con conexión a Internet, lo que proporciona mayor flexibilidad y protección ante desastres físicos.

La ejecución regular de copias de seguridad resulta fundamental para la estrategia de defensa contra ataques de ransomware u otras ofensivas cibernéticas que puedan comprometer y secuestrar la información empresarial. Es esencial proteger tanto la información más reciente recopilada en los equipos como los grandes volúmenes de datos alojados en servidores.

Las copias de seguridad, o backups, constituyen medidas de protección prioritarias que optimizan el resguardo empresarial y minimizan el impacto de cualquier incidente de ciberseguridad, tanto en términos temporales como de magnitud. (Posey, 2016)

CAPITULO III: MARCO METODOLÓGICO

3.1 TIPO Y ENFOQUE DE LA INVESTIGACIÓN

3.1.1 Tipo de investigación

Este capítulo se desarrolla como una investigación de campo, dado que todo el trabajo se realizará directamente en el entorno laboral del departamento de IT. Durante este proceso, aplicaremos diferentes técnicas para recopilar información, principalmente a través de entrevistas con las personas responsables de cada proceso y mediante observaciones directas que nos permitan detectar las posibles vulnerabilidades de seguridad que existen en la compañía en el área de tecnologías de la información.

Además, se muestra el concepto tomado del libro: Metodología de la investigación, donde se explica la definición de la siguiente manera:

“Los instrumentos de recolección de datos en la investigación de campo tienen por objetivo capturar y organizar sistemáticamente la información vinculada al fenómeno seleccionado para su estudio. Constituyen, por consiguiente, herramientas que facilitan la observación y registro controlado de los fenómenos investigados." (Hernández Sampieri et al., 2014, p. 196)

Con esta investigación de campo buscamos identificar todos los eventos o situaciones que están generando el problema actual, para así poder determinar la solución más apropiada. La idea es resolver la situación eliminando las vulnerabilidades existentes y estableciendo procesos estandarizados que sigan las mejores prácticas de seguridad informática.

Como parte de la investigación, realizaremos entrevistas con los encargados de los distintos procesos que se llevan a cabo en el departamento de IT de Procter and Gamble de la sede en Costa Rica. Esto nos permitirá documentar, verificar y dar seguimiento a las actividades diarias del departamento. Necesitamos evaluar el estado actual de la infraestructura tecnológica, incluyendo aspectos como la red local (LAN), la red inalámbrica (WLAN), los cortafuegos (Firewalls) y la gestión del personal que desempeña distintas funciones en la empresa. Todo esto manteniendo siempre el enfoque principal de nuestra investigación: identificar qué factores podrían comprometer la infraestructura y poner en riesgo la información de la compañía.

3.1.2 Enfoque de la investigación

Esta investigación se desarrolla bajo un enfoque cualitativo, debido a que busca comprender de manera profunda la situación actual de la ciberseguridad en el departamento de IT. A través de técnicas como las entrevistas y las observaciones directas, se pretende identificar, analizar e interpretar las vulnerabilidades, los procesos y los factores de riesgo que existen actualmente en la infraestructura tecnológica de la empresa.

Como señalan Hernández Sampieri et al. (2014), el enfoque cualitativo "utiliza la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación" (p. 7). En este sentido, la investigación se enfoca en explorar y entender las debilidades de seguridad a través del análisis detallado de los procesos operativos, la infraestructura tecnológica y las prácticas del personal. Esto permitirá desarrollar estrategias de mejora que estén fundamentadas en la realidad operativa del departamento y que respondan efectivamente a las necesidades identificadas.

Este enfoque resulta especialmente apropiado para el presente estudio, ya que no solo se busca identificar qué vulnerabilidades existen, sino también comprender el contexto en el que se presentan, las razones por las cuales ocurren y cómo impactan en las operaciones diarias de la empresa. De esta manera, se podrá proponer soluciones más integrales y efectivas que consideren tanto los aspectos técnicos como los organizacionales de la ciberseguridad.

3.2 FUENTES Y SUJETOS DE INFORMACIÓN

En esta sección se identifican tanto las fuentes de información como las personas que aportarán datos importantes para el desarrollo del proyecto. Es fundamental trabajar con información confiable que nos ayude a entender bien la situación actual de la empresa y hacia dónde queremos llegar. Una buena selección de fuentes y sujetos es clave para asegurar que la solución que propongamos sea la más adecuada y esté respaldada con datos reales y actualizados.

3.2.1 Fuentes primarias

Las fuentes primarias son aquellas que nos dan información de primera mano, generada directamente durante la investigación. Como explican (Hernández Sampieri, 2014), estas fuentes "proporcionan datos de primera mano, pues se trata de documentos que incluyen los resultados de los estudios correspondientes" (p. 61). Para este proyecto, las fuentes primarias que utilizaré incluyen:

Entrevistas con el personal del departamento de IT: Se realizan entrevistas a los líderes del departamento, el equipo de Redes y el equipo de Ciberseguridad de Procter & Gamble en Costa Rica. Estas conversaciones me permitirán conocer de primera mano cómo funcionan los procesos actuales, qué vulnerabilidades han identificado y cuáles son sus necesidades específicas en cuanto a seguridad.

Observación directa en el lugar de trabajo: Se observará cómo funciona el departamento de IT en su día a día, evaluando el estado de la infraestructura tecnológica. Esto incluye revisar la red local (LAN), la red inalámbrica (WLAN) y los sistemas de cortafuegos (Firewalls) que tienen implementados.

Documentación interna de la empresa: Se revisarán las políticas de seguridad que existen actualmente, reportes de incidentes que hayan ocurrido, procedimientos que sigue el equipo, configuraciones de sistemas y cualquier otro documento técnico que me ayude a entender mejor la situación actual.

Análisis directo de la infraestructura: Se van a evaluar los sistemas, redes y equipos que usa la empresa para tener datos concretos sobre el estado real de la seguridad informática.

Todas estas fuentes primarias son fundamentales porque ayudan a entender la situación real de la empresa, no solo en teoría sino en la práctica, y así poder desarrollar una propuesta que realmente funcione para sus necesidades.

3.2.2 Fuentes secundarias

Las fuentes secundarias son aquella información que ya ha sido recopilada y publicada por otros investigadores Según (Sampieri, 2014), las fuentes secundarias se caracterizan por utilizar

datos que ya fueron recolectados previamente, lo que permite optimizar recursos de tiempo y costos (p. 61). Aunque no son datos que yo mismo genere, son muy útiles porque nos ahorran tiempo y nos dan acceso a conocimiento ya validado. Para este proyecto utilizaré:

Normas y estándares internacionales: Se basará en normativas reconocidas como ISO 27001, ISO 27002 .

Libros especializados: Se consultarán textos académicos sobre ciberseguridad y gestión de riesgos escritos por autores reconocidos como Whitman & Mattord, Stallings & Brown y Andress. Estos libros me darán el marco teórico necesario.

Artículos científicos: Se buscarán publicaciones en revistas especializadas que hablen sobre vulnerabilidades actuales, amenazas cibernéticas y casos de estudio que puedan aplicar a la situación de la empresa.

Documentación técnica: Se revisarán los manuales y guías que proporcionan los fabricantes del hardware y software que usa la empresa, ya que suelen incluir recomendaciones importantes de seguridad.

Reportes de organizaciones especializadas: Se consultarán informes de entidades como CERT y CCN-CERT, que están constantemente analizando las amenazas actuales y las tendencias en ciberseguridad.

Todas estas fuentes secundarias me ayudarán a tener una base sólida de conocimiento teórico y técnico para fundamentar las decisiones que se tomen y las propuestas que se desarrollen. Es importante mencionar que solo se utilizarán fuentes confiables, que estén bien referenciadas y que hayan sido validadas por la comunidad científica.

3.2.3 Sujetos de información

Los sujetos de información son las personas que me proporcionarán información valiosa para desarrollar este proyecto. En mi caso, trabajaré principalmente con colaboradores del departamento de IT de Procter & Gamble en Costa Rica, ya que son ellos quienes conocen a fondo la infraestructura tecnológica y los procesos que se manejan en la empresa.

A continuación detallo quiénes serán los sujetos que consultaré durante la investigación:

Tabla 2

Sujetos de información del proyecto

Puesto laboral	Profesión u oficio	Experiencia	Relación con el tema
Líder del departamento de IT	Se encarga de gestionar todo el departamento de tecnología, tomar decisiones estratégicas y reportar problemas importantes a la gerencia	Alta (más de 5 años trabajando en el área)	Alta - Me dará la visión estratégica de cómo se maneja la seguridad en la empresa y cuáles son las prioridades desde el punto de vista gerencial
Equipo de Redes	Manejan los incidentes técnicos del día a día, revisan el estado de la red y le dan el mantenimiento preventivo	Alta (entre 3 y 5 años en funciones similares)	Alta - Conocen muy bien los procesos operativos diarios y pueden identificar las vulnerabilidades relacionadas con el manejo de la red
Equipo de Ciberseguridad	Se dedican a proteger y monitorear toda la infraestructura, sistemas y activos digitales de la compañía, además de manejar los incidentes de seguridad	Alta (son especialistas en ciberseguridad)	Alta - Son los expertos directos en el tema que estoy investigando, tienen conocimiento técnico profundo de las amenazas que enfrenta la empresa y los controles que ya existen

Nota: Sujetos de información

Fuente: Elaboración propia

3.3 TÉCNICAS DE RECOLECCIÓN DE DATOS

Para la recolección de datos del proyecto se utilizarán entrevistas semiestructuradas como técnica principal, dirigidas al personal del departamento de TI con el fin de obtener información sobre el estado actual de la seguridad de la información, las brechas existentes y el nivel de cumplimiento con las normas ISO/IEC 27001 e ISO/IEC 27002. Como herramienta se empleará

una guía de entrevista elaborada en función de los dominios y controles definidos por dichas normas, lo que permitirá recopilar información de manera ordenada y confiable para analizar la situación actual y proponer acciones de mejora en la gestión de la seguridad de la información.

3.3.1 Entrevista

Las entrevistas constituyen una técnica esencial para obtener información detallada y confiable dentro del desarrollo del proyecto.

Según (Hernández Sampieri, 2014), la entrevista es una técnica cualitativa que permite recopilar datos a través de la interacción directa entre el investigador y los participantes, con el propósito de comprender percepciones, experiencias y opiniones relacionadas con un fenómeno específico. En este proyecto, la entrevista se utilizará para evaluar el nivel de madurez de la cultura de ciberseguridad en el departamento de Tecnologías de la Información, ya que facilita la recolección de información valiosa sobre las prácticas, actitudes y conocimientos del personal en materia de seguridad informática.

3.3.2 Observación

La ciberseguridad exige un seguimiento constante tanto de la infraestructura tecnológica como del comportamiento del personal dentro de la organización, ya que resulta fundamental evaluar aspectos relacionados con la seguridad física y la ingeniería social para prevenir posibles vulnerabilidades. En este proyecto, se aplicará la técnica de observación en los distintos procesos y prácticas del departamento de Tecnologías de la Información, con el propósito de identificar riesgos y recopilar información relevante. De acuerdo con Hernández Sampieri, Fernández Collado y Baptista (2014), la observación directa consiste en la recopilación sistemática de datos mediante la percepción directa del investigador sobre los hechos, comportamientos o condiciones tal como ocurren en su entorno natural, sin intervenir en ellos. En este sentido, la observación permitirá analizar las acciones y condiciones reales sin alterar el comportamiento de los participantes ni las dinámicas habituales, garantizando así la autenticidad de los resultados.

3.4 Variables de investigación

Las variables de investigación son componentes fundamentales dentro de cualquier estudio, ya que nos permiten identificar, analizar y medir los aspectos específicos que queremos entender o mejorar a lo largo del proyecto. En términos simples, una variable es cualquier característica, cualidad o propiedad que puede cambiar o variar, y que podemos observar o cuantificar para obtener información relevante.

Según (Hernández Sampieri, 2014), una variable es "una característica o propiedad que puede tomar diferentes valores y cuya variación puede ser observada o medida". Esto significa que las variables no solo nos ayudan a describir situaciones, sino que también nos permiten establecer relaciones y diferencias dentro del fenómeno que estamos estudiando.

En el contexto de este proyecto, las variables se definen cuidadosamente para reflejar los objetivos específicos que se han planteado, lo cual facilita mantener un enfoque claro y organizado durante todo el proceso de investigación. Así, cada variable representa un aspecto clave relacionado con el fortalecimiento de la gestión de seguridad de la información dentro del departamento de Tecnologías de la Información en Procter & Gamble. De esta manera, el análisis y la interpretación de los datos recopilados serán más precisos y útiles, permitiendo no solo evaluar la situación actual, sino también diseñar estrategias concretas que impulsen mejoras significativas en la seguridad y protección de la información en la empresa.

A continuación, se presenta una serie de tablas en las cuales se distribuyen las variables sujetas a estudio.

Tabla 3

Variables del proyecto

Objetivos	Variable	Descripción	Operación
1. Evaluar el estado actual de los protocolos de seguridad de la información en el departamento de TI de Procter & Gamble, identificando vulnerabilidades y áreas de mejora.	Diagnóstico de la situación actual	Investigación y análisis de los procesos y controles vigentes mediante entrevistas y observación directa.	Análisis de vulnerabilidades e infraestructura a través de entrevistas y observación en campo.
2. Diseñar nuevos protocolos de seguridad que atiendan las deficiencias detectadas y fortalezcan la postura de seguridad.	Identificación de áreas de mejora	Revisión detallada de procesos y controles con base en los resultados del diagnóstico.	Sesiones de análisis y desarrollo de propuestas para optimizar protocolos y reducir riesgos.
3. Establecer métricas de evaluación y monitoreo para medir la efectividad y el impacto de los nuevos protocolos de seguridad implementados, con el fin de garantizar su eficacia a largo plazo y realizar ajustes según sea necesario.	Evaluación del recurso humano	Aplicación de pruebas y evaluaciones para medir el nivel de concientización y madurez en ciberseguridad del personal.	Pruebas de ingeniería social y encuestas para medir conocimiento y prácticas de seguridad.
4. Desarrollar una propuesta de implementación de los protocolos diseñados en el área de TI.	Desarrollo de la mejora de procesos	Formalización y estandarización de procesos y políticas de seguridad de la información.	Elaboración de manuales y protocolos para la correcta aplicación y seguimiento de las medidas de seguridad.

Nota: Implementación y desarrollo del proyecto

Fuente: Elaboración propia

3.5 DISEÑO DE LA INVESTIGACIÓN

En esta sección se describen las etapas del proyecto, detallando la secuencia en la que se llevará a cabo cada fase de forma cronológica, con el objetivo de garantizar un desarrollo ordenado y coherente a lo largo de todo el proceso.

Tabla 4

Diseño de la investigación

1. Evaluar el estado actual	Verificación de la infraestructura existente
	Preparación de un informe con los datos recolectados
2. Detectar oportunidades de mejora	Revisión detallada de la documentación proporcionada
3. Examinar el recurso humano	Realización de entrevistas al personal de IT
	Análisis de la información obtenida durante las entrevistas
4. Diseñar la optimización de procesos	Desarrollo de la propuesta de seguridad.

Nota: Etapas de la implementación de la propuesta

Fuente: Elaboración propia

3.5.1 Etapas del proyecto

3.5.1.1 Situación actual

En la situación actual se busca describir de manera detallada el estado del departamento de IT en relación con la gestión de la seguridad de la información. El propósito es identificar las principales vulnerabilidades, brechas de cumplimiento y riesgos asociados al manejo de datos sensibles. Además, se pretende obtener una visión integral del nivel de madurez en seguridad dentro de la organización, considerando tanto la infraestructura tecnológica como los controles actuales implementados.

3.5.1.2 Identificación de áreas de mejora

En esta etapa se realiza un diagnóstico de los controles existentes frente a los requisitos establecidos por las normas ISO 27001 e ISO 27002. El objetivo es determinar los puntos críticos que requieren fortalecimiento, priorizando aquellos que representen mayores riesgos para la confidencialidad, integridad y disponibilidad de la información. Con base en este análisis, se podrán definir las acciones correctivas y preventivas más pertinentes para reducir las brechas detectadas.

3.5.1.3 Desarrollo de mejoras en los procesos

En función de los resultados obtenidos, se diseñarán propuestas de mejora enfocadas en optimizar los procesos internos relacionados con la gestión de la seguridad de la información. Estas acciones estarán alineadas con las buenas prácticas de la norma ISO 27002 y buscarán garantizar que los flujos operativos sean más seguros, eficientes y sostenibles, sin afectar la productividad ni la funcionalidad de los sistemas.

3.5.1.4 Propuesta de implementación

Finalmente, se presentará una propuesta de implementación estructurada conforme al ciclo de mejora continua (Planificar–Hacer–Verificar–Actuar), contemplado en la ISO 27001. Esta propuesta incluirá herramientas y estrategias para fortalecer el monitoreo, la gestión de incidentes, el registro de auditorías, la trazabilidad de accesos y el cumplimiento de políticas internas. Asimismo, se diseñará un plan de continuidad que permita mantener la operatividad de los sistemas críticos ante eventuales incidentes de seguridad o fallos tecnológicos.

3.6 MATRIZ DE COHERENCIA

Seguidamente, se presenta la matriz de la coherencia elaborada con la finalidad de cumplir con los objetivos desarrollados.

Tabla 5

Matriz de coherencia

Estudiante: Christopher Rivera Steller					
Objetivos	**Entregable**	**Fase, parte o etapa de la metodología del proyecto que posibilita la realización del entregable**	**Técnicas/métodos de recolección de la información**	**Instrumentos**	**Temas relacionados para marco teórico**
Objetivo principal					
Propuesta para el fortalecimiento de la seguridad de la información, basados en la metodología ISO27001 e ISO27002, para reducir brechas de seguridad y cumplir normativas, en el departamento de IT	Informe diagnóstico del nivel de cumplimiento con las normas ISO 27001 e ISO 27002.	Fase de análisis situacional.	Revisión documental, entrevistas, observación directa.	Guía de entrevistas, listas de verificación ISO.	Seguridad de la información, gestión de riesgos, auditoría interna.
Objetivos específicos					
1. Identificar las principales brechas y vulnerabilidades que afectan la confidencialidad, integridad y disponibilidad de la información.	Matriz de brechas y riesgos de seguridad.	Fase de identificación de áreas de mejora.	Evaluación de controles, análisis de vulnerabilidades.	Matriz de riesgos, herramientas de análisis de seguridad.	Análisis de riesgos, control de accesos, gestión de incidentes.

2. Evaluar el nivel de conocimiento y concientización del personal sobre prácticas seguras de información.	Informe de resultados de evaluación del factor humano.	Fase de evaluación del recurso humano.	Entrevistas.		Ingeniería social, concientización en seguridad, comportamiento organizacional.	
3. Diseñar estrategias y propuestas de mejora basadas en la metodología ISO/IEC 27001 e ISO/IEC 27002.	Propuesta de plan de fortalecimiento de la seguridad de la información.	Fase de desarrollo de mejoras y diseño del plan.	Análisis comparativo, revisión normativa, talleres internos.	Plantillas de plan de acción, documentación ISO, registros de reuniones.	ISO/IEC 27001, ISO/IEC 27002, políticas de seguridad, mejora continua.	
4. Desarrollar un plan de acción que permita reducir las brechas de seguridad y cumplir las normativas internacionales.	Documento final de propuesta de implementación.	Fase de implementación y validación del plan.	Validación de resultados, revisión de cumplimiento, retroalimentación.	Informes de auditoría, reportes de seguimiento, indicadores de desempeño.	Continuidad del negocio, cumplimiento normativo, gestión de seguridad.	

Nota: Matriz de coherencia

Fuente: Elaboración propia

CAPÍTULO IV

DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

4.1 INTRODUCCIÓN

El presente capítulo tiene como objetivo analizar de manera exhaustiva la situación actual del departamento de Tecnologías de Información de Procter & Gamble, sede Costa Rica, en lo referente a la gestión de la seguridad de la información. Este diagnóstico se estructura como fase previa al desarrollo de la propuesta de mejora y comprende cuatro dimensiones fundamentales: el diagnóstico operativo, el diagnóstico técnico, el diagnóstico de percepción y el análisis de brechas tecnológicas respecto a los controles establecidos por las normas ISO/IEC 27001 e ISO/IEC 27002 (93 controles totales de la versión 2022).

Para la elaboración del diagnóstico se emplearon las técnicas de investigación definidas en el marco metodológico, incluyendo entrevistas estructuradas al personal de TI, revisión de documentación interna y observación directa de los procesos y la infraestructura tecnológica. El análisis integrado de estas fuentes permite obtener una visión objetiva del estado de madurez del departamento y constituye la base técnica para las propuestas que se presentan en el Capítulo V.

4.2 Diagnóstico Operativo

El diagnóstico operativo tiene como objetivo identificar el estado actual de las políticas, procedimientos y controles organizacionales relacionados con la seguridad de la información que se encuentran formalmente documentados y en vigencia dentro del departamento de IT de Procter & Gamble, sede Costa Rica.

Para cada política o procedimiento identificado, se presenta en primera instancia lo que establece la norma ISO/IEC 27001:2022 e ISO/IEC 27002:2022, seguido del estado actual de la organización y una conclusión que determina el nivel de cumplimiento: Cumple, Cumple Parcialmente o No Cumple. Este análisis constituye la base objetiva para determinar las brechas abordadas en la sección 4.5.

4.2.1.Política de Seguridad de la Información

¿Qué establece ISO/IEC 27001:2022 (Cláusula 5.2) e ISO/IEC 27002:2022 (Control A.5.1)?

La norma ISO/IEC 27001:2022, en su Cláusula 5.2, establece que la alta dirección debe definir una política de seguridad de la información que sea apropiada al propósito de la organización, incluya objetivos de seguridad de la información o proporcione el marco para establecerlos, incluya el compromiso de satisfacer los requisitos aplicables relacionados con la seguridad de la información, y contemple el compromiso de mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Adicionalmente,

el control A.5.1 de ISO/IEC 27002:2022 establece que esta política debe estar aprobada por la dirección, publicada, comunicada al personal pertinente y revisada a intervalos planificados o cuando se produzcan cambios significativos.

Procter & Gamble cuenta con una Política de Seguridad de la Información a nivel corporativo global, formalmente documentada y aprobada por la alta dirección de la compañía. Esta política está disponible para el personal a través de los canales internos corporativos. Sin embargo, dicha política ha sido diseñada bajo el contexto global de la organización multinacional y no ha sido adaptada al contexto normativo, operativo y cultural específico de la sede Costa Rica. Aspectos como la legislación local aplicable (Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales), los procedimientos internos específicos del país y la estructura organizativa local del departamento de TI no están explícitamente contemplados en la política global.

Si bien la organización cuenta con una política de seguridad de la información formalmente documentada y aprobada a nivel corporativo, esta no ha sido adaptada al contexto local de Costa Rica. El 67% del personal entrevistado indica conocer la política global, pero solo el 33% puede describir cómo se aplica en su trabajo diario dentro de la sede, lo que evidencia una brecha de comunicación y adaptación local. La política existe y está activa, pero no cumple completamente con el requisito de ser apropiada al contexto específico de la organización local, por lo cual esta cumple parcialmente.

4.2.2. Procedimiento de Gestión de Accesos

¿Qué establece ISO/IEC 27002:2022 (Controles A.5.15, A.5.16, A.5.18)?

ISO/IEC 27002:2022 establece en los controles A.5.15 (Control de acceso), A.5.16 (Gestión de identidades) y A.5.18 (Derechos de acceso) que la organización debe implementar un proceso formal para la asignación, revisión y revocación de derechos de acceso a sistemas e información. Este proceso debe incluir la provisión de accesos basada en el principio de mínimo privilegio, la revisión periódica de los derechos de acceso asignados para garantizar que siguen siendo apropiados, y la revocación inmediata de accesos cuando un empleado cambia de función o abandona la organización. La norma exige que estas revisiones sean documentadas y que exista evidencia del proceso de aprobación de accesos.

El departamento de TI de P&G Costa Rica cuenta con un procedimiento de gestión de accesos formalmente documentado. Los controles de autenticación están activos, incluyendo autenticación multifactor para acceso a sistemas críticos. Existe un proceso de solicitud de accesos mediante tickets en el sistema corporativo. No obstante, durante las entrevistas realizadas al personal, los líderes de equipo reportaron que las revisiones periódicas de accesos asignados no se realizan de forma documentada y sistemática. Esto

implica que podrían existir accesos huérfanos (de empleados que cambiaron de rol o dejaron la empresa) o con privilegios excesivos que no han sido identificados ni revocados formalmente.

El procedimiento de gestión de accesos existe y está operativo en sus aspectos de provisión inicial (solicitud y aprobación de accesos). Sin embargo, la ausencia de un proceso documentado y periódico de revisión de accesos representa una brecha frente al requisito de los controles A.5.15 y A.5.18 de ISO/IEC 27002:2022, que exigen revisiones regulares con evidencia documentada. Esta brecha expone a la organización al riesgo de accesos indebidos por acumulación de privilegios o cuentas huérfanas no detectadas, por lo cual esta cumple parcialmente.

4.2.3. Política de Resguardo de Información (Backup)

¿Qué establece ISO/IEC 27002:2022 (Control A.8.13)?

El control A.8.13 de ISO/IEC 27002:2022 establece que la organización debe mantener y probar regularmente copias de seguridad de la información, el software y los sistemas. La política de copias de seguridad debe definir los requisitos de retención, la frecuencia de los respaldos, el tipo de información que debe respaldarse, los procedimientos de restauración y la periodicidad de las pruebas de recuperación. La norma enfatiza que no es suficiente con realizar los respaldos; es necesario verificar periódicamente que los datos pueden ser recuperados correctamente dentro de los tiempos establecidos (RTO/RPO), y que esta verificación quede documentada.

Procter & Gamble Costa Rica cuenta con una política de resguardo de información formalmente documentada. Los respaldos se realizan de forma periódica y estructurada sobre los sistemas críticos del departamento de TI. El entorno virtualizado de 22 VMs en VMware vSphere 7.0 cuenta con snapshots activos. La organización también dispone de un Plan de Continuidad del Negocio (BCP/DRP) que contempla los procedimientos de recuperación ante desastres. El proceso de backup está integrado dentro de las operaciones regulares del equipo de infraestructura.

La política de resguardo de información cumple con los requisitos fundamentales establecidos por el control A.8.13 de ISO/IEC 27002:2022. Existe una política formal, los respaldos se realizan de forma periódica y estructurada, y el plan de continuidad del negocio contempla los procedimientos de recuperación. La organización demuestra un

control activo y operativo en esta área, sin brechas críticas identificadas durante el diagnóstico, por lo tanto esta política cumple.

4.2.4. Gestión de Incidentes de Seguridad

¿Qué establece ISO/IEC 27002:2022 (Controles A.5.24, A.5.25, A.5.26, A.5.27)?

ISO/IEC 27002:2022 establece en los controles A.5.24 al A.5.27 que la organización debe planificar y prepararse para gestionar los incidentes de seguridad de la información de manera eficaz. Esto implica la existencia de un procedimiento formal documentado que incluya la identificación, clasificación, contención, erradicación, recuperación y documentación de incidentes. La norma también exige que se registren las lecciones aprendidas de cada incidente y que existan responsables claramente definidos para la gestión de cada etapa. Adicionalmente, los incidentes deben ser reportados oportunamente y las evidencias deben ser preservadas para eventuales procesos legales o auditorías.

El departamento de TI de P&G Costa Rica cuenta con un procedimiento centralizado de gestión de incidentes de seguridad, formalmente documentado y activo. El equipo de Ciberseguridad (20 colaboradores) es el responsable principal de la atención y gestión de incidentes. Las herramientas CrowdStrike Falcon (EDR) y Zscaler generan alertas automáticas que son atendidas por este equipo. Existe un sistema de tickets para el registro y seguimiento de incidentes. Los colaboradores entrevistados indicaron conocer el canal de reporte de incidentes y el procedimiento a seguir ante un evento de seguridad.

La organización cuenta con un proceso de gestión de incidentes que cumple con los requisitos establecidos por ISO/IEC 27002:2022. El procedimiento está formalizado, existe un equipo responsable definido, se utilizan herramientas de detección activa y el personal conoce el proceso de reporte. No se identificaron brechas críticas en esta área durante el diagnóstico, por lo tanto esta política cumple.

4.2.5. Plan de Continuidad del Negocio (BCP/DRP)

¿Qué establece ISO/IEC 27001:2022 (Cláusula 8.6) e ISO/IEC 27002:2022 (Controles A.5.29, A.5.30)?

La cláusula 8.6 de ISO/IEC 27001:2022 y los controles A.5.29 (Seguridad de la información durante la interrupción) y A.5.30 (Preparación para las TIC para la continuidad del negocio) de ISO/IEC 27002:2022 establecen que la organización debe planificar cómo mantener la seguridad de la información a un nivel adecuado durante situaciones adversas. Esto incluye la existencia de un plan de continuidad del negocio (BCP) y un plan de recuperación ante desastres (DRP) formalmente documentados, probados periódicamente y actualizados conforme cambia el entorno tecnológico y organizacional. La norma exige que estos planes incluyan los tiempos de recuperación objetivo (RTO) y los puntos de recuperación objetivo (RPO) para los sistemas críticos.

P&G Costa Rica cuenta con un Plan de Continuidad del Negocio (BCP/DRP) formalmente definido y documentado. La infraestructura tecnológica respalda este plan mediante la conectividad SD-WAN redundante de 1 Gbps con dos enlaces independientes (disponibilidad del 99.8%), el entorno virtualizado con snapshots activos y la política de backup periódico. La conectividad WAN opera con tecnología SD-WAN Versa con capacidad de conmutación entre enlaces ante fallos.

La organización cumple con los requisitos fundamentales de continuidad del negocio establecidos por ISO/IEC 27001:2022 e ISO/IEC 27002:2022. Existe un plan formalmente documentado y la infraestructura tecnológica está diseñada para soportar la continuidad operativa. No se identificaron brechas críticas en esta área durante el diagnóstico, por lo tanto esta política cumple.

4.2.6. Política de Clasificación de la Información

¿Qué establece ISO/IEC 27002:2022 (Controles A.5.9, A.5.10, A.5.11, A.5.12, A.5.13)?

Los controles A.5.9 al A.5.13 de ISO/IEC 27002:2022 establecen que la organización debe identificar, clasificar y etiquetar la información de acuerdo con su nivel de sensibilidad y criticidad. La política de clasificación debe definir las categorías de clasificación (por ejemplo: pública, interna, confidencial, restringida), los criterios para asignar cada categoría, los procedimientos de manejo para cada nivel de clasificación y las responsabilidades del personal en cuanto al tratamiento de la información según su clasificación. La norma exige que esta clasificación sea aplicada de forma consistente en

toda la organización y que el personal conozca y aplique los criterios de clasificación en su trabajo diario.

P&G cuenta con una política de clasificación de la información definida a nivel corporativo global, que establece las categorías de sensibilidad de la información manejada por la compañía. Sin embargo, la aplicación de esta política en la sede Costa Rica es inconsistente. Durante las entrevistas, se identificó que parte del personal no aplica sistemáticamente los criterios de clasificación en los documentos y datos que maneja en su trabajo diario. La clasificación existe formalmente en el papel corporativo, pero no ha sido internalizada ni aplicada de forma uniforme a nivel local, lo que genera riesgos de manejo inadecuado de información sensible.

Aunque la política de clasificación de la información existe a nivel corporativo global, su aplicación inconsistente en la sede Costa Rica representa una brecha frente a los controles A.5.12 y A.5.13 de ISO/IEC 27002:2022, que exigen que la clasificación sea aplicada de forma consistente en toda la organización. La brecha principal radica en la falta de adaptación local y capacitación específica sobre los criterios de clasificación, lo que resulta en una aplicación dispar entre equipos y colaboradores, por lo tanto esta política cumple parcialmente.

4.2.7. Procedimiento de Control de Cambios

¿Qué establece ISO/IEC 27002:2022 (Control A.8.32)?

El control A.8.32 de ISO/IEC 27002:2022 establece que los cambios en las instalaciones de procesamiento de información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios formales. Esto incluye la evaluación del impacto potencial de los cambios en la seguridad de la información antes de su implementación, la autorización formal de los cambios por parte de los responsables correspondientes, la documentación de los cambios realizados y la posibilidad de revertir los cambios si ocurren problemas. La norma enfatiza que la gestión de cambios debe contemplar explícitamente las implicaciones de seguridad de cada modificación propuesta.

El departamento de TI de P&G Costa Rica cuenta con un proceso de control de cambios (change management) activo, gestionado a través del sistema corporativo de tickets. Los

cambios en infraestructura, sistemas y configuraciones deben pasar por un proceso formal de aprobación antes de ser implementados. Sin embargo, durante las entrevistas se identificó que este proceso no siempre incluye una evaluación explícita de las implicaciones de seguridad de la información de cada cambio propuesto. El enfoque del proceso actual está orientado principalmente a la gestión operativa del cambio, pero la dimensión de seguridad no siempre es evaluada de forma sistemática como parte del flujo de aprobación.

El procedimiento de control de cambios existe y está operativo, cumpliendo con los aspectos procedimentales básicos del control A.8.32 de ISO/IEC 27002:2022. No obstante, la ausencia de una evaluación explícita y sistemática de las implicaciones de seguridad como parte obligatoria del proceso de aprobación representa una brecha parcial. Esta brecha es consistente con el hallazgo del equipo de redes, que señaló que aproximadamente el 15% de las reglas de firewall supera los 12 meses sin recertificación, lo que sugiere que los cambios en configuraciones de seguridad no siempre son gestionados con el rigor requerido, por lo tanto esta política cumple parcialmente.

4.2.8. Política de Capacitación y Concientización en Seguridad

¿Qué establece ISO/IEC 27002:2022 (Controles A.6.3, A.7.2)?

El control A.6.3 de ISO/IEC 27002:2022 establece que el personal de la organización y las partes interesadas pertinentes deben recibir concienciación, educación y formación apropiada en materia de seguridad de la información, y actualizaciones regulares sobre las políticas y procedimientos de la organización relevantes para su puesto de trabajo. Complementariamente, el control A.7.2 establece que todos los empleados deben ser conscientes de su responsabilidad en cuanto a la seguridad de la información. La norma especifica que estas actividades de formación deben ser planificadas, estructuradas por rol y área funcional, evaluadas en términos de efectividad y documentadas con evidencia de participación y resultados.

La política de capacitación y concientización en seguridad de la información no se encuentra formalizada como documento independiente en la sede Costa Rica. Las actividades de formación se realizan de forma esporádica y no estructurada, sin un

programa anual definido con módulos por rol, evaluaciones de conocimiento ni métricas de cobertura. De los 14 colaboradores entrevistados, solo el 33% indicó haber recibido capacitación formal en seguridad durante el último año. Esto implica que aproximadamente 112 de los 167 colaboradores del departamento de TI no recibieron formación formal en el período analizado, exponiéndolos a riesgos de ingeniería social, phishing y manejo inadecuado de la información.

La organización no cuenta con una política formalizada de capacitación y concientización en seguridad de la información, y las actividades de formación existentes no cumplen con los requisitos de planificación, estructuración por rol, evaluación y documentación establecidos por los controles A.6.3 y A.7.2 de ISO/IEC 27002:2022. Con solo el 33% del personal capacitado formalmente en el último año, esta es la brecha con mayor exposición al riesgo humano identificada en el diagnóstico, dado que el factor humano representa el vector de ataque más frecuente en incidentes de seguridad de la información, por lo tanto esta política no cumple.

4.3 Diagnóstico Técnico

El diagnóstico técnico tiene como objetivo describir y analizar la infraestructura tecnológica del departamento de IT de Procter & Gamble, sede Costa Rica, evaluando si los componentes tecnológicos son adecuados, se encuentran actualizados, cuentan con soporte activo del fabricante y si existen riesgos asociados a la obsolescencia o a la falta de controles técnicos. Para cada componente se presenta el detalle técnico observado, los hallazgos identificados durante el diagnóstico y el estado resultante del análisis.

Este diagnóstico se elaboró mediante observación directa de la infraestructura, revisión del inventario de equipos del departamento de IT, consulta de las páginas oficiales de los fabricantes (Cisco, Fortinet, Versa Networks, VMware, Infoblox) para la verificación del estado de soporte de cada modelo, y entrevistas al equipo de Redes y Ciberseguridad.

4.3.1. Personal de TI — Estructura Organizativa

El departamento de IT de P&G Costa Rica cuenta con un total de 167 colaboradores, distribuidos en siete equipos funcionales especializados: Redes (20 colaboradores), Ciberseguridad (20 colaboradores), Cloud (15 colaboradores), Análisis de Datos (25 colaboradores), Soporte Técnico (17 colaboradores), SAP (20 colaboradores) y Desarrollo de Software (50 colaboradores). Esta estructura refleja una organización de TI de nivel empresarial con cobertura técnica en las principales disciplinas tecnológicas requeridas por una multinacional de la escala de Procter & Gamble. La distribución del personal permite que cada área cuente con un equipo dedicado, lo que facilita la especialización técnica y la atención diferenciada de los distintos dominios de infraestructura y seguridad.

La estructura organizativa del departamento de IT está claramente definida, formalizada y operativa. Los roles y responsabilidades de cada equipo se encuentran documentados y son conocidos por los colaboradores, lo que permite una gestión ordenada de las operaciones tecnológicas y de seguridad de la sede. La distribución de 167 colaboradores en equipos especializados garantiza la cobertura técnica necesaria para operar y mantener la infraestructura de nivel empresarial que posee P&G Costa Rica. No se identificaron brechas en la estructura organizativa del departamento durante el diagnóstico.

Estructura organizativa formalizada y operativa. Sin brechas identificadas.

4.3.2. Servidores Físicos — Cisco ALICS (Nexus C93180YC-FX3)

El site de P&G Costa Rica cuenta con un servidor físico principal bajo el esquema ALICS (Agile Local IT Computing Services), basado en el modelo Cisco Nexus C93180YC-FX3. Este es un switch-router de alta densidad de la familia Nexus 9000 de Cisco, diseñado para entornos de data center de mediana y alta escala. El equipo cuenta con 48 puertos SFP28 de 25G y 6 puertos QSFP28 de 100G, lo que le otorga capacidades de interconexión de alta

velocidad para el entorno virtualizado. La carga de trabajo de cómputo del departamento de TI se gestiona principalmente mediante el entorno virtualizado administrado sobre VMware, utilizando este servidor físico como plataforma de sustento de las 22 máquinas virtuales activas.

El modelo Cisco Nexus C93180YC-FX3 se encuentra actualmente dentro del ciclo de vida de soporte activo de Cisco, sin alertas de End of Life (EoL) ni End of Sale (EoS) identificadas durante el período de diagnóstico. La principal observación identificada es que la organización depende de un único servidor físico como base del entorno virtualizado, lo que representa un punto único de falla (Single Point of Failure) a nivel de hardware. Si bien los snapshots activos de las VMs mitigan parcialmente este riesgo, la ausencia de redundancia física de cómputo es una brecha de disponibilidad que debe ser considerada en el marco del Plan de Continuidad del Negocio (BCP/DRP).

Hardware con soporte activo. Punto único de falla de cómputo sin redundancia física.

4.3.3. Servidores Virtuales — VMware vSphere 7.0 (22 VMs)

El departamento de TI opera un entorno virtualizado centralizado compuesto por 22 máquinas virtuales (VMs) gestionadas sobre VMware vSphere 7.0. Este entorno constituye la plataforma principal de procesamiento y servicios del departamento, alojando los sistemas críticos de la sede. Las VMs cuentan con snapshots activos que permiten la recuperación rápida ante fallos o cambios erróneos. La versión de sistema operativo utilizada en las máquinas virtuales corresponde a Windows Server 2022, que es la versión más reciente de Microsoft con soporte mainstream hasta 2026 y soporte extendido hasta 2031.

Se identificaron dos hallazgos de relevancia en este componente. En primer lugar, VMware vSphere 7.0 fue adquirido por Broadcom en 2023, y la compañía ha anunciado cambios significativos en su modelo de licenciamiento, descontinuando las licencias perpetuas y migrando a un esquema de suscripción. Esto representa un riesgo de continuidad del soporte que el departamento de TI debe evaluar en términos de renovación o migración a vSphere 8.x. En segundo lugar, no existe una política formal documentada del ciclo de vida de las VMs, lo que puede resultar en la acumulación de máquinas virtuales inactivas o con configuraciones desactualizadas que incrementan la superficie de ataque.

Entorno operativo funcional. Riesgo de licenciamiento VMware y sin política de ciclo de vida de VMs.

4.3.4. Equipos de Red — Switches Cisco Catalyst C9300-24UX (IOS-XE 17.9.5)

La infraestructura de switching de la sede está compuesta por 17 unidades del modelo Cisco Catalyst C9300-24UX, pertenecientes a la familia Catalyst 9300, que es la plataforma de acceso empresarial de siguiente generación de Cisco. Este modelo cuenta con 24 puertos UPOE+ multigigabit (100M/1G/2.5G/5G/10G) y soporte para stacking de alta velocidad. Los equipos corren el sistema operativo Cisco IOS-XE versión 17.9.5, que se encuentra dentro del ciclo de soporte activo de Cisco y corresponde a una versión de larga duración (Extended Maintenance Release). Las VLANs están configuradas y segregadas por área funcional en los 17 switches.

El modelo Cisco Catalyst C9300-24UX cuenta con soporte activo del fabricante y no presenta alertas de End of Life durante el horizonte del presente diagnóstico, lo que representa una posición favorable en términos de ciclo de vida. Sin embargo, se identificaron dos brechas operativas: la ausencia de un estándar documentado de nomenclatura y asignación de VLANs según función, y la falta de documentación completa y actualizada de la topología de switching en NetBrain. Estas ausencias dificultan la auditoría de la red, aumentan el riesgo de errores de configuración y limitan la capacidad de respuesta ante incidentes que involucren la capa de red.

4.3.5. Firewalls — FortiGate 120G (FortiOS 7.4.8)

La seguridad perimetral y el control de acceso entre segmentos de red de la sede están gestionados por 2 firewalls FortiGate 120G de Fortinet, que corren FortiOS versión 7.4.8. Esta versión se encuentra actualmente dentro de la rama de soporte activo 7.4.x de FortiOS, con acceso garantizado a actualizaciones de seguridad y soporte técnico del fabricante. Los FortiGate aplican las políticas de seguridad y el filtrado de tráfico entre todas las zonas de red de la sede, integrándose con los Versa Networks para la gestión del tráfico WAN y con los switches para la segmentación interna mediante VLANs.

Se identificaron dos hallazgos que requieren atención. En primer lugar, el reporte de NetBrain confirma que aproximadamente el 15% de las reglas de firewall supera los 12 meses sin haber sido recertificadas, lo que implica la posible presencia de reglas obsoletas que amplían innecesariamente la superficie de ataque y dificultan la validación del principio de mínimo privilegio. En segundo lugar, no existe una convención formal documentada de nomenclatura para las reglas de firewall, lo que dificulta su gestión, auditoría e interpretación durante revisiones de seguridad. Ambas brechas son abordadas mediante propuestas específicas en el Capítulo V.

FortiOS 7.4.8 con soporte activo. ~15% de reglas sin recertificar y sin estándar de nomenclatura.

4.3.6. Routers SD-WAN — Versa VEP 4600 (22.1.4-GA)

El enrutamiento WAN de la sede está gestionado por 2 unidades del modelo Versa VEP 4600, corriendo la versión de software 22.1.4-GA, que corresponde a la rama de disponibilidad general (GA) de la plataforma Versa Networks. La tecnología SD-WAN implementada permite la selección inteligente del enlace WAN activo en función de parámetros de calidad como latencia, pérdida de paquetes y jitter, con capacidad de conmutación automática entre los dos enlaces disponibles ante la degradación o falla de uno de ellos. Los Versa VEP 4600 trabajan de forma integrada con los firewalls FortiGate para garantizar que todo el tráfico WAN pase por los controles de seguridad perimetral antes de alcanzar la red interna o internet.

La plataforma SD-WAN Versa VEP 4600 se encuentra en su versión de disponibilidad general con soporte activo del fabricante. La implementación está correctamente dimensionada para la sede, con políticas de enrutamiento configuradas y operativas. La integración con los firewalls FortiGate garantiza que el control de seguridad y el enrutamiento inteligente operen de forma coordinada. La conmutación automática entre enlaces opera de forma transparente, lo que contribuye directamente a la disponibilidad del 99.8% reportada para la conectividad WAN de la sede. No se identificaron brechas técnicas en la plataforma SD-WAN durante el diagnóstico.

4.3.7. Access Points y Controladores Inalámbricos — Cisco AP 9130AXI y WLC 9800-40 (IOS-XE 17.15.4d) — Alerta de Fin de Soporte

La red inalámbrica de la sede está compuesta por 177 Access Points modelo Cisco Catalyst 9130AXI y 2 Wireless LAN Controllers (WLC) modelo Cisco Catalyst 9800-40, todos corriendo la versión IOS-XE 17.15.4d. El modelo 9130AXI es un AP de la generación Wi-Fi 6 (802.11ax), con soporte para bandas de 2.4 GHz y 5 GHz, y capacidades de OFDMA y MU-MIMO para entornos de alta densidad de usuarios. Los WLC 9800-40 gestionan centralizadamente los 177 APs, administrando los tres SSIDs activos: Corporativo, Guest e IoT. La cobertura inalámbrica abarca todas las áreas de trabajo de la sede.

Este componente representa la brecha de ciclo de vida más crítica identificada en el diagnóstico técnico. Según información oficial publicada por Cisco en su portal de ciclos de vida de productos, tanto el modelo Cisco Catalyst 9130AXI como el WLC Catalyst 9800-40 alcanzarán su fecha de End of Support (EoS) en diciembre de 2025. A partir de esa fecha, Cisco no proveerá actualizaciones de software, parches de seguridad ni soporte técnico para estos modelos, lo que representa un riesgo de seguridad significativo para la infraestructura inalámbrica de la sede. Para mantener la cobertura de soporte del fabricante, Cisco recomienda la migración al modelo CW9176I como sucesor del AP 9130AXI, y al modelo CW9800M como sucesor del WLC 9800-40, ambos compatibles con IOS-XE 17.15.4d. Adicionalmente, se identificó que no existe un estándar formal documentado de autenticación inalámbrica (WPA3/802.1X) para los SSIDs activos.

Requiere acción inmediata — End of Support Cisco diciembre 2025. Migración requerida a CW9176I (AP) y CW9800M (WLC).

4.3.8. Conectividad WAN — SD-WAN Dual-Link 500 Mbps c/u (1 Gbps total)

La sede cuenta con dos enlaces WAN independientes de 500 Mbps cada uno, gestionados mediante la plataforma SD-WAN de Versa Networks. Los enlaces son de tipo directo al ISP (sin MPLS), con un ancho de banda total disponible de 1 Gbps. Esta arquitectura de doble enlace garantiza redundancia de conectividad a nivel de acceso WAN, con conmutación automática gestionada por la plataforma Versa ante la degradación o pérdida de uno de los enlaces. El tráfico de usuarios corporativos, servicios cloud y la conectividad Zero Trust a través de Zscaler se benefician de esta arquitectura dual de conectividad.

La conectividad WAN de la sede opera en condiciones óptimas, con una disponibilidad histórica del 99.8% que refleja la robustez de la arquitectura de doble enlace implementada. La plataforma SD-WAN Versa gestiona de forma eficiente la distribución del tráfico entre ambos enlaces y la conmutación automática ante eventos de fallo, garantizando la continuidad operativa de la sede. El ancho de banda total de 1 Gbps es adecuado para las necesidades actuales del departamento de TI y los 167 colaboradores. No se identificaron brechas en la infraestructura de conectividad WAN durante el diagnóstico.

4.3.9. Herramientas de Monitoreo — NetBrain y Zabbix

El departamento de TI utiliza dos plataformas complementarias para el monitoreo y la documentación de la infraestructura de red. NetBrain es la plataforma principal de gestión y documentación de la topología de red, utilizada para mapear la infraestructura de switches, routers, firewalls y APs, generar reportes de configuración y ejecutar auditorías de reglas de firewall, incluyendo la identificación de reglas con antigüedad superior a 12 meses. Zabbix es la herramienta de monitoreo de infraestructura en tiempo real, configurada para supervisar el estado de disponibilidad y rendimiento de los componentes de red y servidores. Ambas plataformas trabajan de forma complementaria, con NetBrain proveyendo visibilidad documental y de configuración, y Zabbix proveyendo visibilidad operativa en tiempo real.

Las plataformas de monitoreo NetBrain y Zabbix están activas y proveen cobertura adecuada sobre la infraestructura de la sede. NetBrain permite la documentación y auditoría de la topología de red y configuraciones de dispositivos, mientras Zabbix garantiza la visibilidad operativa en tiempo real sobre el estado de los componentes críticos. La combinación de ambas herramientas otorga al equipo de Redes y Ciberseguridad una visibilidad completa tanto a nivel documental como operativo, lo que constituye una base sólida para la gestión proactiva de la infraestructura. No se identificaron brechas críticas en las plataformas de monitoreo durante el diagnóstico.

4.3.10. Gestión de DNS y DHCP — Infoblox (versión 8.6.3)

El departamento de TI gestiona los servicios de DNS (Domain Name System) y DHCP (Dynamic Host Configuration Protocol) de la sede mediante la plataforma Infoblox, corriendo la versión 8.6.3. Infoblox es una solución de gestión de red de nivel empresarial especializada en la administración centralizada de la infraestructura de DNS, DHCP e IPAM (IP Address Management), conocida como DDI. Esta plataforma es responsable de la asignación dinámica de direcciones IP a todos los dispositivos de la red corporativa, la resolución de nombres de dominio internos y externos, y la gestión del inventario de direcciones IP en uso. La integración de Infoblox con la infraestructura de red de la sede garantiza que la asignación de IPs y la resolución de nombres operen de forma centralizada, confiable y auditable.

La plataforma Infoblox versión 8.6.3 se encuentra operativa y dentro del ciclo de soporte activo del fabricante. Los servicios de DNS y DHCP funcionan de forma estable y sin interrupciones identificadas durante el período de diagnóstico. La gestión centralizada de DDI mediante Infoblox representa una práctica de nivel empresarial que otorga visibilidad y control sobre la asignación de direcciones IP en toda la infraestructura de la sede, facilita la auditoría de la red y reduce el riesgo de conflictos de direccionamiento. No se identificaron brechas técnicas ni operativas en esta plataforma durante el diagnóstico.

4.3.11. Protección de Endpoints — CrowdStrike Falcon (EDR) y Zscaler (Zero Trust)

La protección de los equipos de usuario final y servidores se gestiona mediante dos plataformas de seguridad empresarial de última generación. CrowdStrike Falcon actúa como plataforma de Detección y Respuesta en Endpoints (EDR), proveyendo protección contra malware, ransomware y amenazas avanzadas persistentes (APT) mediante análisis de comportamiento basado en inteligencia artificial. Zscaler Internet Access (ZIA) implementa el modelo de seguridad Zero Trust Network Access (ZTNA), garantizando que todo el tráfico de internet de los endpoints pase por un proxy seguro en la nube, independientemente de la ubicación física del usuario. Esta arquitectura provee una doble capa de protección: CrowdStrike a nivel de dispositivo y Zscaler a nivel de acceso a red y servicios externos.

La combinación de CrowdStrike Falcon y Zscaler representa una arquitectura de seguridad de endpoint robusta y alineada con las mejores prácticas de la industria para entornos corporativos distribuidos. Ambas plataformas están activas y operativas sobre todos los endpoints del departamento de TI. No se identificaron brechas críticas en estas plataformas durante el diagnóstico. Sin embargo, se observó que no existe un reporte documentado que certifique el porcentaje de cobertura de CrowdStrike sobre el total de endpoints, lo que impide validar formalmente que el 100% de los dispositivos cuenta con protección activa. Documentar y revisar periódicamente este indicador de cobertura fortalecería el cumplimiento del control A.6.1 de ISO/IEC 27002:2022.

El hallazgo de mayor urgencia corresponde a la infraestructura inalámbrica: los 177 Access Points Cisco 9130AXI y los 2 WLC Catalyst 9800-40 alcanzarán su fecha de End of Support (EoS) en diciembre de 2025, lo que implica que a partir de esa fecha no recibirán actualizaciones de seguridad ni soporte del fabricante. Esta situación requiere una planificación de refresh tecnológico hacia los modelos Cisco CW9176I y CW9800M como parte de las propuestas de mejora desarrolladas en el Capítulo V. El hallazgo secundario de mayor impacto corresponde a los firewalls FortiGate, donde el ~15% de las reglas activas supera los 12 meses sin recertificación, brecha que también es abordada en el Capítulo V con un estándar formal de nomenclatura y proceso de recertificación periódica.

4.4 Diagnóstico de Percepción

El diagnóstico de percepción tiene como objetivo identificar la perspectiva, el conocimiento y la experiencia del personal del departamento de TI de Procter & Gamble, sede Costa Rica, en relación con las prácticas de seguridad de la información. Para ello se realizaron entrevistas semiestructuradas a un total de 14 colaboradores, representando los siete equipos del departamento: Redes, Ciberseguridad, Cloud, Análisis de Datos, Soporte Técnico, SAP y Desarrollo de Software.

A continuación se presenta, para cada pregunta de la guía de entrevista, los hallazgos consolidados de las respuestas obtenidas y la conclusión derivada del análisis. Los resultados de este diagnóstico constituyen evidencia cualitativa complementaria a los diagnósticos operativo y técnico, y alimentan directamente la matriz de brechas de la sección 4.5.

P1Área: Políticas de Seguridad

¿Conoce usted la política de seguridad de la información de P&G? ¿Puede describir cómo aplica en su trabajo diario?

De los 14 colaboradores entrevistados, el 67% (aproximadamente 9 personas) indicó conocer la existencia de la política de seguridad de la información de P&G a nivel corporativo global. Sin embargo, al solicitarles que describieran cómo aplica esta política en su trabajo diario, solo el 33% (aproximadamente 5 personas) pudo articular procedimientos o prácticas concretas relacionadas con la política. El 67% restante mencionó conocer la política de forma general pero no pudo describir su aplicación práctica en el contexto específico de la sede Costa Rica. Los colaboradores del equipo de Ciberseguridad y Redes mostraron mayor familiaridad con la política, mientras que los equipos de Soporte Técnico, SAP y Desarrollo de Software evidenciaron menor conocimiento de su aplicación local.

Conclusión: Existe un conocimiento superficial de la política de seguridad entre la mayoría del personal. La brecha entre conocer la política globalmente (67%) y poder describir su aplicación local (33%) evidencia que la política corporativa no ha sido suficientemente adaptada ni comunicada al contexto operativo de la sede Costa Rica, generando riesgo de incumplimiento por desconocimiento práctico.

P2Área: Políticas de Seguridad

¿Existe algún procedimiento local documentado que complemente la política corporativa global para la sede Costa Rica?

La totalidad de los colaboradores entrevistados (100%) indicó no tener conocimiento de la existencia de un procedimiento o documento formal que adapte la política corporativa global de P&G al contexto específico de la sede Costa Rica. Algunos colaboradores del equipo de Redes mencionaron que existen prácticas operativas que siguen de forma habitual, pero reconocieron que estas no están formalizadas ni documentadas en ningún instrumento normativo local. El equipo de Ciberseguridad señaló que trabajan principalmente con las directrices corporativas globales y que no existe un complemento local documentado.

Conclusión: No existe ningún procedimiento local documentado que adapte la política corporativa global al contexto de la sede Costa Rica. Esta ausencia confirma la brecha identificada en el diagnóstico operativo respecto al control A.5.1 de ISO/IEC 27002:2022, y representa un riesgo de aplicación inconsistente de la política entre los diferentes equipos del departamento.

P3Área: Capacitación

¿Ha recibido capacitación formal en seguridad de la información en el último año? ¿Sobre qué temas?

Solo el 33% de los colaboradores entrevistados (aproximadamente 5 personas) indicó haber recibido algún tipo de capacitación formal en seguridad de la información durante el último año. Los temas mencionados por quienes sí recibieron formación incluyeron: uso correcto de las herramientas corporativas, concienciación sobre phishing y gestión de contraseñas. El 67% restante (aproximadamente 9 colaboradores) indicó no haber recibido capacitación formal en el período, aunque algunos mencionaron haber accedido de forma autónoma a materiales informativos en línea. Los equipos con menor cobertura de capacitación fueron Soporte Técnico, SAP y Desarrollo de Software.

Conclusión: Solo un tercio del personal del departamento de TI recibió capacitación formal en seguridad durante el último año. Esto implica que aproximadamente 112 de los 167 colaboradores del departamento no recibieron formación estructurada, lo que representa la brecha de mayor exposición al riesgo humano identificada en el diagnóstico, alineada con la no conformidad del control A.6.3 y A.7.2 de ISO/IEC 27002:2022.

P4 Área: Capacitación

¿Considera que el programa de formación actual es suficiente para las responsabilidades de su rol?

El 86% de los colaboradores entrevistados (12 de 14) consideró que la formación actual en seguridad de la información no es suficiente para las responsabilidades que demanda su rol. Los entrevistados señalaron que las capacitaciones son esporádicas, no están diferenciadas por área funcional y no abordan los riesgos específicos que enfrenta cada equipo en su trabajo diario. El equipo de Redes, por ejemplo, indicó que necesitaría formación específica sobre seguridad en infraestructura de red, mientras que el equipo de Desarrollo de Software mencionó la necesidad de capacitación en prácticas de desarrollo seguro (Secure SDLC). Solo el 14% (2 personas del equipo de Ciberseguridad) consideró que su formación actual es adecuada para su rol.

Conclusión: El personal reconoce abiertamente la insuficiencia del programa de formación actual. La percepción generalizada es que las capacitaciones son genéricas y no están adaptadas a las necesidades específicas de cada equipo, lo que refuerza la necesidad de implementar un programa estructurado de capacitación por rol como se propone en el Capítulo V.

P5Área: Gestión de Accesos

¿Cómo se gestionan las solicitudes de acceso a sistemas o recursos críticos? ¿Existe un proceso de revisión periódica de accesos asignados?

El 100% de los entrevistados confirmó que existe un proceso formal para la solicitud y aprobación de nuevos accesos a sistemas críticos, gestionado a través del sistema corporativo de tickets de P&G. Los colaboradores describieron un flujo de solicitud que incluye la justificación del acceso requerido y la aprobación por parte del líder del equipo correspondiente. Sin embargo, cuando se les consultó sobre la revisión periódica de los

accesos ya asignados, los líderes de equipo de las áreas de Redes, Cloud y SAP reportaron de forma consistente que estas revisiones no se realizan de manera periódica ni documentada. Ninguno de los entrevistados pudo mencionar una fecha o frecuencia específica de revisión de accesos en su área.

Conclusión: El proceso de provisión de accesos está bien establecido y es conocido por el personal. Sin embargo, la ausencia de revisiones periódicas documentadas de los accesos asignados es una brecha reconocida por los propios líderes de equipo, lo que expone a la organización al riesgo de acumulación de accesos huérfanos o con privilegios excesivos no detectados.

P6Área: Estándares de Red

¿Existe un estándar documentado para la nomenclatura de VLANs y reglas de firewall en la infraestructura de red?

El equipo de Redes, que es el principal responsable de la gestión de la infraestructura de switching y firewall, indicó de forma unánime que no existe un estándar formal documentado para la nomenclatura de VLANs ni para las reglas de firewall en los equipos FortiGate. Los colaboradores de Redes señalaron que existen prácticas informales que se han heredado históricamente entre los miembros del equipo, pero que estas no están escritas ni formalizadas en ningún documento oficial. Mencionaron que la ausencia de este estándar genera inconsistencias cuando se incorporan nuevos miembros al equipo o cuando se deben realizar cambios en la configuración de los equipos. Los equipos de otras áreas no tenían conocimiento del estado de documentación de la red.

Conclusión: La ausencia de un estándar documentado de nomenclatura para VLANs y reglas de firewall es reconocida y confirmada por el propio equipo de Redes. Esta brecha genera inconsistencias operativas y dificulta la auditoría y la transferencia de conocimiento dentro del equipo, validando el hallazgo técnico identificado en el diagnóstico técnico (sección 4.3).

P7Área: Estándares de Red

¿Con qué frecuencia se revisan las reglas de firewall FortiGate para verificar su vigencia y necesidad operativa?

Los colaboradores del equipo de Redes y Ciberseguridad coincidieron en que no existe un proceso formal ni una frecuencia definida para la revisión periódica de las reglas de firewall FortiGate. Indicaron que las reglas se revisan de forma reactiva, principalmente cuando se detecta un problema o cuando se solicita un nuevo acceso que genera conflicto con una regla existente. Ningún miembro del equipo pudo mencionar la última vez que se realizó una revisión sistemática del conjunto completo de reglas. Este hallazgo es consistente con el dato obtenido del reporte de NetBrain, que confirma que aproximadamente el 15% de las reglas activas en los FortiGate supera los 12 meses sin haber sido revisadas o recertificadas.

Conclusión: La revisión de reglas de firewall se realiza de forma reactiva y no sistemática, sin una frecuencia ni un proceso formal definido. La correlación entre esta percepción del personal y el dato técnico del 15% de reglas sin recertificar en más de 12 meses confirma esta brecha desde dos fuentes independientes: la percepción del equipo y la evidencia técnica de NetBrain.

P8Área: Gestión de Incidentes

¿Cómo se gestiona actualmente un incidente de seguridad? ¿Existe un procedimiento formal documentado?

El 100% de los colaboradores entrevistados confirmó conocer el canal de reporte de incidentes de seguridad y el procedimiento a seguir ante un evento. Los entrevistados describieron un flujo claro: detección del incidente, reporte al equipo de Ciberseguridad a través del sistema de tickets corporativo, y gestión centralizada por parte del equipo especializado. Los colaboradores del equipo de Ciberseguridad describieron con mayor detalle el proceso de clasificación, contención, erradicación y cierre de incidentes. Los equipos de otras áreas demostraron conocer al menos los pasos iniciales del proceso de reporte. Las herramientas CrowdStrike Falcon y Zscaler fueron mencionadas como fuentes de alertas automáticas que facilitan la detección temprana.

Conclusión: La gestión de incidentes de seguridad es el área con mayor nivel de madurez y conocimiento identificado en el diagnóstico de percepción. El proceso está formalizado, es conocido por todo el personal entrevistado y cuenta con herramientas de detección activa que generan alertas automáticas. No se identificaron brechas en esta área.

P9Área: General

¿Qué aspectos de la seguridad de la información considera que requieren mayor atención o mejora en el departamento de TI?

Las respuestas a esta pregunta abierta convergieron en tres áreas principales de mejora identificadas de forma espontánea por los entrevistados. En primer lugar, la capacitación y concientización fue mencionada por el 79% de los entrevistados (11 de 14) como el área que más requiere atención, destacando la necesidad de formación diferenciada por rol y más frecuente. En segundo lugar, la documentación y estandarización de la infraestructura de red fue señalada por el equipo de Redes (6 colaboradores) como una prioridad, incluyendo la formalización de estándares para VLANs, reglas de firewall y gestión del tráfico GUEST. En tercer lugar, la adaptación local de las políticas de seguridad corporativas fue mencionada por el 43% de los entrevistados (6 personas), quienes indicaron que las políticas globales no siempre son aplicables o comprensibles en el contexto operativo de la sede Costa Rica.

Conclusión: El personal del departamento identifica espontáneamente las mismas tres áreas de mejora que fueron detectadas en los diagnósticos operativo y técnico: capacitación estructurada, estandarización de la red y adaptación local de políticas. Esta convergencia entre la percepción del personal y los hallazgos técnicos refuerza la validez y relevancia de las propuestas de mejora desarrolladas en el Capítulo V.

El diagnóstico de percepción recoge los hallazgos obtenidos a través de entrevistas estructuradas realizadas al personal del departamento de TI de Procter & Gamble, sede Costa Rica. Se entrevistaron un total de 14 colaboradores, representando los equipos de Redes, Ciberseguridad, Cloud, Análisis de Datos, Soporte Técnico, SAP y Desarrollo de Software. Las entrevistas abordaron aspectos relacionados con el conocimiento de políticas, la capacitación recibida, la gestión de accesos y la percepción sobre la madurez de la seguridad de la información dentro de la organización.

4.5 Determinación de Brechas Tecnológicas – Matriz de Cumplimiento ISO 27002

A partir de los resultados obtenidos en los tres diagnósticos anteriores, se elaboró una matriz de brechas que contrasta el estado actual del departamento con los controles establecidos por la norma ISO/IEC 27002:2022. Para cada control se determina si la organización cumple, cumple parcialmente o no cumple, acompañado de la evidencia correspondiente. Esta matriz se enfoca en los controles más relevantes según el contexto de la organización.

Para evaluar el nivel de madurez de cada control de seguridad analizado, se utilizó una escala basada en el **Modelo de Madurez de Capacidades (CMM, por sus siglas en inglés: Capability Maturity Model)**, desarrollado por el Software Engineering Institute (SEI) de la Universidad Carnegie Mellon (1993). Este modelo fue posteriormente adaptado al contexto de los Sistemas de Gestión de Seguridad de la Información (SGSI) y es ampliamente referenciado en la literatura de ciberseguridad para medir el nivel de implementación de controles organizacionales.

La escala utilizada comprende seis niveles:

- **Nivel 0 — Inexistente:** No existe ningún control ni proceso relacionado.
- **Nivel 1 — Inicial/Ad hoc:** Existen prácticas, pero son informales, reactivas y dependen de personas individuales, sin documentación ni repetibilidad garantizada.
- **Nivel 2 — Repetible pero informal:** Las prácticas se aplican de forma recurrente, pero sin un estándar documentado que las formalice.
- **Nivel 3 — Definido:** Los procesos están documentados, estandarizados y comunicados formalmente a los responsables.
- **Nivel 4 — Gestionado y medido:** Los procesos se ejecutan con métricas de seguimiento, revisión periódica y evidencia documentada de su efectividad.
- **Nivel 5 — Optimizado:** Existe un ciclo de mejora continua documentado, con ajustes proactivos basados en métricas y lecciones aprendidas.

Tabla 9

Matriz de Brechas Tecnológicas — Controles ISO/IEC 27002:2022 con Nivel de Madurez y Justificación Técnica

Política / Procedimiento	Control ISO 27002:2022	Descripción del Control	Estado de Cumplimiento	Nivel de Madurez (Actual → Prop.)	Evidencia Técnica Observada	Criterio de Cumplimiento	Justificación Técnica de la Brecha
Política de Seguridad de la Información	**A.5.1 Cláusula 5.2**	Políticas para la seguridad de la información	**Cumple parcialmente**	2 → 4	Política corporativa global P&G documentada y accesible. Sin versión adaptada al contexto operativo de la sede Costa Rica.	Cumple: Política local aprobada, publicada y revisada anualmente. Cumple parcialmente: Política global existente sin adaptación local. No cumple: Ausencia de política documentada.	La política corporativa de P&G cubre los principios generales pero no incluye procedimientos específicos aplicables al contexto normativo y operativo de Costa Rica. El 67% del personal conoce la política global, pero solo el 33% puede describir su aplicación local, evidenciando una brecha de adaptación y comunicación.
Procedimiento de Gestión de Accesos	**A.5.15 A.5.16 A.5.18**	Roles y responsabilidades / Control de acceso e identidades	**Cumple parcialmente**	2 → 4	Controles de autenticación activos. Sin revisión periódica documentada de accesos asignados. Riesgo de accesos huérfanos o con privilegios excesivos identificado en entrevistas.	Cumple: Proceso formal con revisión periódica documentada. Cumple parcialmente: Provisión activa sin revisión periódica formal. No cumple: Sin proceso de gestión de accesos.	El proceso de provisión de accesos está operativo, pero la ausencia de revisiones periódicas documentadas representa una brecha frente a los controles A.5.15 y A.5.18. Podrían existir accesos huérfanos o con privilegios excesivos no detectados que expongan a la organización a riesgos de acceso indebido.
Política de Resguardo de Información (Backup)	**A.8.13**	Copias de seguridad de la información	**Cumple**	4 → 4	Respaldos periódicos estructurados activos. 22 VMs con snapshots en VMware vSphere 7.0. BCP/DRP formalmente definido y documentado.	Cumple: Política formal, respaldos periódicos y pruebas de recuperación documentadas. Cumple parcialmente: Respaldos sin política formal o sin pruebas. No cumple: Sin proceso de backup.	La organización cuenta con política formal, respaldos periódicos y estructurados, y un plan de continuidad que contempla los procedimientos de recuperación. No se identificaron brechas en este control.

Política / Procedimiento	Control ISO 27002:2022	Descripción del Control	Estado de Cumplimiento	Nivel de Madurez (Actual → Prop.)	Evidencia Técnica Observada	Criterio de Cumplimiento	Justificación Técnica de la Brecha
Gestión de Incidentes de Seguridad	**A.5.24 A.5.25 A.5.26 A.5.27**	Gestión de incidentes de seguridad de la información	**Cumple**	4 → 4	Procedimiento centralizado activo. Equipo de Ciberseguridad (20 personas) como responsable. CrowdStrike Falcon y Zscaler generan alertas automáticas. Sistema de tickets activo.	Cumple: Procedimiento formal, equipo responsable definido y herramientas de detección activas. Cumple parcialmente: Proceso informal o sin herramientas activas. No cumple: Sin proceso de gestión de incidentes.	La organización cuenta con un proceso de gestión de incidentes formalizado, equipo responsable definido y herramientas de detección activa. El personal conoce el canal de reporte. No se identificaron brechas en este control.
Plan de Continuidad del Negocio (BCP/DRP)	**A.5.29 A.5.30**	Seguridad de la información durante la interrupción / Preparación TIC para continuidad	**Cumple**	4 → 4	BCP/DRP formalmente definido. SD-WAN redundante con disponibilidad del 99.8%. Dos enlaces independientes con conmutación automática entre ellos.	Cumple: Plan formal documentado y probado periódicamente con RTO/RPO definidos. Cumple parcialmente: Plan existente sin pruebas periódicas. No cumple: Sin plan de continuidad.	La organización cuenta con un BCP/DRP formal y una infraestructura tecnológica redundante (SD-WAN dual, snapshots activos) que respalda la continuidad operativa. No se identificaron brechas en este control.
Política de Clasificación de la Información	**A.5.9 A.5.10 A.5.12 A.5.13**	Inventario y clasificación de activos de información	**Cumple parcialmente**	2 → 4	Clasificación definida a nivel corporativo global. Aplicación inconsistente en sede Costa Rica. Personal no aplica criterios de forma sistemática en su trabajo diario.	Cumple: Política local con criterios claros, aplicación consistente y capacitación específica. Cumple parcialmente: Clasificación global sin adaptación ni aplicación local consistente. No cumple: Sin política de clasificación.	La política existe a nivel corporativo pero no ha sido adaptada ni internalizada en la sede Costa Rica. La aplicación es dispar entre equipos y colaboradores, generando riesgo de manejo inadecuado de información sensible por desconocimiento de los criterios aplicables localmente.
Procedimiento de Control de Cambios	**A.8.32**	Gestión de cambios en instalaciones y sistemas de información	**Cumple parcialmente**	2 → 4	Proceso de change management activo con sistema de tickets. No siempre incluye evaluación explícita del impacto en seguridad. NetBrain confirma ~15% de reglas firewall sin recertificar en más de 12 meses.	Cumple: Proceso formal con evaluación de impacto en seguridad como paso obligatorio. Cumple parcialmente: Proceso activo sin evaluación de seguridad sistemática. No cumple: Sin proceso de control de cambios.	El proceso de control de cambios está operativo pero la dimensión de seguridad no siempre se evalúa de forma sistemática como paso obligatorio. Esto es consistente con el hallazgo de reglas de firewall con más de 12 meses sin recertificar, evidenciando que cambios en configuraciones de seguridad no siempre siguen el rigor requerido.

Política / Procedimiento	Control ISO 27002:2022	Descripción del Control	Estado de Cumplimiento	Nivel de Madurez (Actual → Prop.)	Evidencia Técnica Observada	Criterio de Cumplimiento	Justificación Técnica de la Brecha
Política de Capacitación y Concientización en Seguridad	**A.6.3 A.7.2**	Concientización, educación y capacitación en seguridad de la información	**No cumple**	1 → 3	Política no formalizada. Solo el 33% del personal recibió capacitación formal en el último año (14 entrevistas realizadas). Sin programa estructurado por rol, evaluaciones ni métricas de cobertura.	Cumple: Programa anual estructurado por rol, cobertura 100%, evaluaciones y métricas documentadas. Cumple parcialmente: Capacitaciones esporádicas sin programa formal. No cumple: Ausencia de política y programa de capacitación.	La organización no cuenta con política formalizada de capacitación en seguridad. Con solo el 33% del personal capacitado formalmente, aproximadamente 112 de los 167 colaboradores del departamento de TI no recibieron formación en el período analizado. Es la brecha con mayor exposición al riesgo humano identificada en el diagnóstico.
—	**A.5.2**	Roles y responsabilidades de seguridad de información	**Cumple parcialmente**	2 → 4	Roles técnicos definidos por equipos (Redes 20, Ciberseguridad 20, Cloud 15, etc.). Sin matriz RACI de seguridad formalmente documentada.	Cumple: Matriz RACI publicada, comunicada y revisada. Cumple parcialmente: Roles definidos sin RACI formal de seguridad. No cumple: Roles no definidos.	Aunque la estructura organizativa está definida, no existe un documento RACI que asigne responsabilidades específicas de seguridad por control ISO. Esto dificulta la rendición de cuentas ante auditorías internas y externas.
—	**A.6.1**	Dispositivos endpoint y trabajo remoto	**Cumple**	4 → 4	CrowdStrike Falcon (EDR) activo en todos los endpoints. Zscaler Zero Trust implementado para acceso seguro a internet. Política de trabajo remoto vigente.	Cumple: EDR activo en 100% de endpoints con cobertura documentada y política de teletrabajo vigente. Cumple parcialmente: Cobertura parcial o política sin formalizar. No cumple: Sin solución endpoint ni política.	Control cubierto satisfactoriamente. CrowdStrike Falcon provee detección y respuesta en endpoints; Zscaler garantiza acceso seguro remoto bajo modelo Zero Trust. No se identificaron brechas en este control.
—	**A.8.3**	Gestión de medios de almacenamiento	**Cumple parcialmente**	2 → 3	No existe procedimiento formal documentado para el ciclo de vida de medios físicos (clasificación, traslado, destrucción segura). Sin registro de trazabilidad de medios.	Cumple: Procedimiento formal con clasificación, traslado, destrucción certificada y registro trazable. Cumple parcialmente: Prácticas informales sin procedimiento documentado. No cumple: Sin gestión de medios.	La organización gestiona medios de almacenamiento de forma práctica pero sin un procedimiento formal que garantice la destrucción segura de activos con información confidencial al final de su vida útil. Esto expone a la organización a riesgo de filtración de datos mediante medios mal desechados.

Política / Procedimiento	Control ISO 27002:2022	Descripción del Control	Estado de Cumplimiento	Nivel de Madurez (Actual → Prop.)	Evidencia Técnica Observada	Criterio de Cumplimiento	Justificación Técnica de la Brecha
—	**A.8.24**	Uso de criptografía	**Cumple**	4 → 4	Comunicaciones cifradas con TLS activo. Discos encriptados en todos los equipos corporativos. Zscaler gestiona el tráfico cifrado hacia internet.	Cumple: Cifrado TLS en comunicaciones, discos encriptados en endpoints y política de criptografía documentada. Cumple parcialmente: Cifrado parcial o sin política formal. No cumple: Sin controles criptográficos.	Control cubierto satisfactoriamente. La organización aplica cifrado tanto en tránsito (TLS, Zscaler) como en reposo (discos encriptados). No se identificaron brechas en este control.
—	**A.8.20 A.8.21**	Seguridad en redes y servicios de red (VLANs y Firewall FortiGate)	**Cumple parcialmente**	2 → 4	17 switches con VLANs activas segregadas por área. 2 firewalls FortiGate operativos. NetBrain confirma ~15% de reglas con más de 12 meses sin recertificar. Sin estándar documentado de nomenclatura VLAN ni convención de reglas firewall.	Cumple: Estándar de nomenclatura documentado, reglas recertificadas anualmente, trazabilidad en NetBrain. Cumple parcialmente: VLANs y FW activos sin estándares formales documentados. No cumple: Sin segmentación ni firewall.	Los equipos FortiGate y los 17 switches operan correctamente, pero la ausencia de estándar formal genera: (1) inconsistencias de nomenclatura entre equipos que dificultan la auditoría, (2) ~15% de reglas firewall con más de 12 meses sin recertificar, y (3) dificultad para validar el principio de mínimo privilegio en las reglas existentes.
—	**A.8.20 A.8.22**	Segmentación de red inalámbrica GUEST (177 APs, 2 WLC)	**Cumple parcialmente**	2 → 4	VLAN Guest aislada existente en los 177 APs administrados por 2 WLC. SSID IoT sin segmentación adicional documentada. Sin estándar formal de filtrado, autenticación (WPA3/802.1X) ni proceso de revisión periódica.	Cumple: Estándar documentado con VLAN GUEST dedicada, WPA3/802.1X, reglas FW restrictivas, monitoreo Zabbix y revisión semestral. Cumple parcialmente: Aislamiento existente sin estándar formal. No cumple: Sin segmentación de tráfico GUEST.	Aunque existe una VLAN Guest configurada, la ausencia de estándar documentado implica: (1) sin garantía de implementación uniforme en los 177 APs, (2) protocolo de autenticación no estandarizado (WPA3/802.1X no requerido formalmente), y (3) tráfico GUEST sin monitoreo documentado en Zabbix para detectar anomalías.
—	**A.5.19 A.5.20**	Seguridad en relaciones con proveedores	**Cumple**	3 → 3	Contratos corporativos P&G con cláusulas de seguridad vigentes a nivel global para todos los proveedores tecnológicos.	Cumple: Contratos con cláusulas de seguridad formales, revisión periódica y gestión de riesgo de terceros documentada. Cumple parcialmente: Contratos sin cláusulas explícitas o sin revisión. No cumple: Sin acuerdos de seguridad con proveedores.	Control cubierto por la política corporativa global de P&G, que incluye cláusulas de seguridad en todos los contratos con proveedores tecnológicos. No se identificaron brechas específicas para la sede Costa Rica en este control.

Leyenda de Estado: ■ Cumple ■ Cumple parcialmente ■ No cumple Escala de Madurez: 0-Inexistente | 1-Inicial | 2-Repetible | 3-Definido | 4-Gestionado | 5-Optimizado

Nota: Matriz de cumplimiento basada en los controles de ISO/IEC 27002:2022. El nivel de madurez se evalúa con escala CMM adaptada a SGSI (0-5). La evidencia técnica proviene de observación directa, entrevistas al personal de TI y revisión de configuraciones en NetBrain (2026).

Fuente: Elaboración propia

4.6 Síntesis del Diagnóstico

A partir del análisis técnico, operativo y de percepción realizado en el departamento de Tecnologías de Información de Procter & Gamble en Costa Rica, se identifican una serie de brechas significativas en la gestión de la seguridad de la información, en comparación con los lineamientos establecidos por la norma ISO/IEC 27001:2022 y los controles de la ISO/IEC 27002:2022.

En primer lugar, a nivel organizacional, se evidencia que, aunque existen políticas y procedimientos relacionados con la seguridad de la información, estos no se encuentran completamente formalizados bajo un Sistema de Gestión de Seguridad de la Información (SGSI). Esto limita la capacidad de la organización para gestionar la seguridad de forma estructurada, basada en riesgos y alineada a un ciclo de mejora continua (PHVA).

En cuanto a la gestión de accesos, se identificó la ausencia de un proceso formal de revisión periódica de privilegios, lo cual incrementa el riesgo de accesos indebidos y posibles vulneraciones a la confidencialidad de la información. Esta situación representa una desviación relevante respecto a los controles A.5.15, A.5.16 y A.5.18 de la norma ISO/IEC 27002:2022.

A nivel técnico, la infraestructura tecnológica presenta un alto grado de madurez en cuanto a herramientas de seguridad (EDR, Zero Trust, firewalls, SD-WAN), sin embargo, se detecta una falta de estandarización y documentación formal en aspectos críticos como:

- Segmentación de redes (especialmente IoT y Guest)
- Nomenclatura de VLANs
- Gestión de reglas de firewall
- Monitoreo estructurado de eventos de seguridad

Esto genera un riesgo operativo, ya que la dependencia de configuraciones no documentadas puede afectar la continuidad operativa y la capacidad de respuesta ante incidentes.
Adicionalmente, se identificó obsolescencia tecnológica en componentes críticos como los Access Points y controladores inalámbricos, lo cual representa un riesgo alto de seguridad debido a la pérdida de soporte del fabricante.
Desde la perspectiva de cultura organizacional, los resultados de percepción evidencian oportunidades de mejora en la concientización y capacitación en seguridad de la información, lo que puede incrementar la probabilidad de incidentes asociados al factor humano.
Finalmente, la matriz de cumplimiento ISO 27002 evidencia que la organización presenta un nivel de madurez intermedio, con controles parcialmente implementados, pero sin un enfoque integral de gestión basado en riesgos.

En conclusión, las principales brechas identificadas se concentran en:

- Ausencia de un SGSI formal
- Falta de gobernanza y estandarización
- Deficiencias en gestión de accesos
- Debilidades en documentación técnica
- Riesgos asociados a obsolescencia tecnológica
- Limitaciones en cultura de seguridad

Estas brechas justifican la necesidad de una propuesta estructurada que permita evolucionar hacia un modelo de seguridad alineado con ISO 27001.

TABLA DE TRAZABILIDAD (Acá en la columna que dice propuesta sería como explicar un poco a solución, no solo poner lo que te puse en la columna)

Hallazgo (Cap 4)	**Riesgo**	**Control ISO**	**Propuesta (Cap 5)**
No existe SGSI formal	Alto	Cláusulas 4–10 ISO 27001	Implementación de SGSI
No hay revisión de accesos	Alto	A.5.15, A.5.18	Proceso de recertificación de accesos
Red sin estándar definido	Medio	A.8.20	Estándar de segmentación WiFi
VLAN sin nomenclatura	Medio	A.5.9	Estándar de VLANs
Reglas firewall sin control	Alto	A.8.20	Gestión y monitoreo de reglas
Equipos sin soporte	Alto	A.5.30	Plan de renovación tecnológica
Falta capacitación	Medio	A.6.3	Programa de concientización
Falta control de medios	Medio	A.7.10	Procedimiento de medios

4.7 Cierre del Capítulo

En este capítulo se desarrolló el diagnóstico integral de la situación actual del departamento de IT de Procter & Gamble, sede Costa Rica, abordando cuatro dimensiones complementarias. El diagnóstico operativo evidenció que la organización cuenta con procesos consolidados en gestión de incidentes, respaldos y continuidad del negocio, mientras que áreas como la capacitación en seguridad, la adaptación local de políticas y la revisión periódica de accesos presentan brechas que requieren atención. El diagnóstico técnico confirmó una infraestructura de nivel empresarial con equipos activos y con soporte del fabricante, destacando como hallazgo crítico que los 177 Access Points Cisco 9130AXI y los 2 WLC Catalyst 9800-40 alcanzarán su End of Support en diciembre de 2025, además de identificar el ~15% de reglas de firewall FortiGate sin recertificar y la ausencia de estándares documentados para VLANs. El diagnóstico de percepción, basado en entrevistas semiestructuradas a 14 colaboradores, validó estos hallazgos desde la perspectiva del propio personal: el 79% identificó la capacitación como prioridad, el equipo de Redes confirmó la ausencia de estándares de red, y la convergencia entre la percepción sobre las revisiones de firewall y el dato técnico de NetBrain reforzó la solidez del análisis. Finalmente, la matriz de cumplimiento ISO/IEC 27002:2022 concluyó que cuatro controles cumplen satisfactoriamente, nueve cumplen parcialmente y uno no cumple, con la mayoría de los controles en nivel de madurez 2, lo que refleja que las brechas son principalmente de formalización y documentación. Estos hallazgos constituyen la base objetiva sobre la cual se desarrollan las propuestas de mejora del Capítulo V.

CAPÍTULO V

PROPUESTA DE PROYECTO

5.1 Introducción

El presente capítulo desarrolla las propuestas de mejora para el fortalecimiento de la seguridad de la información en el departamento de Tecnologías de Información de Procter & Gamble, sede Costa Rica. Estas propuestas se elaboran desde la perspectiva de un análisis consultor profesional, partiendo de los hallazgos concretos identificados en el Capítulo IV y respondiendo directamente a cada brecha documentada en la matriz de cumplimiento ISO/IEC 27002:2022.

Las propuestas se estructuran en cuatro bloques que siguen la lógica de un Sistema de Gestión de Seguridad de la Información (SGSI): primero se abordan las políticas y procedimientos como base normativa, luego la infraestructura de red y hardware como capa técnica, y finalmente las capacitaciones como pilar del factor humano. Cada propuesta incluye la situación actual identificada, la mejora propuesta, el control ISO que la justifica, los recursos técnicos requeridos y el impacto esperado en términos de nivel de madurez.

La metodología aplicada sigue el ciclo de mejora continua PDCA (Plan–Do–Check–Act) adoptado por ISO/IEC 27001:2022, garantizando que cada iniciativa sea planificada, ejecutada, evaluada y ajustada de forma sistemática.

5.2 Enfoque Metodológico de la Propuesta

La propuesta se fundamenta en la implementación progresiva de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001:2022, orientado a gestionar los riesgos identificados en el diagnóstico y fortalecer la gobernanza de la seguridad de la información.

5.3 Adaptación Local de la Política de Seguridad de la Información

5.3.1 Situación Actual

Procter & Gamble dispone de una Política de Seguridad de la Información formalmente documentada y aprobada a nivel corporativo global. Sin embargo, dicha política está diseñada para el contexto multinacional de la compañía y no ha sido adaptada al marco normativo, operativo y cultural específico de la sede Costa Rica. El diagnóstico evidenció que el 67% del personal conoce la política global, pero solo el 33% puede describir cómo

aplica en su trabajo diario. Ninguno de los 14 colaboradores entrevistados indicó conocer un procedimiento local documentado que complemente la política corporativa para la sede.

5.3.2 Brecha Identificada

La ausencia de una adaptación local de la política implica que aspectos críticos como la legislación costarricense aplicable (Ley 8968 de Protección de Datos Personales), los procedimientos operativos específicos de la sede y la estructura organizativa local del departamento de TI no están contemplados en el documento vigente. Esto genera riesgo de incumplimiento normativo local y de aplicación inconsistente de los controles de seguridad entre los diferentes equipos del departamento.

5.3.3 Propuesta Central

Se propone como punto de partida y marco estructural de todas las iniciativas de mejora la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con ISO/IEC 27001:2022 para el departamento de Tecnologías de Información de Procter & Gamble, sede Costa Rica. Un SGSI no es una herramienta tecnológica ni un producto que se adquiere, sino un conjunto integrado de políticas, procesos, procedimientos y controles que, gestionados de forma sistemática, permiten proteger la confidencialidad, integridad y disponibilidad de la información de la organización. Esta propuesta central actúa como el paraguas que dota de coherencia y continuidad a todas las propuestas técnicas específicas desarrolladas en las secciones siguientes: cada propuesta de red, política, capacitación o hardware constituye un control que forma parte del SGSI propuesto.

El primer elemento del SGSI es la definición del alcance, que establece con precisión qué activos, procesos, ubicaciones y personas quedan bajo el sistema de gestión. Conforme a la Cláusula 4.3 de ISO/IEC 27001:2022, el alcance propuesto para P&G Costa Rica comprende el departamento de TI en su totalidad: los 167 colaboradores distribuidos en los equipos de Redes, Ciberseguridad, Cloud, Análisis de Datos, Soporte Técnico, SAP y Desarrollo de Software; la infraestructura tecnológica de la sede incluyendo switches Cisco Catalyst C9300-24UX, firewalls FortiGate 120G, routers SD-WAN Versa VEP 4600, los 177 APs y 2 WLC, el entorno virtualizado de 22 VMs en VMware vSphere 7.0, la plataforma Infoblox 8.6.3 y las soluciones CrowdStrike Falcon y Zscaler; y los procesos operativos de gestión de incidentes, control de cambios, gestión de accesos y continuidad del negocio. Quedan fuera del alcance inicial otras sedes de P&G en la región y los sistemas de producción industrial.

El segundo elemento es la Política de Seguridad de la Información, que según la Cláusula 5.2 de ISO/IEC 27001:2022 debe ser establecida por la alta dirección, apropiada al propósito de la organización e incluir el compromiso de mejora continua del SGSI. Como se identificó en el diagnóstico operativo, P&G dispone de una política corporativa global que no ha sido adaptada al contexto local de Costa Rica. La Propuesta 1 (sección 5.4) desarrolla en detalle

el contenido del documento adaptado; sin embargo, en el marco del SGSI es importante señalar que esta política debe incluir la declaración de compromiso de la dirección local, el alcance definido, los objetivos medibles de seguridad para la sede, la referencia explícita a la Ley 8968 de Protección de Datos Personales de Costa Rica, la designación formal de un responsable del SGSI dentro del equipo de Ciberseguridad, y el ciclo de revisión anual obligatorio.

El tercer elemento es la gestión de riesgos, que constituye el núcleo del SGSI según la Cláusula 6.1 de ISO/IEC 27001:2022. Este proceso permite identificar qué activos pueden verse afectados, por qué amenazas, con qué probabilidad y con qué impacto, para seleccionar los controles más adecuados. Para P&G Costa Rica se propone un proceso de cuatro pasos: primero, inventariar todos los activos de información dentro del alcance y asignarles un propietario responsable; segundo, identificar para cada activo las amenazas relevantes y las vulnerabilidades que podrían ser explotadas — entre las ya identificadas en el diagnóstico se destacan el phishing por falta de capacitación, las reglas de firewall obsoletas por ausencia de recertificación y el riesgo de operar equipos inalámbricos sin soporte del fabricante a partir de diciembre de 2025; tercero, evaluar el nivel de riesgo de cada combinación activo-amenaza-vulnerabilidad clasificándolo en Crítico, Alto, Medio o Bajo para priorizar las acciones; y cuarto, definir la estrategia de tratamiento para cada riesgo: mitigar mediante un control, aceptar con justificación documentada, transferir o evitar. Los resultados de este proceso deben documentarse en un registro formal de riesgos que se revise al menos una vez al año.

El cuarto elemento es la Declaración de Aplicabilidad (Statement of Applicability — SoA), documento obligatorio según la Cláusula 6.1.3 de ISO/IEC 27001:2022. La SoA lista los controles del Anexo A de ISO/IEC 27002:2022, indica si cada uno es aplicable al contexto de P&G Costa Rica, justifica su inclusión o exclusión, y referencia la propuesta que lo implementa. Es el puente que conecta la evaluación de riesgos con los controles implementados, garantizando que cada propuesta responde a un riesgo identificado.

La siguiente tabla presenta la Declaración de Aplicabilidad para los controles más relevantes identificados durante el diagnóstico:

Tabla SGSI-A

Declaración de Aplicabilidad (SoA) — Controles Seleccionados ISO/IEC 27002:2022 — P&G Costa Rica

Control	Descripción	Aplicabilidad	Propuesta / Justificación
A.5.1	Políticas para la seguridad de la información	**Aplicable**	P1 — Adaptación local de Política de Seguridad
A.5.15	Control de acceso	**Aplicable**	P2 — Revisión periódica de accesos

Control	Descripción	Aplicabilidad	Propuesta / Justificación
A.5.9	Inventario y clasificación de activos	**Aplicable**	P3 — Clasificación local de información
A.6.3	Concientización y formación en seguridad	**Aplicable**	P8 — Programa de capacitación
A.8.3	Gestión de medios de almacenamiento	**Aplicable**	P9 — Procedimiento de gestión de medios
A.8.8	Gestión de vulnerabilidades técnicas	**Aplicable**	P7 — Migración APs/WLC (EoS dic. 2025)
A.8.20	Seguridad en redes	**Aplicable**	P4, P5, P6 — WiFi, VLANs, Firewall
A.8.22	Separación en redes	**Aplicable**	P4 — Estándar red inalámbrica GUEST
A.8.32	Gestión de cambios	**Aplicable**	Integración con proceso de cambios P&G
A.8.13	Copias de seguridad	**Aplicable — ya cumple**	Política de backup corporativa vigente
A.8.24	Uso de criptografía	**Aplicable — ya cumple**	TLS, discos encriptados, Zscaler vigente
A.5.24	Gestión de incidentes de seguridad	**Aplicable — ya cumple**	Procedimiento centralizado vigente
A.5.29	Seguridad durante interrupciones (BCP/DRP)	**Aplicable — ya cumple**	BCP/DRP formalmente definido y vigente
A.5.19	Seguridad en relaciones con proveedores	**Aplicable — ya cumple**	Política corporativa global P&G vigente

Leyenda: ■ Aplicable (requiere mejora) ■ Aplicable — ya cumple (sin acción requerida)

Fuente: Elaboración propia

El quinto elemento es el ciclo de mejora continua PHVA (Planear–Hacer–Verificar–Actuar), adoptado por ISO/IEC 27001:2022 como modelo rector del SGSI. Este ciclo garantiza que el sistema no sea un esfuerzo puntual sino un proceso continuo que se adapta a los cambios del entorno tecnológico, organizacional y normativo. En el contexto de P&G Costa Rica, la fase de Planear corresponde a los primeros dos meses del plan, durante los cuales se formaliza el alcance, se aprueba la política local y se ejecuta la evaluación de riesgos inicial. La fase de Hacer abarca los meses 2 al 9, durante los cuales se implementan las nueve propuestas técnicas del capítulo. La fase de Verificar, en los meses 9 y 10, consiste en auditar los controles implementados, medir el nivel de madurez alcanzado en la matriz ISO/IEC 27002:2022 y revisar los indicadores del programa de capacitación. Finalmente, la fase de

Actuar define las acciones correctivas para los controles que no alcanzaron el nivel proyectado y reinicia el ciclo para el siguiente período anual.

Tabla SGSI-B

Ciclo PHVA aplicado al SGSI de P&G Costa Rica

PLANEAR (P)	HACER (H)	VERIFICAR (V)	ACTUAR (A)
Definir alcance, política y evaluación de riesgos	Implementar controles, estándares y capacitaciones	Auditar controles y medir nivel de madurez ISO	Corregir brechas y reiniciar el ciclo de mejora

Fuente: Elaboración propia

La implementación de este SGSI no es un prerrequisito bloqueante para las propuestas técnicas específicas: estas pueden avanzar en paralelo durante la fase de Hacer del ciclo PHVA. Sin embargo, el SGSI provee el contexto normativo y estratégico que justifica, prioriza y da sostenibilidad a cada una de las propuestas desarrolladas en las secciones 5.4 a 5.11, transformándolas de iniciativas aisladas en un sistema integrado de gestión de la seguridad de la información alineado con ISO/IEC 27001:2022.

5.3.4 Propuesta de Mejora

Se propone la revisión, actualización y formalización de la Política de Seguridad de la Información adaptada al contexto de la sede Costa Rica, tomando como base la política corporativa global de P&G. El documento local deberá incluir los siguientes elementos mínimos:

- Declaración de compromiso de la dirección local con la seguridad de la información.
- Alcance y ámbito de aplicación específico para la sede Costa Rica.
- Marco normativo local aplicable: Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales.
- Definición de roles y responsabilidades, incluyendo la designación formal de un responsable del SGSI local.
- Principios de confidencialidad, integridad y disponibilidad aplicados al contexto operativo local.
- Sanciones por incumplimiento conforme a la legislación laboral costarricense.
- Ciclo de revisión periódica de la política (mínimo anual o ante cambios significativos).
- Procedimiento de comunicación y capacitación sobre la política para los 167 colaboradores del departamento.

Control ISO que justifica esta propuesta: A.5.1 (Políticas para la seguridad de la información) — Cláusula 5.2 ISO/IEC 27001:2022
Impacto esperado: Elevar el nivel de madurez de 2 (Repetible) a 4 (Gestionado). Reducción del riesgo de incumplimiento normativo local y mejora en la comprensión y aplicación de los controles por parte del personal.

5.4 Formalización del Proceso de Revisión Periódica de Accesos

5.4.1 Situación Actual

El departamento de TI de P&G Costa Rica cuenta con un proceso operativo de provisión de accesos mediante el sistema corporativo de tickets, con autenticación multifactor activa para sistemas críticos. Sin embargo, el diagnóstico de percepción reveló que el 100% de los líderes de equipo entrevistados confirmó que las revisiones periódicas de los accesos ya asignados no se realizan de forma documentada y sistemática. Ningún líder pudo indicar la fecha o frecuencia de la última revisión completa de accesos en su área.

5.4.2 Brecha Identificada

La ausencia de un proceso formal de revisión periódica de accesos genera riesgo de acumulación de accesos huérfanos (cuentas de empleados que cambiaron de rol o abandonaron la organización) y accesos con privilegios excesivos no detectados. Este riesgo es especialmente relevante en un departamento con 167 colaboradores distribuidos en siete equipos con diferentes niveles de acceso a sistemas críticos.

5.4.3 Propuesta de Mejora

Se propone la implementación de un proceso formal trimestral de revisión de accesos, que incluya los siguientes componentes:

Ciclo de revisión trimestral: cada equipo del departamento de TI deberá ejecutar una revisión completa de los accesos asignados a sus colaboradores, verificando que cada acceso tenga justificación de negocio vigente y que corresponda al rol actual del colaborador.

Responsable del proceso: el líder de cada equipo es el responsable de ejecutar y documentar la revisión. El equipo de Ciberseguridad actúa como auditor del proceso.

Evidencia documentada: cada revisión debe generar un registro formal que indique: usuario, sistemas accedidos, justificación del acceso, fecha de revisión y resultado (mantener, modificar o revocar).

Integración con el proceso de offboarding: al momento de que un colaborador cambie de rol o se desvincule de la organización, el sistema de tickets debe disparar automáticamente una tarea de revisión y revocación de accesos.

Métricas de seguimiento: número de accesos revisados, número de accesos revocados y tiempo promedio de revocación tras baja de usuario.

Control ISO que justifica esta propuesta: A.5.15 (Control de acceso), A.5.16 (Gestión de identidades), A.5.18 (Derechos de acceso) — ISO/IEC 27002:2022

Impacto esperado: Elevar el nivel de madurez de 2 (Repetible) a 4 (Gestionado). Eliminación de accesos huérfanos y reducción del riesgo de acceso indebido a sistemas críticos.

5.5 Adaptación Local de la Política de Clasificación de la Información

5.5.1 Situación Actual

P&G cuenta con una política corporativa global de clasificación de la información que define categorías de sensibilidad. Sin embargo, el diagnóstico operativo y de percepción identificaron que su aplicación en la sede Costa Rica es inconsistente: parte del personal no aplica sistemáticamente los criterios de clasificación en su trabajo diario, y no existe un procedimiento local que explique cómo aplicar las categorías corporativas al contexto específico de los documentos y datos que maneja el departamento de TI de Costa Rica.

5.5.2 Brecha Identificada

La aplicación dispar de los criterios de clasificación entre equipos genera riesgo de manejo inadecuado de información sensible, especialmente en áreas como Análisis de Datos, SAP y Desarrollo de Software, donde se trabaja con datos de producción, información financiera y datos de clientes corporativos.

5.5.3 Propuesta de Mejora

Se propone elaborar un procedimiento local de clasificación de la información que adapte los criterios corporativos globales al contexto operativo de la sede Costa Rica, estableciendo ejemplos concretos por categoría aplicados a los tipos de información que maneja cada equipo del departamento:

•Pública: Comunicados de prensa, información publicada en sitio web corporativo, presentaciones de productos.

•Interna: Procedimientos operativos, manuales de usuario, documentación técnica de infraestructura no sensible.

•Confidencial: Datos de clientes, información financiera, configuraciones de sistemas de seguridad, credenciales de acceso.

•Restringida: Datos personales protegidos por Ley 8968, información de auditorías de seguridad, claves criptográficas.

El procedimiento también deberá incluir las instrucciones de manejo, almacenamiento, transmisión y destrucción segura para cada nivel de clasificación, adaptadas a las herramientas tecnológicas que utiliza P&G Costa Rica.

Control ISO que justifica esta propuesta: A.5.9 (Inventario de activos de información), A.5.12 (Clasificación de la información), A.5.13 (Etiquetado de la información) — ISO/IEC 27002:2022

Impacto esperado: Elevar el nivel de madurez de 2 (Repetible) a 4 (Gestionado). Aplicación consistente de los criterios de clasificación en todos los equipos del departamento.

5.6 Estándar para la Red Inalámbrica GUEST, Corporativa e IoT

5.6.1 Situacion Actual

La red inalámbrica de P&G Costa Rica opera con 177 Access Points Cisco 9130AXI administrados por 2 WLC Catalyst 9800-40, con tres SSIDs activos: corporativo, Guest e IoT. Si bien existe un aislamiento básico del tráfico GUEST mediante una VLAN dedicada, no existe un estándar formal documentado que defina el protocolo de autenticación, la segmentación, las reglas de firewall y el proceso de monitoreo aplicable a cada SSID. El SSID IoT tampoco cuenta con segmentación adicional documentada.

5.6.2 Brecha Identificada

La ausencia de un estándar formal implica que no hay garantía de que los 177 APs implementen el aislamiento de forma uniforme, que el protocolo de autenticación inalámbrica no está estandarizado (WPA3/802.1X no está formalmente requerido), y que el tráfico GUEST no cuenta con monitoreo documentado en Zabbix para detectar anomalías o usos indebidos de la red de invitados.

5.6.3 Propuesta de Mejora — Estándar de SSIDs

Se propone la definición e implementación del siguiente estándar de autenticación y segmentación para los tres SSIDs activos:

Tabla P2-A

Estándar de SSIDs, Protocolos de Autenticación y Segmentación de Red Inalámbrica — P&G Costa Rica

SSID	Nombre de Red	Protocolo de Autenticación	VLAN y Rango IP	Acceso Permitido
SSID Corporativo	PGCR-CORP	WPA3-Enterprise + 802.1X (RADIUS)	VLAN 200 — 10.200.0.0/22	Acceso total red interna + internet
SSID Invitados	PGCR-GUEST	WPA3-Personal (PSK rotativa 30d)	VLAN 201 — 10.201.0.0/23	Solo internet, bloqueado a red Corp
SSID IoT	PGCR-IOT	WPA2-PSK (AES)	VLAN 202 — 10.202.0.0/23	Aislado, bloqueado a Corp y Guest

Nota: WPA3-Enterprise requiere infraestructura de autenticación RADIUS/802.1X. PSK GUEST debe rotarse cada 30 días conforme al estándar propuesto.

Fuente: Elaboración propia basada en estándares IEEE 802.11ax, Wi-Fi Alliance WPA3 y controles A.8.20/A.8.22 de ISO/IEC 27002:2022 (2026).

5.6.4 Flujo de Autenticación 802.1X (WPA3-Enterprise) para Red Corporativa

El estándar propuesto para el SSID corporativo implementa autenticación basada en IEEE 802.1X con servidor RADIUS. El flujo de autenticación opera de la siguiente manera: el dispositivo se conecta al AP y el WLC redirige las credenciales al servidor RADIUS corporativo de P&G, que valida contra el Active Directory. Según el resultado, el WLC asigna dinámicamente la VLAN correspondiente.

Tabla P2-B

Flujo de Autenticación 802.1X — Asignación Dinámica de VLAN por Tipo de Cliente

Tipo de Cliente	Método de Autenticación	Validación	VLAN Asignada
Dispositivo corporativo	Certificado digital (EAP-TLS)	Dominio P&G + CrowdStrike activo	**VLAN 200 CORP**

Tipo de Cliente	Método de Autenticación	Validación	VLAN Asignada
Usuario con credenciales	Usuario/contraseña (PEAP-MSCHAPv2)	Active Directory P&G	**VLAN 200 CORP**
Dispositivo no reconocido	Falla de autenticación	Sin match en AD o sin certificado	**VLAN 999 QUARANTINE**
Invitado / externo	PSK GUEST (sin 802.1X)	WLC valida SSID GUEST	**VLAN 201 GUEST**

Nota: EAP-TLS requiere certificado digital emitido por la PKI corporativa P&G. PEAP-MSCHAPv2 utiliza credenciales de Active Directory. Dispositivos no reconocidos son enviados a VLAN 999 (Quarantine) hasta validación manual.

Fuente: Elaboración propia basada en RFC 3748 (EAP), IEEE 802.1X y controles A.8.22 de ISO/IEC 27002:2022 (2026).

5.6.5 Configuración de Referencia en WLC (Cisco WLC / FortiGate)

A continuación se presenta la configuración de referencia para implementar el estándar en los 2 WLC Cisco 9800-40 y en los firewalls FortiGate 120G. Esta configuración debe aplicarse en ambos WLC y documentarse en NetBrain como configuración base auditada. Se incluye una explicación del propósito de seguridad de cada comando para facilitar su comprensión y auditoría.

Explicación de los comandos — WLC Cisco (SSID GUEST)

Comando / Parámetro	Función y propósito en seguridad
`wlan PGCR-GUEST 2`	Crea el perfil WLAN con el nombre 'PGCR-GUEST' y le asigna el identificador de red 2. Este nombre es el SSID que verán los invitados al buscar redes Wi-Fi.
`security wpa akm psk`	Activa el método de autenticación PSK (Pre-Shared Key), es decir, una contraseña compartida para la red de invitados. No requiere servidor RADIUS.
`security wpa wpa3`	Configura el protocolo de seguridad WPA3, que ofrece cifrado más robusto que WPA2 y protección contra ataques de diccionario en la contraseña.
`security wpa akm psk set-key ascii 0 [PSK]`	Define la contraseña de la red GUEST. Debe rotarse cada 30 días por el equipo de Ciberseguridad conforme al estándar propuesto.
`client vlan WLAN-GUEST`	Asigna la VLAN 201 a todos los clientes que se conecten al SSID GUEST, garantizando su segmentación respecto a la red corporativa.
`no peer-blocking drop`	Permite comunicación básica entre dispositivos de invitados (necesario para algunos servicios de invitados), manteniendo el bloqueo hacia la red corporativa que se aplica en el firewall.

Comando / Parámetro	Función y propósito en seguridad
`session-timeout 3600`	Limita la sesión de cada invitado a 1 hora máximo, reduciendo el tiempo de exposición de dispositivos no gestionados en la red.
`dhcp-opt82 enable`	Agrega información de ubicación del AP en las solicitudes DHCP, permitiendo rastrear desde qué AP se conectó cada dispositivo invitado para fines de auditoría.
`no shutdown`	Activa el perfil WLAN para que los APs comiencen a transmitir el SSID GUEST.

Configuración WLC — SSID GUEST (Extracto de referencia)

```
! === CONFIGURACIÓN WLC — SSID GUEST ===
! Aplicar en ambos WLC: WLC-PRIMARY y WLC-SECONDARY
! Documentar en NetBrain tras cada cambio

wlan PGCR-GUEST 2 PGCR-GUEST
  security wpa akm psk
  security wpa wpa3
  security wpa akm psk set-key ascii 0 [PSK-ROTATIVA-30D]
  client vlan WLAN-GUEST
  no peer-blocking drop
  session-timeout 3600
  dhcp-opt82 enable
  no shutdown
```

Explicación de los comandos — FortiGate (Reglas de Firewall para GUEST)

Comando / Parámetro	Función y propósito en seguridad
`config firewall policy`	Entra al modo de configuración de políticas de firewall en FortiGate. Desde aquí se definen todas las reglas de tráfico.
`set name 'CR-SJO-ANY-Allow-GUEST2INET'`	Asigna el nombre a la regla siguiendo la convención estándar: País-Ciudad-Protocolo-Acción-Propósito. Facilita la identificación y auditoría de la regla.
`set srcintf 'VLAN201-GUEST'`	Define la interfaz de origen: todo el tráfico que provenga de la VLAN 201 (red de invitados) será evaluado por esta regla.
`set dstintf 'wan1'`	Define la interfaz de destino: el tráfico se dirige hacia la WAN (internet). Los invitados SOLO pueden salir a internet.
`set srcaddr 'GUEST-SUBNET'`	Especifica el rango de IPs de origen: 10.201.0.0/23. Solo los dispositivos en este rango aplican a esta regla.

Comando / Parámetro	Función y propósito en seguridad
`set service 'HTTP' 'HTTPS' 'DNS'`	Restringe los servicios permitidos: solo navegación web (HTTP/HTTPS) y resolución de nombres (DNS). Los invitados no pueden usar otros protocolos.
`set action accept`	Esta regla permite el tráfico. Los invitados SÍ tienen acceso a internet con los servicios definidos.
`set logtraffic all`	Registra todo el tráfico de esta regla en los logs de FortiGate, cumpliendo con el control A.8.15 de trazabilidad y monitoreo.
`set name 'CR-SJO-ANY-Deny-GUEST2CORP'`	Segunda regla: bloquea el acceso desde la VLAN GUEST hacia la red corporativa interna. Esta es la regla de seguridad crítica.
`set dstintf 'VLAN10-USERS' 'VLAN30-SERVERS'`	Define como destino bloqueado las VLANs de usuarios y servidores corporativos. Ningún dispositivo GUEST puede llegar a estas redes.
`set action deny`	Esta regla bloquea el tráfico. Cualquier intento de un invitado de acceder a la red corporativa será rechazado.

Configuración FortiGate — Reglas GUEST (Extracto de referencia)

```
! === REGLAS FIREWALL FortiGate — RED GUEST ===
! Aplicar en ambos FW FortiGate 120G

config firewall policy

  ! --- Regla 1: GUEST accede solo a internet ---
  edit 0
    set name 'CR-SJO-ANY-Allow-GUEST2INET'
    set srcintf 'VLAN201-GUEST'
    set dstintf 'wan1'
    set srcaddr 'GUEST-SUBNET'
    set dstaddr 'all'
    set service 'HTTP' 'HTTPS' 'DNS'
    set action accept
    set logtraffic all
    set comments 'GUEST solo internet - ISO A.8.22'
  next

  ! --- Regla 2: BLOQUEAR GUEST hacia red corporativa ---
  edit 0
    set name 'CR-SJO-ANY-Deny-GUEST2CORP'
    set srcintf 'VLAN201-GUEST'
    set dstintf 'VLAN10-USERS' 'VLAN30-SERVERS'
    set srcaddr 'GUEST-SUBNET'
    set dstaddr 'CORP-ALL'
    set service 'ALL'
    set action deny
```

```
    set logtraffic all
    set comments 'Bloqueo total GUEST a red interna - ISO A.8.22'
  next

end
```

Nota: El valor [PSK-ROTATIVA-30D] debe ser reemplazado por la contraseña real, gestionada conforme al procedimiento de credenciales corporativo de P&G. Las reglas de FortiGate deben registrarse con fecha de creación en NetBrain para su recertificación anual.

Fuente: Elaboración propia basada en Cisco WLC CLI Reference Guide y FortiGate Administration Guide 7.x (2026).

Control ISO que justifica esta propuesta: A.8.20 (Seguridad en redes), A.8.22 (Separación en redes) — ISO/IEC 27002:2022

Impacto esperado: Elevar el nivel de madurez de 2 (Repetible) a 4 (Gestionado). Segmentación inalámbrica formal, auditada y uniforme en los 177 APs.

5.7 Estándar de Nomenclatura para VLANs según Función

5.7.1 Situación Actual

Los 17 switches Cisco Catalyst C9300-24UX de la sede operan con VLANs configuradas y segregadas por área funcional. Sin embargo, el diagnóstico técnico y de percepción confirmaron que no existe un estándar documentado que defina la nomenclatura, el rango de direccionamiento IP y la asignación de cada VLAN según su función. El equipo de Redes indicó de forma unánime que existen prácticas informales heredadas, pero sin formalización en NetBrain ni en ningún documento oficial.

5.7.2 Brecha Identificada

La ausencia del estándar genera inconsistencias de nomenclatura entre los 17 switches, dificulta la auditoría de la red, aumenta el riesgo de errores de configuración al incorporar nuevos miembros al equipo y limita la capacidad de respuesta ante incidentes que involucren la capa de red.

5.7.3 Propuesta de Mejora — Estándar de VLANs

Tabla P5-A

Estándar de Nomenclatura, Función y Direccionamiento de VLANs — P&G Costa Rica

ID	Nombre Estándar	Función	Rango IP	Criticidad	Segmento FortiGate
1	DO NOT USE	Reservada — no usar	N/A	**–**	–
7	SATELLITE-PGTV	Señal de televisión P&G (PGTV)	10.7.0.0/24	**Baja**	–
10–29	USERS-[AREA]	VLANs de usuarios corporativos por área	10.10.x.0/24	**Alta**	VLAN10-USERS
30	SERVERS-INT	Servidores internos	10.30.0.0/24	**Alta**	VLAN30-SERVERS
40	SERVERS-DMZ	Servidores en zona desmilitarizada	10.40.0.0/24	**Alta**	VLAN40-DMZ
50–58	SECURITY-[TIPO]	Sistemas de control de acceso físico	10.50.x.0/24	**Alta**	–
59	SECURITY-CAM	Cámaras de seguridad	10.59.0.0/24	**Media**	–
99	PRINTERS	Dispositivos de impresión	10.99.0.0/24	**Baja**	–
101–105	WLAN-MGMT-[N]	Administración de APs y WLC	10.100.x.0/24	**Alta**	–
200	WLAN-CORP	Wi-Fi corporativo autenticado (802.1X)	10.200.0.0/22	**Alta**	VLAN200-CORP
201	WLAN-GUEST	Wi-Fi invitados (solo internet)	10.201.0.0/23	**Media**	VLAN201-GUEST
202	WLAN-IOT	Dispositivos IoT aislados	10.202.0.0/23	**Media**	VLAN202-IOT
800–819	VOICE-IPT-[N]	Telefonía IP corporativa	10.80.x.0/24	**Alta**	–
999	QUARANTINE	Dispositivos en cuarentena	10.99.9.0/24	**Alta**	VLAN999-QUAR

Nota: Los IDs de VLAN siguen el estándar corporativo global P&G. El direccionamiento IP debe validarse contra el esquema IPAM global antes de implementar.

Fuente: Elaboración propia

5.7.4 Configuración de Referencia en Switches Cisco Catalyst

A continuación se presenta la configuración de referencia para implementar el estándar de nomenclatura en los 17 switches Cisco Catalyst C9300-24UX. Se incluye la explicación de cada comando para facilitar su comprensión, auditoría y aplicación por parte del equipo de Redes.

Explicación de los comandos — Configuración de VLANs

Comando / Parámetro	Función y propósito en seguridad
`vlan [ID]`	Crea la VLAN con el número de identificador especificado en el estándar. Cada VLAN es un segmento de red lógicamente aislado que agrupa dispositivos con función similar.
`name [NOMBRE-ESTÁNDAR]`	Asigna el nombre estandarizado a la VLAN según la convención definida (ej: USERS-GENERAL, WLAN-GUEST). Permite identificar la función de cada VLAN sin necesidad de revisar su ID numérico.
`interface GigabitEthernet1/0/1`	Selecciona el puerto físico del switch que se va a configurar. Cada puerto debe configurarse según el tipo de dispositivo que conecta.
`description [DESCRIPCION]`	Agrega una etiqueta descriptiva al puerto, indicando su función y ubicación. Facilita la identificación durante mantenimiento y auditorías sin necesidad de documentación externa.
`switchport mode access`	Configura el puerto como 'acceso', lo que significa que solo transporta tráfico de UNA VLAN. Se usa para conectar dispositivos de usuario final (PCs, impresoras, teléfonos).
`switchport access vlan [ID]`	Asigna el puerto a una VLAN específica. Todo el tráfico que entre por este puerto pertenece a esa VLAN y queda aislado de las demás.
`spanning-tree portfast`	Permite que el puerto pase directamente al estado activo sin esperar el ciclo completo de Spanning Tree (hasta 30 segundos). Solo se usa en puertos de acceso donde se conectan dispositivos finales, no switches.
`spanning-tree bpduguard enable`	Activa la protección contra ataques de Spanning Tree: si alguien conecta un switch no autorizado en este puerto, el puerto se deshabilita automáticamente. Es un control crítico de seguridad de red.
`switchport mode trunk`	Configura el puerto como 'trunk', lo que permite transportar tráfico de MÚLTIPLES VLANs simultáneamente. Se usa para los enlaces hacia firewalls, routers y otros switches.
`switchport trunk allowed vlan [lista]`	Define exactamente qué VLANs pueden circular por el enlace trunk. Solo las VLANs listadas aquí son permitidas, aplicando el principio de mínimo privilegio a nivel de red.

Comando / Parámetro	Función y propósito en seguridad
`switchport trunk native vlan 999`	Configura la VLAN 999 (Quarantine) como nativa en los puertos trunk. El tráfico no etiquetado (sin VLAN asignada) cae automáticamente en cuarentena, aislándolo de la red productiva.
`show vlan brief`	Comando de verificación: muestra un resumen de todas las VLANs configuradas y los puertos asignados a cada una. Permite validar que el estándar fue aplicado correctamente.
`show interfaces trunk`	Muestra los puertos trunk activos y las VLANs que están circulando por cada uno. Se usa para verificar la segmentación y detectar VLANs no autorizadas.

Configuración Switches Cisco C9300-24UX (Extracto de referencia)

```
! === CONFIGURACIÓN DE VLANs — SWITCHES CISCO C9300-24UX ===
! Aplicar en los 17 switches de la sede P&G Costa Rica
! Documentar en NetBrain tras cada cambio

! --- Paso 1: Creación de VLANs con nomenclatura estándar ---
vlan 10
 name USERS-GENERAL
vlan 20
 name USERS-IT
vlan 30
 name SERVERS-INT
vlan 40
 name SERVERS-DMZ
vlan 59
 name SECURITY-CAM
vlan 99
 name PRINTERS
vlan 101
 name WLAN-MGMT-PRIMARY
vlan 200
 name WLAN-CORP
vlan 201
 name WLAN-GUEST
vlan 202
 name WLAN-IOT
vlan 800
 name VOICE-IPT-PRIMARY
vlan 999
 name QUARANTINE

! --- Paso 2: Puerto de acceso (dispositivo de usuario) ---
interface GigabitEthernet1/0/1
 description USERS-GENERAL-FLOOR1
 switchport mode access
 switchport access vlan 10
```

```
 spanning-tree portfast
 spanning-tree bpduguard enable
 no shutdown

! --- Paso 3: Puerto trunk hacia FortiGate ---
interface GigabitEthernet1/0/48
 description TRUNK-TO-FORTIGATE
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,59,99,101,200,201,202,800,999
 switchport trunk native vlan 999
 no shutdown

! --- Verificación posterior ---
show vlan brief
show interfaces trunk
show spanning-tree summary
```

Nota: La VLAN nativa 999 (QUARANTINE) garantiza que el tráfico no etiquetado quede aislado. El BPDU Guard previene la conexión de switches no autorizados. Toda modificación debe registrarse en NetBrain y en el sistema de control de cambios corporativo de P&G.

Fuente: Elaboración propia

Control ISO que justifica esta propuesta: A.8.20 (Seguridad en redes), A.8.21 (Seguridad de servicios de red) — ISO/IEC 27002:2022

Impacto esperado: Elevar el nivel de madurez de 2 (Repetible) a 4 (Gestionado). Nomenclatura uniforme en los 17 switches, auditoría de red facilitada y reducción de errores de configuración.

5.8 Estándar de Nomenclatura y Monitoreo de Reglas de Firewall FortiGate

5.8.1 Situación Actual

Los 2 firewalls FortiGate 120G de la sede operan con FortiOS 7.4.8 y gestionan el filtrado de tráfico entre todos los segmentos de red. El reporte de NetBrain confirma que aproximadamente el 15% de las reglas activas supera los 12 meses sin haber sido recertificadas. No existe una convención formal de nomenclatura para las reglas, lo que dificulta su identificación, auditoría y gestión. El equipo de Redes confirmó durante las entrevistas que las revisiones de reglas se realizan de forma reactiva, sin frecuencia definida.

5.8.2 Brecha Identificada

La ausencia de un estándar de nomenclatura impide identificar rápidamente el propósito de cada regla durante auditorías. Las reglas con más de 12 meses sin recertificar pueden ser obsoletas, ampliando innecesariamente la superficie de ataque y dificultando la validación del principio de mínimo privilegio.

5.8.3 Propuesta de Mejora — Convención de Nomenclatura

Se propone la siguiente convención obligatoria para el nombre de cada regla de firewall:

```
CONVENCIÓN: [PAÍS]-[CIUDAD]-[PROTOCOLO]-[ACCIÓN]-[PROPÓSITO]

Ejemplos válidos:
  CR-SJO-HTTPS-Allow-BROWSING      → Navegación web corporativa
  CR-SJO-ANY-Deny-GUEST2CORP       → Bloqueo Guest a red interna
  CR-SJO-SSH-Allow-NETMGMT         → Admin SSH desde gestión de red
  CR-SJO-ANY-Deny-DEFAULT          → Regla base deny all (última)

Valores permitidos por campo:
  [PAÍS]      : CR
  [CIUDAD]    : SJO
  [PROTOCOLO] : HTTP | HTTPS | DNS | SSH | RDP | SQL | VOICE | ANY
  [ACCIÓN]    : Allow | Deny
  [PROPÓSITO] : Texto descriptivo MAYÚSCULAS sin espacios (máx 20 chars)
```

5.8.4 Catálogo de Reglas de Referencia

Tabla P6-A

Catálogo de Reglas de Referencia — Firewall FortiGate P&G Costa Rica

Nombre de Regla	Origen	Destino	Servicio	Acción	Justificación
CR-SJO-HTTPS-Allow-BROWSING	USERS (10.10.x.0/24)	Internet (any)	TCP 443	**ALLOW**	Navegación web corporativa desde red de usuarios
CR-SJO-DNS-Allow-RESOLVER	ALL-VLANS	10.30.0.10 (DNS)	UDP 53	**ALLOW**	Resolución DNS interna para todos los segmentos
CR-SJO-SSH-Allow-NETMGMT	NETMGMT (10.100.0.0/24)	Switches/APs	TCP 22	**ALLOW**	Administración SSH solo desde hosts de gestión de red
CR-SJO-ANY-Deny-GUEST2CORP	GUEST (10.201.0.0/23)	CORP-ALL	any	**DENY**	Bloqueo total del tráfico de invitados hacia red interna
CR-SJO-ANY-Allow-GUEST2INET	GUEST (10.201.0.0/23)	Internet (any)	HTTP/HTTPS	**ALLOW**	GUEST accede solo a internet con servicios restringidos
CR-SJO-VOICE-Allow-IPT	VOICE (10.80.x.0/24)	PBX (10.30.0.20)	UDP 5060/RTP	**ALLOW**	Tráfico VoIP corporativo hacia el sistema PBX
CR-SJO-ANY-Deny-DEFAULT	any	any	any	**DENY**	Regla base: denegar todo lo no explícitamente permitido

Nota: El orden de las reglas es crítico en FortiGate (first-match). La regla Deny-DEFAULT debe ser siempre la última. Todas las reglas deben tener logtraffic habilitado para cumplir con el control A.8.15.

Fuente: Elaboración propia

5.8.5 Configuración de Referencia en FortiGate (CLI)

A continuación se presenta la configuración CLI de referencia para las reglas críticas del estándar propuesto. Se incluye la explicación de cada comando para facilitar su comprensión, auditoría y aplicación por parte del equipo de Ciberseguridad y Redes.

Explicación de los comandos — FortiGate Firewall Policy

Comando / Parámetro	Función y propósito en seguridad
`config firewall policy`	Entra al modo de configuración de políticas de firewall. Desde aquí se crean, modifican y eliminan las reglas de tráfico que controlan qué puede comunicarse con qué.
`edit 0`	Crea una nueva regla de firewall (el 0 indica nueva entrada; FortiGate asigna el ID automáticamente). Para editar una regla existente se usa su ID numérico.
`set name 'CR-SJO-...'`	Asigna el nombre a la regla siguiendo la convención estándar. Un nombre descriptivo permite identificar el propósito de la regla sin abrir su configuración completa.
`set srcintf 'VLAN...'`	Define la interfaz o VLAN de origen. El firewall aplica esta regla solo al tráfico que provenga de esta interfaz, implementando segmentación por zona de origen.
`set dstintf 'wan1' / 'VLAN...'`	Define la interfaz de destino. Combinado con srcintf, determina entre qué zonas aplica la regla. 'wan1' es la salida a internet.
`set srcaddr 'OBJECT'`	Referencia un objeto de dirección IP predefinido como origen. Usar objetos en lugar de IPs directas facilita cambios futuros: se actualiza el objeto y todas las reglas que lo usan se actualizan automáticamente.
`set dstaddr 'OBJECT'`	Referencia un objeto de dirección IP como destino. Mismo principio que srcaddr.
`set service 'HTTP' 'HTTPS' 'DNS'`	Define los protocolos y puertos permitidos por la regla. Restringir los servicios al mínimo necesario implementa el principio de mínimo privilegio.
`set action accept / deny`	'accept' permite el tráfico; 'deny' lo bloquea. En FortiGate el tráfico bloqueado puede registrarse (logtraffic) para análisis de seguridad.
`set utm-status enable`	Activa los módulos UTM (Unified Threat Management) sobre el tráfico permitido: antivirus, IPS, filtrado web. Agrega una capa de inspección profunda al tráfico.
`set webfilter-profile 'GUEST-WebFilter'`	Aplica un perfil de filtrado web específico para invitados, bloqueando categorías de sitios no deseados (malware, adultos, torrents) en la red GUEST.
`set logtraffic all`	Registra todo el tráfico (permitido y denegado) que coincide con esta regla. Es fundamental para auditorías, análisis forense y cumplimiento del control A.8.15 de trazabilidad.
`set comments 'ISO A.8.XX - ...'`	Agrega una nota explicativa referenciando el control ISO que justifica la regla. Facilita las auditorías de cumplimiento y la comprensión del contexto de negocio de cada regla.
`next / end`	'next' guarda la regla actual y permite configurar la siguiente. 'end' cierra el modo de configuración de políticas y aplica todos los cambios.

Configuración FortiGate CLI — Reglas críticas (Extracto de referencia)

```
! === REGLAS CRÍTICAS — FortiGate 120G P&G Costa Rica ===
! Versión: 1.0 | Responsable: Equipo Redes y Ciberseguridad
! Documentar fecha de creación en NetBrain para recertificación anual

config firewall policy

  ! --- Regla 1: BLOQUEO GUEST a red corporativa (ALTA PRIORIDAD) ---
  edit 10
    set name 'CR-SJO-ANY-Deny-GUEST2CORP'
    set srcintf 'VLAN201-GUEST'
    set dstintf 'VLAN10-USERS' 'VLAN30-SERVERS' 'VLAN40-DMZ'
    set srcaddr 'GUEST-SUBNET'
    set dstaddr 'CORP-ALL'
    set schedule 'always'
    set service 'ALL'
    set action deny
    set logtraffic all
    set comments 'ISO A.8.22 - GUEST no accede a red interna'
  next

  ! --- Regla 2: GUEST accede solo a internet ---
  edit 11
    set name 'CR-SJO-ANY-Allow-GUEST2INET'
    set srcintf 'VLAN201-GUEST'
    set dstintf 'wan1'
    set srcaddr 'GUEST-SUBNET'
    set dstaddr 'all'
    set schedule 'always'
    set service 'HTTP' 'HTTPS' 'DNS'
    set action accept
    set utm-status enable
    set webfilter-profile 'GUEST-WebFilter'
    set logtraffic all
    set comments 'ISO A.8.22 - Acceso internet invitados'
  next

  ! --- Regla final: DENY ALL (debe ser siempre la última) ---
  edit 999
    set name 'CR-SJO-ANY-Deny-DEFAULT'
    set srcintf 'any'
    set dstintf 'any'
    set srcaddr 'all'
    set dstaddr 'all'
    set schedule 'always'
    set service 'ALL'
    set action deny
    set logtraffic all
    set comments 'ISO A.8.20 - Denegar todo lo no permitido'
  next
```

```
end

! === PROCESO DE RECERTIFICACIÓN TRIMESTRAL ===
! 1. Extraer reporte NetBrain: reglas con antigüedad > 365 días
! 2. Verificar uso: config firewall policy → show | grep 'bytes'
! 3. Reglas con 0 bytes en 90 días → candidatas a eliminación
! 4. Documentar resultado en NetBrain y sistema de cambios P&G
! Meta: 0% de reglas con más de 12 meses sin recertificar
```

Nota: Los objetos GUEST-SUBNET, CORP-ALL y NETMGMT-HOSTS deben crearse previamente en 'config firewall address'. El orden de las reglas es crítico: las más específicas deben preceder a las generales, y Deny-DEFAULT debe ser siempre la última.

Fuente: Elaboración propia

5.8.6 Proceso de Recertificación de Reglas con Más de 12 Meses de Antigüedad

El reporte de NetBrain confirma que aproximadamente el 15% de las reglas activas en los FortiGate supera los 12 meses sin recertificación. Se establece el siguiente proceso formal de recertificación, que debe ejecutarse trimestralmente como parte del calendario operativo del equipo de redes y ciberseguridad:

```
PROCESO DE RECERTIFICACIÓN DE REGLAS FIREWALL — CICLO TRIMESTRAL

Paso 1 — Extracción de reporte (Responsable: Equipo de Redes)
  > En NetBrain: Ejecutar reporte 'Firewall Rules Aging Report'
  > Filtro: Reglas con fecha de creación > 365 días
  > Exportar a plantilla NET-FWL-02 (Apéndice C)

Paso 2 — Análisis de uso (Responsable: Equipo de Ciberseguridad)
  > En FortiGate: config firewall policy → show | grep 'bytes'
  > Reglas con 0 bytes en últimos 90 días → candidatas a eliminación
  > Reglas con tráfico → validar que el caso de negocio sigue vigente

Paso 3 — Decisión y acción
  > VIGENTE: Actualizar fecha de recertificación en NetBrain
  > MODIFICAR: Generar ticket de cambio en sistema P&G, aplicar, documentar
  > ELIMINAR: Generar ticket de cambio, aplicar en horario de mantenimiento,
              documentar en NetBrain y registrar en bitácora de seguridad
```

```
Paso 4 — Documentación (Responsable: Equipo de Redes)
  > Actualizar NetBrain con resultado de recertificación por regla
  > Enviar resumen a Líder de Ciberseguridad para aprobación
  > Archivar evidencia en repositorio de auditoría interna P&G

Meta: 0% de reglas con antigüedad > 12 meses sin recertificar al cierre de cada
ciclo
```

Nota: El proceso de recertificación debe integrarse al calendario de mantenimiento trimestral del equipo de Redes y Ciberseguridad. La evidencia de cada ciclo de recertificación debe conservarse por al menos 2 años para fines de auditoría interna y externa bajo ISO/IEC 27001.

Fuente: Elaboración propia

Control ISO que justifica esta propuesta: A.8.20 (Seguridad en redes), A.8.21 (Servicios de red), A.8.15 (Logging), A.8.16 (Monitoreo) — ISO/IEC 27002:2022

Impacto esperado: Elevar el nivel de madurez de 2 (Repetible) a 4 (Gestionado). Nomenclatura uniforme, recertificación trimestral documentada y reducción de superficie de ataque por reglas obsoletas.

5.9 Migración de Access Points y Controladores Inalámbricos (End of Support)

Alerta crítica: Los modelos Cisco Catalyst 9130AXI (177 APs) y Cisco Catalyst 9800-40 (2 WLC) alcanzarán su End of Support oficial en diciembre de 2025, según el portal de ciclos de vida de Cisco. A partir de esa fecha no recibirán actualizaciones de seguridad ni soporte técnico del fabricante.

5.9.1 Situación Actual

La red inalámbrica de P&G Costa Rica está compuesta por 177 Access Points modelo Cisco Catalyst 9130AXI y 2 Wireless LAN Controllers (WLC) modelo Cisco Catalyst 9800-40, todos corriendo IOS-XE 17.15.4d. Estos equipos constituyen la plataforma inalámbrica completa de la sede, administrando los SSIDs corporativo, GUEST e IoT para los 167 colaboradores del departamento de TI y los usuarios invitados.

Según información publicada oficialmente por Cisco en su portal de End-of-Life Policy, ambos modelos — el AP 9130AXI y el WLC 9800-40 — alcanzarán su fecha de End of Support (EoS) en diciembre de 2025. A partir de esa fecha, Cisco no publicará parches de seguridad, actualizaciones de firmware ni brindará soporte técnico para estos modelos, lo que representa un riesgo de seguridad significativo para la infraestructura inalámbrica de la sede.

5.9.2 Brecha Identificada

Operar equipos sin soporte del fabricante genera las siguientes vulnerabilidades de seguridad: ausencia de parches para vulnerabilidades conocidas (CVEs publicados sin corrección disponible), incumplimiento del control A.8.8 de ISO/IEC 27002:2022 (gestión de vulnerabilidades técnicas), y riesgo de pérdida de compatibilidad con versiones futuras de IOS-XE que sí recibirán actualizaciones de seguridad.

5.9.3 Propuesta de Mejora — Migración a Modelos Sucesores

Se propone la migración de la infraestructura inalámbrica a los modelos sucesores oficiales de Cisco, manteniendo la misma marca e infraestructura de gestión que P&G utiliza globalmente, lo que garantiza compatibilidad con los estándares corporativos y facilita el soporte técnico centralizado.

Tabla P7-A

Comparativo de Modelos — Infraestructura Inalámbrica Actual vs. Propuesta

Componente	Modelo Actual	Modelo Propuesto	Mejoras Principales
Access Point	Cisco Catalyst 9130AXI (Wi-Fi 6 — EoS dic. 2025)	**Cisco Catalyst CW9176I (Wi-Fi 6E — Soporte activo)**	Wi-Fi 6E (6 GHz): mayor capacidad y menor interferencia. Mayor densidad de usuarios simultáneos. Compatible con IOS-XE 17.15.4d. Soporte activo del fabricante.
WLC / Controlador	Cisco Catalyst 9800-40 (EoS dic. 2025)	**Cisco Catalyst CW9800M (Soporte activo)**	Controlador de nueva generación para la plataforma Catalyst Center. Mayor rendimiento de procesamiento. Compatible con los APs CW9176I. Soporte activo del fabricante.

Nota: El modelo CW9176I es el sucesor oficial del 9130AXI según el portal de Cisco End-of-Life. El CW9800M es el sucesor oficial del 9800-40. Ambos son compatibles con IOS-XE 17.15.4d, lo que facilita la migración sin cambio de versión de software.

Fuente: Elaboración propia

5.9.4 Justificación de Marca Cisco

P&G opera toda su infraestructura de red — switches, routers, APs y WLC — bajo la marca Cisco a nivel global. Esta estandarización de marca permite: soporte técnico centralizado desde un único proveedor, compatibilidad garantizada entre todos los componentes de la red, gestión unificada mediante Cisco Catalyst Center, y continuidad del contrato de soporte empresarial (Cisco Smart Net) que P&G mantiene a nivel corporativo. Por estas razones, la propuesta de migración se realiza dentro del mismo ecosistema Cisco, reemplazando los modelos sin soporte por sus sucesores directos de la misma familia de productos.

5.9.5 Plan de Migración Propuesto

Dado que el End of Support de los modelos actuales ocurrirá en diciembre de 2025, se propone ejecutar la migración en tres fases para minimizar el impacto operativo:

Fase 1 (Meses 1-2): Adquisición y staging de los equipos CW9176I y CW9800M. Configuración y pruebas en laboratorio. Validación de compatibilidad con la configuración existente de VLANs, SSIDs y políticas de firewall.

Fase 2 (Meses 3-6): Migración por zonas del site, comenzando por las áreas de menor impacto operativo. Operación en paralelo de equipos nuevos y existentes durante la transición para garantizar continuidad del servicio inalámbrico.

Fase 3 (Meses 7-9): Migración completa de los 177 APs y 2 WLC. Descomisión de los equipos 9130AXI y 9800-40. Documentación completa en NetBrain de la nueva infraestructura inalámbrica.

Si la adquisición de los modelos CW9176I y CW9800M no pudiera completarse antes del vencimiento del soporte en diciembre de 2025, se recomienda que cualquier equipo alternativo que se evalúe cumpla con las siguientes características mínimas: soporte Wi-Fi 6 o 6E (802.11ax/be), compatibilidad con WPA3-Enterprise y 802.1X, capacidad de gestión centralizada mediante controlador y segmentación de SSIDs por VLAN.

Control ISO que justifica esta propuesta: A.8.8 (Gestión de vulnerabilidades técnicas), A.8.20 (Seguridad en redes) — ISO/IEC 27002:2022

Impacto esperado: Eliminación del riesgo de operar sin soporte del fabricante. Infraestructura inalámbrica con soporte activo de seguridad y compatibilidad con estándares modernos (Wi-Fi 6E, WPA3).

5.10 Programa Estructurado de Capacitación y Concientización en Seguridad

5.10.1 Situación Actual

El diagnóstico operativo y de percepción evidenció que la Política de Capacitación y Concientización en Seguridad es la única política en estado de No Cumple en el departamento de TI de P&G Costa Rica. Solo el 33% del personal (aproximadamente 55 de 167 colaboradores) recibió capacitación formal en seguridad durante el último año. Las actividades de formación existentes son esporádicas, genéricas y no están estructuradas por rol o área funcional. El 86% del personal entrevistado consideró que la formación actual es insuficiente para las responsabilidades de su puesto.

Esta brecha es crítica porque el factor humano es el vector de ataque más frecuente en incidentes de seguridad de la información: el phishing, la ingeniería social y el manejo inadecuado de credenciales son responsables de la mayoría de las brechas de seguridad en organizaciones empresariales.

5.10.2 Brecha Identificada

La ausencia de un programa estructurado de capacitación implica que aproximadamente 112 de los 167 colaboradores del departamento de TI no reciben formación formal en seguridad, exponiéndolos a riesgos de ingeniería social, phishing, manejo inadecuado de información clasificada y uso incorrecto de las herramientas de seguridad corporativas (CrowdStrike, Zscaler).

5.10.3 Propuesta de Mejora — Programa Anual de Capacitación

Se propone el diseño e implementación de un Programa Anual de Capacitación y Concientización en Seguridad de la Información, estructurado en dos niveles: módulos de concientización general para todos los 167 colaboradores del departamento, y módulos técnicos especializados diferenciados por rol y área funcional.

Módulo 1 — Concientización General (Obligatorio para todos los 167 colaboradores)

Este módulo debe impartirse al menos dos veces al año, en formato de e-learning a través de la plataforma corporativa de P&G, con una duración de 2 horas por sesión y una evaluación de conocimientos al finalizar con nota mínima aprobatoria del 80%.

Tabla P8-A

Contenido del Módulo de Concientización General — Todos los Colaboradores de TI

#	Tema	Contenido	Duración
1	**Phishing e Ingeniería Social**	Cómo identificar correos de phishing, llamadas de vishing y mensajes de smishing. Técnicas de manipulación social más comunes. Qué hacer al recibir un mensaje sospechoso: reportar, no hacer clic, no responder.	30 min
2	**Política de Contraseñas**	Requisitos de contraseñas seguras en P&G: mínimo 16 caracteres, combinación de tipos. Uso obligatorio del gestor de contraseñas corporativo. No compartir credenciales bajo ninguna circunstancia.	20 min
3	**Clasificación y Manejo de Información**	Categorías de clasificación de P&G (Pública, Interna, Confidencial, Restringida). Cómo etiquetar documentos. Procedimientos de manejo, almacenamiento y destrucción por nivel de clasificación.	25 min
4	**Uso Aceptable de Recursos Tecnológicos**	Política de uso aceptable de equipos, internet y correo corporativo. Qué está permitido y qué está prohibido. Consecuencias del uso indebido.	20 min
5	**Herramientas de Seguridad Corporativas**	Para qué sirve CrowdStrike Falcon en el equipo: qué monitorea y cómo reaccionar a sus alertas. Para qué sirve Zscaler: cómo protege el acceso a internet y por qué no debe deshabilitarse.	20 min
6	**Reporte de Incidentes**	Qué es un incidente de seguridad. Cómo y dónde reportarlo: canal de tickets corporativo. Tiempo esperado de respuesta del equipo de Ciberseguridad.	25 min

Nota: El módulo de concientización general debe impartirse al inicio de cada semestre (enero y julio). La plataforma de e-learning corporativa de P&G debe registrar la participación y los resultados de cada colaborador para generar métricas de cobertura.

Fuente: Elaboración propia.

Módulo 2 — Capacitación Técnica por Rol (Diferenciada por equipo)

Adicionalmente al módulo general, cada equipo del departamento debe recibir una capacitación técnica anual específica según las responsabilidades de su rol. Se recomienda

que estas capacitaciones sean impartidas por el equipo de Ciberseguridad de P&G o a través de cursos certificados de fabricantes.

Tabla P8-B

Plan de Capacitación Técnica por Rol y Área Funcional

Equipo	Personas	Temas de Capacitación	Cursos Recomendados
Redes	20	Seguridad en infraestructura de red: VLANs, firewall policies, IDS/IPS. Configuración segura de switches y APs. Gestión de logs de red.	Cisco: Implementing and Administering Cisco Solutions (CCNA). Fortinet: NSE 4 Network Security Professional.
Ciberseguridad	20	Análisis de amenazas avanzadas. Uso avanzado de CrowdStrike Falcon. Respuesta a incidentes (IR) y análisis forense básico.	CrowdStrike: Falcon Responder certification. SANS: SEC504 Incident Handling.
Cloud	15	Seguridad en entornos cloud (AWS/Azure/GCP). Gestión de identidades en la nube. Políticas de acceso y cifrado en servicios cloud.	AWS Security Specialty. Microsoft AZ-500: Azure Security Engineer.
Desarrollo de Software	50	Desarrollo seguro (Secure SDLC). OWASP Top 10. Revisión de código seguro y manejo seguro de credenciales en aplicaciones.	OWASP: curso gratuito en OWASP.org. Cisco: DevNet Security.
Análisis de Datos	25	Manejo seguro de datos sensibles y personales. Cumplimiento de Ley 8968 en el tratamiento de datos. Cifrado de datos en reposo y en tránsito.	ISACA: Certificación en Privacidad de Datos. Coursera: Privacy in the Digital Age.
Soporte Técnico	17	Ingeniería social y phishing avanzado. Seguridad en manejo de credenciales de usuarios. Procedimiento de hardening básico de equipos de usuario final.	Cisco: CyberOps Associate (curso gratuito en Cisco Networking Academy).
SAP	20	Seguridad en sistemas ERP y SAP. Control de accesos y roles en SAP. Manejo seguro de datos financieros y de producción.	SAP: SAP Security and Authorizations. ISACA: CISM (para líderes).

Nota: Los cursos de Cisco Networking Academy (netacad.com) son gratuitos para inscripción individual, lo que permite reducir el costo de implementación del programa. Los cursos de SANS, AWS y Microsoft tienen costo asociado y deben presupuestarse anualmente.

Fuente: Elaboración propia basada en controles A.6.3, A.7.2 de ISO/IEC 27002:2022 y catálogos de formación de Cisco, Fortinet, AWS, Microsoft, SAP e ISACA (2026).

5.10.4 Métricas de Seguimiento del Programa

Para garantizar la efectividad del programa y su mejora continua, se definen las siguientes métricas de seguimiento que deben medirse y reportarse semestralmente por el equipo de Ciberseguridad:

Cobertura: porcentaje de los 167 colaboradores que completaron el módulo general (meta: 100% en cada semestre).

Aprobación: porcentaje de colaboradores que aprobaron la evaluación con nota ≥80% (meta: 90% o superior).

Capacitación técnica: porcentaje de colaboradores que completaron el módulo técnico de su área (meta: 100% anual).

Incidentes por factor humano: número de incidentes de seguridad atribuibles a error humano por trimestre (meta: reducción progresiva).

Simulaciones de phishing: porcentaje de colaboradores que hicieron clic en un correo de phishing simulado (meta: <10% en cada prueba trimestral).

Control ISO que justifica esta propuesta: A.6.3 (Concientización, educación y formación en seguridad), A.7.2 (Responsabilidades de seguridad) — ISO/IEC 27002:2022

Impacto esperado: Elevar el nivel de madurez de 1 (Inicial) a 3 (Definido). Reducción del riesgo humano en todos los equipos del departamento. Cobertura del 100% de los 167 colaboradores en formación anual.

5.11 Formalización del Procedimiento de Gestión de Medios de Almacenamiento

5.11.1 Situación Actual

El diagnóstico identificó que P&G Costa Rica no cuenta con un procedimiento formal documentado para el ciclo de vida completo de los medios de almacenamiento físicos (discos duros, USBs, cintas de backup, equipos dados de baja). Si bien la organización aplica prácticas informales de manejo de medios, estas no están escritas ni formalizadas, no existe un registro de trazabilidad de los medios gestionados y no hay un proceso documentado de destrucción segura al final de la vida útil de los dispositivos.

5.11.2 Brecha Identificada

La ausencia de un procedimiento formal expone a la organización al riesgo de filtración de información sensible a través de medios de almacenamiento mal desechados o extraviados. Dado que el departamento de TI maneja datos financieros, información de clientes, configuraciones de sistemas críticos y datos de producción, este riesgo es especialmente relevante en el contexto de la Ley 8968 de Protección de Datos Personales de Costa Rica.

5.11.3 Propuesta de Mejora — Procedimiento Formal de Gestión de Medios

Se propone la documentación e implementación de un procedimiento formal que cubra el ciclo de vida completo de los medios de almacenamiento, estructurado en las siguientes etapas:

Etapa 1 — Clasificación e Inventario

Responsable: Equipo de Soporte Técnico en coordinación con Ciberseguridad.

Todo medio de almacenamiento debe ser clasificado al momento de su adquisición o registro según el nivel de información que puede contener, utilizando las categorías de la Política de Clasificación de la Información (Pública, Interna, Confidencial, Restringida). Cada medio debe ser registrado en el inventario del departamento con: identificador único, tipo de medio, nivel de clasificación asignado, fecha de registro, responsable asignado y estado actual (en uso, en reserva, en proceso de baja).

Etapa 2 — Manejo Seguro durante el Ciclo de Vida

Responsable: Colaborador asignado al medio.

Los medios clasificados como Confidencial o Restringida solo pueden ser manipulados por personal autorizado, deben almacenarse en espacios físicamente seguros cuando no están en uso, y no pueden ser retirados de las instalaciones sin autorización formal del líder del equipo. El traslado de medios entre instalaciones debe documentarse en el registro de inventario.

Etapa 3 — Proceso de Baja y Destrucción Segura

Responsable: Equipo de Soporte Técnico con supervisión de Ciberseguridad.

Al finalizar la vida útil de un medio, el proceso de baja debe seguir los siguientes pasos según el nivel de clasificación:

Tabla P9-A

Métodos de Destrucción Segura según Nivel de Clasificación

Clasificación	Método de Borrado	Descripción	Evidencia Requerida
Pública / Interna	Borrado lógico estándar	Formateo completo del medio o borrado mediante herramienta estándar del sistema operativo.	Registro en inventario con fecha y responsable.
Confidencial	Borrado seguro certificado (DoD 5220.22-M)	Sobreescritura de 7 pasadas sobre todos los sectores del medio usando herramienta certificada (ej: DBAN, Eraser).	Reporte generado por la herramienta con hash de verificación.
Restringida	Destrucción física	Trituración física del medio mediante empresa certificada de destrucción documental o destrucción in-situ con supervisión de Ciberseguridad.	Certificado de destrucción emitido por la empresa o acta de destrucción in-situ firmada.

Nota: El método DoD 5220.22-M es el estándar del Departamento de Defensa de los EE.UU. para borrado seguro de medios, ampliamente adoptado como referencia de buenas prácticas en gestión de medios en organizaciones corporativas. DBAN (Darik's Boot and Nuke) y Eraser son herramientas gratuitas certificadas para implementar este método.

Fuente: Elaboración propia

Control ISO que justifica esta propuesta: A.8.3 (Gestión de medios de almacenamiento) — ISO/IEC 27002:2022

Impacto esperado: Elevar el nivel de madurez de 2 (Repetible) a 3 (Definido).
Eliminación del riesgo de filtración de información sensible por medios mal desechados.
Cumplimiento de Ley 8968.

5.12 Cronograma de Implementación

El cronograma de implementación se diseñó considerando la complejidad técnica, el impacto operativo y la urgencia de cada propuesta. Las actividades de formalización documental (políticas y procedimientos) pueden ejecutarse en paralelo y en los primeros meses del plan, mientras que la migración de infraestructura inalámbrica requiere un horizonte de 9 meses por su complejidad técnica y el volumen de equipos involucrados (177 APs + 2 WLC). El programa de capacitación se establece como una actividad continua y recurrente durante toda la vida del proyecto.

Plan por fases:
Corto plazo (0–3 meses):

- Política de seguridad
- Gestión de accesos
- Estándar WiFi

Mediano plazo (3–6 meses):

- SGSI completo
- VLAN y firewall
- Capacitación

Largo plazo (6–12 meses):

- Renovación tecnológica
- Auditoría interna
- Mejora continua

Tabla P-CRONO

Cronograma de Implementación — Propuestas de Mejora P&G Costa Rica

Propuesta	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	Prioridad
P1 — Adaptación local Política de Seguridad	●	●	–	–	–	–	–	–	–	–	**Alta**
P2 — Proceso revisión periódica de accesos	●	●	–	–	–	–	–	–	–	–	**Alta**

Propuesta	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	Prioridad
P3 — Clasificación local de información	●	●	–	–	–	–	–	–	–	–	**Alta**
P4 — Estándar red inalámbrica (WiFi/GUEST)	–	●	●	●	–	–	–	–	–	–	**Alta**
P5 — Estándar nomenclatura VLANs (17 switches)	–	●	●	●	–	–	–	–	–	–	**Alta**
P6 — Estándar nomenclatura y recertif. FW FortiGate	–	–	●	●	●	–	–	–	–	–	**Alta**
P7 — Migración APs (9130AXI → CW9176I) + WLC	●	●	●	●	●	●	●	●	●	–	**Crítica**
P8 — Programa capacitación y concientización	–	–	●	●	●	●	●	●	●	●	**Media**
P9 — Procedimiento gestión medios almacenamiento	–	–	–	●	●	–	–	–	–	–	**Media**

Fuente: Elaboración propia

5.13 Comparativo de Nivel de Madurez — Antes y Después

La siguiente tabla presenta el nivel de madurez actual y el nivel proyectado para cada área de control, como resultado de la implementación de las nueve propuestas de este capítulo. La escala utilizada corresponde al Modelo de Madurez de Capacidades (CMM) adaptado al contexto de SGSI, cuya fundamentación teórica se presenta en la sección 4.5 del Capítulo IV.

Tabla P-MADUREZ

Comparativo de Nivel de Madurez por Propuesta — Estado Actual vs. Estado Propuesto

Área de Control / Propuesta	Nivel Actual (0-5)	Nivel Propuesto (0-5)	Controles ISO 27002:2022
P1 — Política de Seguridad (adaptación local)	**2 — Repetible**	**4 — Gestionado**	A.5.1, Cláusula 5.2
P2 — Revisión periódica de accesos	**2 — Repetible**	**4 — Gestionado**	A.5.15, A.5.16, A.5.18
P3 — Clasificación de información (local)	**2 — Repetible**	**4 — Gestionado**	A.5.9, A.5.12, A.5.13
P4 — Estándar red inalámbrica GUEST	**2 — Repetible**	**4 — Gestionado**	A.8.20, A.8.22
P5 — Nomenclatura VLANs	**2 — Repetible**	**4 — Gestionado**	A.8.20, A.8.21
P6 — Nomenclatura y monitoreo FW FortiGate	**2 — Repetible**	**4 — Gestionado**	A.8.20, A.8.21, A.8.15, A.8.16
P7 — Migración infraestructura inalámbrica	**2 — Repetible**	**4 — Gestionado**	A.8.8, A.8.20
P8 — Programa de capacitación	**1 — Inicial**	**3 — Definido**	A.6.3, A.7.2
P9 — Gestión de medios de almacenamiento	**2 — Repetible**	**3 — Definido**	A.8.3

Fuente: Elaboración propia (2026).

La implementación de la propuesta permitirá:

- Reducir riesgos de seguridad
- Cumplir con estándares ISO
- Mejorar la continuidad del negocio
- Aumentar la trazabilidad y control
- Fortalecer la cultura organizacional

5.14 Cierre del Capítulo

En este capítulo se desarrollaron nueve propuestas de mejora directamente derivadas de las brechas identificadas en el diagnóstico integral del Capítulo IV. Las propuestas se organizan en cuatro bloques que siguen la lógica de un SGSI: políticas y procedimientos, infraestructura de red, hardware e infraestructura y capacitación. Cada propuesta fue elaborada desde una perspectiva de consultoría profesional, detallando la situación actual, la brecha específica, la mejora propuesta con sus configuraciones técnicas y explicaciones de comandos, el control ISO que la fundamenta y el impacto esperado en términos de nivel de madurez.

La propuesta de mayor urgencia es la migración de la infraestructura inalámbrica (P7), dado que los 177 APs Cisco 9130AXI y los 2 WLC Catalyst 9800-40 alcanzarán su End of Support en diciembre de 2025, requiriendo acción inmediata para evitar operar equipos sin soporte de seguridad del fabricante. La propuesta de mayor impacto en el factor humano es el programa de capacitación (P8), que busca elevar el nivel de formación en seguridad de un 33% actual a una cobertura del 100% de los 167 colaboradores del departamento. La implementación ordenada de todas las propuestas, siguiendo el cronograma de 10 meses definido, elevará el nivel de madurez de todos los controles evaluados del nivel 2 (Repetible) al nivel 3 o 4 (Definido o Gestionado), fortaleciendo significativamente la postura de seguridad de la información en P&G Costa Rica.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

Conclusiones

A partir del diagnóstico integral realizado en el departamento de Tecnologías de Información de Procter & Gamble, sede Costa Rica, y del desarrollo de las propuestas de mejora fundamentadas en los controles de la norma ISO/IEC 27001:2022 e ISO/IEC 27002:2022, se presentan las siguientes conclusiones:

1. La organización cuenta con una base operativa sólida como punto de partida

El departamento de TI de P&G Costa Rica opera con una infraestructura tecnológica de nivel empresarial que incluye herramientas de seguridad robustas como CrowdStrike Falcon (EDR), Zscaler (Zero Trust), firewalls FortiGate 120G, routers SD-WAN Versa VEP 4600, switches Cisco Catalyst C9300-24UX y la plataforma Infoblox 8.6.3 para gestión centralizada de DNS, DHCP e IPAM. Los procesos de gestión de incidentes, respaldos periódicos y plan de continuidad del negocio (BCP/DRP) cumplen satisfactoriamente con los requisitos de ISO/IEC 27002:2022. Esta condición favorable distingue a la organización de entornos con brechas críticas y constituye una base sólida sobre la cual construir las mejoras propuestas.

2. Las brechas identificadas son principalmente de formalización y documentación, no de capacidad tecnológica

El diagnóstico evidenció que ninguno de los controles evaluados se encuentra en estado de No Cumple por ausencia de tecnología o infraestructura. La única política en estado de No Cumple es la capacitación y concientización, cuya brecha es de gestión organizacional. Los demás controles en Cumple Parcialmente presentan brechas de formalización: la política de seguridad existe globalmente pero no está adaptada localmente, los estándares de red existen en la práctica pero no están documentados, y los accesos se gestionan pero sin revisiones periódicas formales. Esto implica que las mejoras propuestas no requieren inversión en nueva infraestructura tecnológica para la mayoría de los casos, reduciendo significativamente el costo de implementación.

3. La infraestructura inalámbrica representa el hallazgo de mayor urgencia

Los 177 Access Points Cisco Catalyst 9130AXI y los 2 Wireless LAN Controllers Catalyst 9800-40 alcanzarán su End of Support oficial de Cisco en diciembre de 2025. A partir de esa fecha, estos equipos no recibirán actualizaciones de seguridad, parches de vulnerabilidades ni soporte técnico del fabricante, generando un riesgo de seguridad significativo para la infraestructura inalámbrica que da cobertura a los 167 colaboradores del departamento. La propuesta de migración hacia los modelos sucesores Cisco CW9176I y CW9800M es la acción de mayor urgencia del plan de mejora.

4. El diagnóstico de percepción valida y refuerza los hallazgos técnicos

Las entrevistas semiestructuradas realizadas a 14 colaboradores de los siete equipos del departamento convergieron en identificar espontáneamente las mismas tres áreas de mejora detectadas en los diagnósticos operativo y técnico: capacitación en seguridad (79% de los entrevistados la señaló como prioridad), documentación y estandarización de la infraestructura de red, y adaptación local de las políticas corporativas. La convergencia entre la percepción del equipo de Redes sobre la revisión reactiva de reglas de firewall y el dato técnico del 15% de reglas sin recertificar proveniente de NetBrain constituye una validación cruzada desde dos fuentes independientes, reforzando la solidez del diagnóstico.

5. El factor humano es la brecha de mayor exposición al riesgo

Con solo el 33% del personal del departamento de TI habiendo recibido capacitación formal en seguridad durante el último año, aproximadamente 112 de los 167 colaboradores no cuentan con formación estructurada en materia de seguridad de la información. El 86% del personal entrevistado reconoció que la formación actual es insuficiente para las responsabilidades de su rol. Dado que el factor humano es el principal vector de ataque en incidentes de seguridad —a través de phishing, ingeniería social y manejo inadecuado de credenciales— esta brecha representa el mayor riesgo organizacional identificado en el diagnóstico.

6. Los marcos ISO/IEC 27001 e ISO/IEC 27002 resultaron adecuados para estructurar el análisis consultor

La aplicación de los controles del Anexo A de ISO/IEC 27002:2022 como referencia para el diagnóstico y la propuesta de mejora permitió establecer un marco objetivo, medible y alineado con estándares internacionales para evaluar la situación actual de P&G Costa Rica. La escala de madurez CMM (Capability Maturity Model) permitió cuantificar el estado actual de cada control (nivel 1-4) y proyectar el impacto de las mejoras propuestas, facilitando la comunicación de resultados tanto a nivel técnico como directivo. Este enfoque garantiza que las propuestas no son percepciones subjetivas sino hallazgos fundamentados en evidencia técnica y normativa internacional.

7. La propuesta de mejora es viable, de bajo costo y alto impacto

Con excepción de la migración de la infraestructura inalámbrica (que requiere adquisición de hardware), el conjunto de las nueve propuestas desarrolladas puede implementarse con los recursos internos del departamento de TI de P&G Costa Rica, aprovechando las plataformas tecnológicas ya existentes: FortiGate, NetBrain, Zabbix, SD-WAN Versa, WLC, switches Cisco y la plataforma de e-learning corporativa. El esfuerzo estimado de implementación es de 208 a 268 horas-hombre distribuidas en un horizonte de 10 meses, con un costo incremental prácticamente nulo para la organización en el componente documental y de capacitación.

Recomendaciones

Con base en los hallazgos del diagnóstico y las propuestas de mejora desarrolladas en el Capítulo V, se presentan las siguientes recomendaciones dirigidas al departamento de TI de Procter & Gamble, sede Costa Rica:

1. Iniciar de forma inmediata la planificación de la migración de Access Points y WLC

Dado que los modelos Cisco Catalyst 9130AXI (177 APs) y Catalyst 9800-40 (2 WLC) alcanzarán su End of Support en diciembre de 2025, se recomienda iniciar de forma inmediata el proceso de adquisición y planificación de la migración hacia los modelos sucesores Cisco CW9176I y CW9800M. La fase de adquisición y configuración en laboratorio debe completarse en los primeros dos meses del plan para garantizar que la migración pueda ejecutarse antes del vencimiento del soporte del fabricante. Operar equipos sin soporte de seguridad representa un riesgo crítico e incumple el control A.8.8 de gestión de vulnerabilidades técnicas de ISO/IEC 27002:2022.

2. Priorizar la formalización documental de las políticas locales en los primeros dos meses

Se recomienda que en los primeros dos meses del plan de implementación se formalicen las tres políticas documentales de mayor impacto: la adaptación local de la Política de Seguridad de la Información, el procedimiento formal de revisión periódica de accesos y el procedimiento local de clasificación de la información. Estas tres acciones son de bajo costo, pueden ejecutarse en paralelo por los equipos de Ciberseguridad y liderazgo de TI, y establecen el marco normativo local sobre el cual se sustentan todas las demás propuestas técnicas.

3. Implementar el programa de capacitación como actividad continua y no como evento único

Se recomienda establecer el Programa de Capacitación y Concientización en Seguridad como una actividad recurrente y permanente, no como una iniciativa puntual. El módulo de concientización general debe impartirse obligatoriamente dos veces al año (enero y julio) para los 167 colaboradores del departamento, con evaluaciones de conocimiento y métricas de cobertura documentadas. Los módulos técnicos por rol deben realizarse anualmente. Se recomienda también implementar simulaciones de phishing trimestrales para medir la efectividad del programa, con una meta de menos del 10% de colaboradores que hagan clic en correos de prueba.

4. Estandarizar la infraestructura de red antes de ampliarla

Se recomienda que antes de realizar cualquier expansión o modificación significativa de la infraestructura de red, el equipo de Redes implemente los estándares de nomenclatura propuestos para VLANs y reglas de firewall, y documente la topología completa en NetBrain. Estandarizar primero garantiza que cualquier adición futura a la red siga los criterios definidos, previniendo la acumulación de inconsistencias que actualmente dificultan la auditoría. Una vez documentado el estándar, todas las nuevas VLANs, reglas de firewall y SSIDs deben seguir obligatoriamente la convención de nomenclatura establecida.

5. Establecer un proceso trimestral de recertificación de reglas de firewall

Se recomienda incluir en el calendario operativo del equipo de Redes y Ciberseguridad un proceso trimestral de revisión y recertificación de reglas de firewall FortiGate, utilizando el reporte de NetBrain de reglas con antigüedad superior a 12 meses como fuente de entrada. La meta es mantener el 0% de reglas sin recertificar al cierre de cada ciclo trimestral. Este proceso es fundamental para reducir la superficie de ataque generada por el actual ~15% de reglas obsoletas y para cumplir con los controles A.8.15 y A.8.16 de trazabilidad y monitoreo de ISO/IEC 27002:2022.

6. Evaluar la migración de VMware vSphere a una versión con licenciamiento activo

Se recomienda que el equipo de Cloud y el liderazgo de TI evalúen a corto plazo las opciones de renovación o migración del entorno VMware vSphere 7.0, dado que Broadcom (propietario actual de VMware) ha descontinuado las licencias perpetuas y migrado a un modelo de suscripción. La continuidad del soporte del entorno virtualizado que aloja las 22 VMs críticas de la sede depende de regularizar el esquema de licenciamiento. Se recomienda evaluar la migración a vSphere 8.x o alternativas de virtualización que cuenten con soporte activo y sean compatibles con las políticas de estándares tecnológicos corporativos de P&G.

7. Usar NetBrain como plataforma central de documentación y auditoría de la red

Se recomienda establecer NetBrain como la fuente única de verdad (single source of truth) para toda la documentación de la infraestructura de red de la sede Costa Rica. Cada cambio en switches, firewalls, APs o WLC debe quedar registrado en NetBrain dentro de las 24

horas posteriores a su implementación. Asimismo, se recomienda integrar los reportes de NetBrain con el proceso de control de cambios corporativo de P&G, de modo que toda modificación de infraestructura quede vinculada a un ticket de cambio aprobado, mejorando la trazabilidad y el cumplimiento del control A.8.32 de gestión de cambios.

8. Realizar una evaluación del nivel de madurez al cierre del plan de implementación

Se recomienda que al finalizar el plan de implementación de 10 meses, el equipo de Ciberseguridad realice una evaluación formal del nivel de madurez alcanzado en cada uno de los controles ISO/IEC 27002:2022 evaluados en este proyecto, utilizando como referencia la matriz de cumplimiento desarrollada en el Capítulo IV. Esta evaluación permitirá verificar el avance real respecto al nivel proyectado en cada propuesta, identificar controles que no alcanzaron el nivel esperado y definir las acciones correctivas para el siguiente ciclo de mejora continua. El resultado de esta evaluación debe quedar documentado como evidencia formal de auditoría.

Las conclusiones y recomendaciones presentadas en este capítulo reflejan el resultado de un análisis consultor profesional fundamentado en evidencia técnica, documental y cualitativa, recopilada a través de observación directa, revisión de infraestructura, entrevistas semiestructuradas y evaluación contra los controles de la norma ISO/IEC 27002:2022. La implementación ordenada de las nueve propuestas desarrolladas en el Capítulo V, siguiendo el cronograma de 10 meses y las prioridades establecidas, permitirá a Procter & Gamble Costa Rica elevar significativamente su nivel de madurez en la gestión de la seguridad de la información, reducir las brechas identificadas y fortalecer su postura de seguridad de manera sostenible y alineada con los estándares internacionales.

CAPÍTULO VII: APÉNDICES Y ANEXOS

7.1 Apéndices

Los apéndices presentados a continuación corresponden a plantillas y herramientas utilizadas durante el desarrollo del proyecto para la validación de controles de seguridad de red. Dichos documentos fueron empleados como apoyo en la recolección y análisis de la información, permitiendo documentar de forma estructurada los resultados obtenidos durante la evaluación de controles relacionados con accesos inalámbricos y reglas de firewall.

Estas plantillas fueron adaptadas y utilizadas conforme al alcance definido del proyecto, y constituyen evidencia objetiva de la aplicación de las técnicas de investigación y del análisis realizado en el área de seguridad de la información.

Apéndice A

Plantilla de evaluación de controles de acceso para red Guest

Esta plantilla fue utilizada para documentar la validación de los controles asociados al acceso inalámbrico de dispositivos y usuarios externos a la red corporativa. Su aplicación permitió evaluar el cumplimiento del control NET-WRL-01, enfocado en la limitación del acceso desde la red Guest hacia la red interna de Procter & Gamble, mediante la revisión de reglas de firewall que protegen la DMZ Guest.

La herramienta facilitó la verificación de que las configuraciones de seguridad implementadas bloquean accesos no autorizados y cumplen con los criterios establecidos para la protección de la infraestructura interna.

CSA	
Proceso de CSA	ITS Network & Voice
Control	NET-WRL-01
Descripción del Control	El acceso inalámbrico para dispositivos y personas que no pertenecen a P&G es limitado.

Prueba	Revise, desde las herramientas de garantía del cortafuegos (por ejemplo, Netbrain), las reglas del cortafuegos que protegen la DMZ inalámbrica de invitados en cada CNF donde se implementan los controladores de anclaje.	
Criterios de Selección de Muestras	Todos los conjuntos de reglas de firewall destinados a proteger la DMZ inalámbrica de invitados en cada CNF donde se implementan controladores de anclaje.	
Atributos de Prueba	Atributo 1:	Las reglas del cortafuegos no permiten a los usuarios de la red de invitados de P&G acceder a la red de P&G.
Ejemplo de Referencia	De Skybox	Coloque un 1 si está bien
CNF-INT-GW-PGGUEST-WLC	si	1
CNF-INT-GT-PGGUEST-ISE	si	1

Apéndice B

Plantilla de validación de reglas de firewall – Control NET-FWL-01

La presente plantilla fue utilizada para evaluar la efectividad de las reglas de firewall en la identificación y bloqueo de tráfico no autorizado dentro de la red corporativa. Su aplicación

permitió validar el cumplimiento del control NET-FWL-01, mediante la revisión de una muestra representativa de firewalls globales, verificando la correcta filtración del tráfico entre zonas de red.

Esta herramienta permitió documentar de forma estructurada la existencia de reglas de seguridad adecuadas, tales como la ausencia de configuraciones any/any/allow y la presencia de reglas default deny, contribuyendo al análisis de la postura de seguridad de la red.

CSA		
Proceso de CSA	ITS Network & Voice	
Control	NET-FWL-01	
Descripción del Control	El tráfico no autorizado se detecta y elimina de la red de P&G.	
Prueba	Muestra del 10 % de los cortafuegos globales elegidos aleatoriamente en toda la red.	
Criterios de Selección de Muestras	10 % de los cortafuegos elegidos al azar en toda la red.	
Atributos de Prueba	Atributo 1	Los cortafuegos filtran el tráfico, permitiendo el tráfico autorizado y denegando el tráfico no autorizado.
	Atributo 2	Verificación de que los conjuntos de reglas del cortafuegos no permiten ningún tipo de tráfico entre zonas.
	Atributo 3	Verificación de que los conjuntos de reglas del cortafuegos contienen una opción predeterminada de denegación.

Ejemplo de Referencia	Atributo 1	Atributo 2	Atributo 3	Coloque 1 si esta bien
crsjo01fwl001ebp	1	1	1	
crsjo01fwl001cldcons	1	1	1	

Apéndice C

Plantilla de recertificación de reglas de firewall – Control NET-FWL-02

Esta plantilla fue utilizada para documentar la revisión y recertificación de reglas de firewall con antigüedad mayor a doce meses, conforme al proceso de gestión del ciclo de vida de reglas de firewall. Su aplicación permitió validar que las reglas existentes se encuentran autorizadas y alineadas con las necesidades actuales del negocio.

La herramienta facilitó el seguimiento de las acciones realizadas sobre cada regla evaluada, tales como confirmación, actualización o eliminación, aportando evidencia del cumplimiento del control NET-FWL-02 y fortaleciendo la trazabilidad del proceso de gestión de reglas.

CSA		
Proceso de CSA	ITS Network & Voice	
Control	NET-FWL-02	
Descripción del Control	Las reglas del cortafuegos deben estar autorizadas y recertificarse periódicamente en función de las necesidades empresariales actuales.	
Prueba	Analice el 10 % de las reglas de firewall seleccionadas aleatoriamente del informe de Netbrain de todas las reglas de firewall con más de 12 meses de antigüedad extraídas para su certificación	
Criterios de Selección de Muestras	Informe Netbrain de todas las reglas de firewall con más de 12 meses de antigüedad extraídas para su certificación: 10 %.	
Atributos de Prueba	Atributo 1	La regla tiene 12 meses o más.
Ejemplo de muestra	Coloque 1 si esta bien	
LC-CRTNJ0101-UT-ENERGY2PCTU	1	
LC-2798-UT-ENERGY2LPUT	1	

Apéndice D

Guía de Entrevista Semiestructurada – Diagnóstico de Seguridad de la Información

La presente guía fue utilizada como instrumento de recoleción de datos primarios para las 14 entrevistas semiestructuradas realizadas al personal del departamento de TI de P&G Costa

Rica. Su aplicación, descrita en la sección 3.3 del marco metodológico, permitió obtener la información que sustenta el diagnóstico de percepción presentado en la sección 4.4 del Capítulo IV.

CSA		
Proceso de CSA	ITS Network & Voice / People & Organization	
Instrumento	Guía de entrevista semiestructurada	
Población	14 colaboradores del departamento de TI: Redes, Ciberseguridad, Cloud, Análisis de Datos, Soporte, SAP y Desarrollo de Software.	
Propósito	Recopilar información sobre el estado actual de la seguridad de la información, nivel de conocimiento de políticas, brechas percibidas y cumplimiento con ISO/IEC 27001 e ISO/IEC 27002.	
Atributos de Prueba	Área temática	Pregunta
1	Políticas	¿Conoce usted la política de seguridad de la información de P&G? ¿Puede describir cómo aplica en su trabajo diario?
2	Políticas	¿Existe algún procedimiento local documentado que complemente la política corporativa global para la sede Costa Rica?
3	Capacitación	¿Ha recibido capacitación formal en seguridad de la información en el último año? ¿Sobre qué temas?
4	Capacitación	¿Considera que el programa de formación actual es suficiente para las responsabilidades de su rol?
5	Accesos	¿Cómo se gestionan las solicitudes de acceso a sistemas o recursos críticos? ¿Existe un proceso de revisión periódica de accesos asignados?
6	Red	¿Existe un estándar documentado para la nomenclatura de VLANs y reglas de firewall en la infraestructura de red?

7	Red	¿Con qué frecuencia se revisan las reglas de firewall FortiGate para verificar su vigencia y necesidad operativa?
8	Incidentes	¿Cómo se gestiona actualmente un incidente de seguridad? ¿Existe un procedimiento formal documentado?
9	General	¿Qué aspectos de la seguridad de la información considera que requieren mayor atención o mejora en el departamento de TI?

Apéndice E

Estándar de Nomenclatura y Asignación de VLANs – Infraestructura P&G Costa Rica

La presente plantilla documenta el estándar corporativo de asignación de IDs de VLAN definido por P&G a nivel global. Este estándar existía a nivel corporativo pero no se encontraba registrado formalmente en NetBrain para la sede Costa Rica al momento del

diagnóstico, lo cual fue identificado como brecha en el control A.8.20/A.8.21 de ISO/IEC 27002:2022. Su documentación forma parte de la Propuesta 3 del Capítulo V.

CSA		
Proceso de CSA	ITS Network & Voice	
Control	NET-VLAN-STD-01 (Prop. 3 – ISO A.8.20/A.8.21)	
Descripción	Estándar corporativo P&G de asignación de IDs de VLAN según función, a documentar en NetBrain para los 17 switches de la sede Costa Rica.	
Atributos	ID / Rango	Función / Nombre
Estándar P&G	1	DO NOT USE
	7	Satellite (PGTV)
	10–29	User VLANs
	50–58	Security or Access Control Systems
	59	Security Cameras
	60–69	Reserved for TelePresence (VCS and VCR) Use
	61	Plug-in-video devices
	62	VCR devices
	64	TelePresence
	68	Wireless Sharing
	69	Production Only DVR devices
	99	Printer VLAN
	100–199	Reserved for WLAN
	101	AP Network Management VLAN (/23 max) – Primary
	102	WLC Network Management VLAN (/28) – Primary
	103	AP Network Management VLAN (/23 max) – Secondary
	104	WLC 5520 CIMC interface

	105	AP Network Management VLAN (/23 max) – Tertiary
	106	WLC Network Management VLAN (/28) – Secondary
	800–819	IPT Voice
Brecha identificada	El estándar de asignación de IDs existía a nivel corporativo global pero no estaba documentado en NetBrain para la sede Costa Rica, generando inconsistencias en la configuración de los 17 switches al momento del diagnóstico.	
Herramienta de documentación	NetBrain (registro de topología y configuración de switches)	

Apéndice F

Plantilla de Solicitud y Registro de Reglas de Firewall FortiGate – Control NET-FWL-STD-01

Esta plantilla fue diseñada como herramienta de implementación para la Propuesta 4 del Capítulo V, que establece el estándar de nomenclatura y monitoreo de reglas de firewall en los equipos FortiGate. Su uso formaliza el ciclo de vida de cada regla: creación, aprobación, documentación en NetBrain y recertificación periódica, cerrando la brecha identificada en el control A.8.20/A.8.21 de ISO/IEC 27002:2022.

CSA		
Proceso de CSA	ITS Network & Voice	
Control	NET-FWL-STD-01 (Prop. 4 – ISO A.8.20/A.8.21)	
Descripción del Control	Las reglas de firewall FortiGate deben seguir una convención de nombre estándar, contar con justificación de negocio documentada y recertificarse periódicamente (máximo cada 12 meses).	
Convención de nombre	Codigo pais-Codigo Ciudad-Protocolo-Servicio-Proposito – Ejemplo: CR-SJO-HTTPS-Allow-BROWSING	
Atributos de Prueba	Campo	Descripción
Solicitud	Nombre de la regla	Conforme a convención Codigo pais-Codigo Ciudad-Protocolo-Servicio-Proposito
	Zona origen / destino	Zonas definidas en FortiGate
	Servicio / Puerto	Puerto TCP/UDP o grupo de servicios FortiGate
	Acción	ALLOW / DENY
	Justificación de negocio	Descripción del caso de uso que requiere la regla
	Solicitante / Aprobador	Equipo solicitante / Líder Ciberseguridad o Redes
Recertificación	Fecha de creación	DD/MM/AAAA
	Fecha de revisión programada	DD/MM/AAAA (máximo 12 meses desde creación)
	Estado en última recertificación	Vigente / Modificada / Eliminada

	Documentado en NetBrain	Sí / No
Ejemplo de Referencia	De NetBrain	Coloque un 1 si está bien
	CR-SJO-HTTPS-Allow-BROWSING	1
	CR-SJO-SQL-Deny-Database	1

5	Accesos	¿Cómo se gestionan las solicitudes de acceso a sistemas o recursos críticos? ¿Existe un proceso de revisión periódica de accesos asignados?
6	Red	¿Existe un estándar documentado para la nomenclatura de VLANs y reglas de firewall en la infraestructura de red?
7	Red	¿Con qué frecuencia se revisan las reglas de firewall FortiGate para verificar su vigencia y necesidad operativa?
8	Incidentes	¿Cómo se gestiona actualmente un incidente de seguridad? ¿Existe un procedimiento formal documentado?
9	General	¿Qué aspectos de la seguridad de la información considera que requieren mayor atención o mejora en el departamento de TI?

Apéndice G

Evaluación Diagnóstica de Conocimiento en Seguridad de la Información – Programa de Capacitación P5

Este instrumento fue diseñado como herramienta de implementación para la Propuesta 5 del Capítulo V. Su aplicación al inicio del programa permite medir el nivel de conocimiento previo de los 167 colaboradores del departamento de TI y segmentar los módulos de formación por rol y área, conforme al control A.7.2 de ISO/IEC 27002:2022.

CSA		
Proceso de CSA	People & Organization / ITS Security	
Control	SEC-TRN-01 (Prop. 5 – ISO A.7.2)	
Descripción del Control	El personal debe recibir capacitación y concientización adecuada en seguridad de la información, con evaluación de conocimientos al inicio del programa para segmentar los módulos según el nivel de cada colaborador.	
Instrucciones	Seleccione la opción correcta. Duración estimada: 15 minutos. Los resultados son confidenciales y se usarán únicamente para definir el nivel del módulo asignado.	
Atributos de Prueba	#	Pregunta y opciones
Políticas y clasificación	1	¿Qué significa clasificar información como “Confidencial”? a) No tiene ningún valor b) Solo personas autorizadas pueden acceder c) Puede compartirse libremente
Amenazas	2	¿Qué debe hacer si recibe un correo sospechoso con enlace desconocido? a) Hacer clic para verificar b) Reportarlo al equipo de Ciberseguridad c) Reenviarlo a compañeros
Accesos	3	¿Cuál describe mejor el principio de “mínimo privilegio”? a) Dar acceso a todos los sistemas por defecto b) Otorgar solo los accesos necesarios

		para la función del usuario c) Bloquear todo el tráfico de red
Herramientas	4	¿Qué es CrowdStrike Falcon? a) Un sistema de respaldo b) Una plataforma de protección de endpoints c) Una herramienta de documentación de red
Incidentes	5	¿Cuál es el procedimiento correcto ante un incidente de seguridad? a) Resolverlo directamente sin reportar b) Reportarlo mediante el canal de gestión de incidentes establecido c) Esperar a ver si se resuelve solo
Contraseñas	6	¿Cuál es una práctica segura de contraseñas? a) Compartir la contraseña con un compañero de confianza b) Usar la misma contraseña en todos los sistemas c) Usar contraseñas únicas y activar autenticación de dos factores
Escala de resultados	0–2 correctas: Módulo básico obligatorio • 3–4: Módulo intermedio • 5–6: Módulo avanzado	

Bibliografía

Laudon, K. C., & Laudon, J. P. (2016). Sistemas de información gerencial (14ª ed.). Pearson Educación.

https://archive.org/details/laudon-sistemas-de-informacion-gerencial-14-edicion/page/xiv/mode/2up

Mintzberg, H. (1987). The Strategy Concept I: Five Ps for Strategy. California Management Review, 30(1), 11-24. https://journals.sagepub.com/doi/10.2307/41165263

Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th ed.). Pearson Education.

https://www.cs.csubak.edu/~jyang/Computer-Networks---A-Tanenbaum---5th-edition.pdf

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology, Special Publication 800-30.

https://csrc.nist.gov/pubs/sp/800/30/final

Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice (4th ed.). Pearson Education.

https://unidel.edu.ng/focelibrary/books/Computer%20Security%20_%20Principles%20-%20WILLIAM%20STALLINGS_2089.pdf

Tipton, H. F., & Krause, M. (2020). Information Security Management Handbook (7th ed.). CRC Press.

https://engineering.futureuniversity.com/BOOKS%20FOR%20IT/Book%20Information%20Security%20Mangement%206th%20ed.pdf

Easttom, C. (2021). Computer Security Fundamentals (4th ed.). Pearson IT Certification.

https://repository.gctu.edu.gh/files/original/b43a80b26d40bfba7457ed65506df82a.PDF

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). Metodología de la investigación (6.ª ed.). McGraw-Hill Education.

https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102.

https://www.scirp.org/reference/referencespapers?referenceid=2904943

Researchgate (2020).

https://www.researchgate.net/figure/nformation-security-risk-management-process_fig2_261310411

Engebretson, P. (2013). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (2nd ed.). Syngress Publishing.

https://wqreytuk.github.io/Patrick+Engebretson+The+Basics+of+Hacking+and+Penetration+Testing,+Second+Edition+%282013%29.pdf

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.

https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf

Posey (2016). Why Backup Policies as Code Is Becoming a Cloud Essential

https://virtualizationreview.com/articles/2025/11/13/why-backup-policies-as-code-is-becoming-a-cloud-essential.aspx?utm_source=chatgpt.com