Escuela Superior Politécnica del Litoral

Facultad de Ingeniería en Electricidad y Computación

Diseño de políticas de seguridad para la protección de la información de una empresa de desarrollo de software, basadas en las normativas internacionales ISO 27001 e ISO 22301

Proyecto de Titulación:

Previo a la obtención del Título de:

Magíster en Seguridad Informática

Presentado por:

Milton Fabrizio García Cox

Andrea Fernanda Vivanco Rodriguez

Guayaquil - Ecuador

Año: 2025

AGRADECIMIENTO

A Dios, mi familia y amigos, quienes han sido mi principal apoyo, brindándome siempre palabras oportunas para continuar con mi profesionalización.

A mi querida Universidad ESPOL, a mis profesores y compañeros pilares fundamentales en la búsqueda del éxito profesional que siempre he anhelado.

A mi futuro esposo, Joe Junco, quien ha estado a mi lado durante 11 años brindándome su apoyo incondicional y recordándome siempre que todo lo que sueño es posible.

Lic. Andrea Fernanda Vivanco Rodriguez

Quiero agradecer a mis increíbles padres, Milton y Janet, por su soporte inagotable y su guía. A mi hermano incondicional, Geovanny, por su apoyo.

A mi maravillosa Carolina, por su cariño y aliento en cada paso.

Y a mis traviesas Meshi, Moli, Pepa, Fiona, Tom, Luna y Krisol, por llenar mis días de alegría.

Ing. Milton Fabrizio García Cox

DEDICATORIA

En primer lugar, a Dios que nunca me abandona y me ha dado la fortaleza necesaria para seguir adelante incluso en los momentos más adversos.

A mi mamá y mis hermanos, por su amor y apoyo constante, que han sido fundamentales para mantenerme firme en cada meta que me propongo.

Y, sobre todo, en memoria de mi padre, José Luis Vivanco Gómez, por haberme dejado la difícil misión de llevar la batuta a mis hermanos. Espero estar cumpliendo con la labor que me encomendaste.

Lic. Andrea Fernanda Vivanco Rodriguez

Dedicado a Milton, Janet, Geovanny y a mi amada Carolina. A mi Meshi, Moli, Pepa, Fiona, Tom, Luna y Krisol.

Y a Barcelona SC, que un día alcanzará la gloria eterna y la cúspide del fútbol mundial.

Ing. Milton Fabrizio García Cox

EVALUADORES

Firmado electrónicamente por:
LENIN EDUARDO FREIRE COBO
Validar únicamente con FirmaEC

Lenin Eduardo Freire Cobo

Tutor de proyecto

Firmado electrónicamente por:
JUAN CARLOS GARCIA PLUA
Validar únicamente con FirmaEC

Juan Carlos García Plúa

Revisor de proyecto

DECLARACIÓN EXPRESA

Nosotros Andrea Fernanda Vivanco Rodríguez y Milton Fabrizio García Cox acordamos y reconocemos que:

La titularidad de los derechos patrimoniales de autor (derechos de autor) del proyecto de graduación corresponderá al autor o autores, sin perjuicio de lo cual la ESPOL recibe en este acto una licencia gratuita de plazo indefinido para el uso no comercial y comercial de la obra con facultad de sublicenciar, incluyendo la autorización para su divulgación, así como para la creación y uso de obras derivadas. En el caso de usos comerciales se respetará el porcentaje de participación en beneficios que corresponda a favor del autor o autores.

La titularidad total y exclusiva sobre los derechos patrimoniales de patente de invención, modelo de utilidad, diseño industrial, secreto industrial, software o información no divulgada que corresponda o pueda corresponder respecto de cualquier investigación, desarrollo tecnológico o invención realizada por nosotros durante el desarrollo del proyecto de graduación, pertenecerán de forma total, exclusiva e indivisible a la ESPOL, sin perjuicio del porcentaje que nos corresponda de los beneficios económicos que la ESPOL reciba por la explotación de nuestra innovación, de ser el caso.

En los casos donde la Oficina de Transferencia de Resultados de Investigación (OTRI) de la ESPOL comunique a los autores que existe una innovación potencialmente patentable sobre los resultados del proyecto de graduación, no se realizará publicación o divulgación alguna, sin la autorización expresa y previa de la ESPOL.

Guayaquil, 21 de Agosto del 2025

Firmado electrónicamente por:
MILTON FABRIZIO GARCIA COX
Validar únicamente con FirmaEC

Milton Fabrizio García Cox

ANDREA FERNANDA VIVANCO RODRIGUEZ

Firmado digitalmente por ANDREA FERNANDA VIVANCO RODRIGUEZ
Fecha: 2025.08.21 22:26:59 -05'00'

Andrea Fernanda Vivanco Rodriguez

RESUMEN

El presente trabajo de titulación se enfoca en la evaluación y fortalecimiento de la seguridad informática en entornos empresariales, con el objetivo de mitigar riesgos y vulnerabilidades en infraestructuras críticas, asegurando la protección de la información y la continuidad del negocio. A diferencia de enfoques generales de ciberseguridad, este estudio se centra en la aplicación de metodologías de evaluación de riesgos adaptadas a empresas de desarrollo de software, considerando sus necesidades específicas y el cumplimiento de normativas internacionales.

El estudio propone un modelo de gestión de riesgos basado en el análisis de seguridad en infraestructura tecnológica y recursos humanos. La investigación documental y el levantamiento de información a través del talento humano permiten identificar brechas de seguridad y evaluar el impacto de posibles incidentes. Además, la aplicación de las normativas ISO 27001 e ISO 22301 facilita la definición de estrategias efectivas para la gestión y tratamiento de estos incidentes. Este enfoque facilita la detección de vulnerabilidades y la implementación de estrategias de mitigación efectivas.

Uno de los aspectos clave de este proyecto es el desarrollo de un marco de trabajo integrado por políticas que combinan buenas prácticas en

ciberseguridad con la automatización de procesos de monitoreo y respuesta ante amenazas. Este modelo optimiza la detección temprana de riesgos y fortalece la resiliencia operativa de las organizaciones frente a posibles ataques.

Como resultado, el estudio presenta una serie de recomendaciones y un esquema de seguridad adaptable a distintas empresas del sector tecnológico. La implementación de estas medidas no solo mejora la postura de seguridad de las organizaciones, sino que también contribuye a una mayor continuidad operativa y protección de activos digitales.

ÍNDICE GENERAL

ABREVIATURA Y SIMBOLOGIA

BCM Business Continuity Management (Gestión de la Continuidad del Negocio)

BCP Business Continuity Plan (Plan de Continuidad del Negocio)

BIA Business Impact Analysis (Análisis de Impacto en el Negocio)

CD Continuous Deployment (Despliegue Continuo)

CI Continuous Integration (Integración Continua)

DRP Disaster Recovery Plan (Plan de Recuperación ante Desastres)

HTTPS HyperText Transfer Protocol Secure (Protocolo Seguro de Transferencia de Hipertexto)

IAM Identity and Access Management (Gestión de Identidad y Accesos)

IPS Intrusion Prevention System (Sistema de Prevención de Intrusiones)

MTPD Maximum Tolerable Period of Disruption (Periodo Máximo Tolerable de Interrupción)

NVD National Vulnerability Database (Base de Datos Nacional de Vulnerabilidades)

OSINT Open Source Intelligence (Inteligencia de Código Abierto)

OWASP Open Web Application Security Project (Proyecto de Seguridad en Aplicaciones Web de Código Abierto)

PHVA Plan-Do-Check-Act (Planear-Hacer-Verificar-Actuar)

RPO Recovery Point Objective (Objetivo de Punto de Recuperación)

RTO Recovery Time Objective (Objetivo de Tiempo de Recuperación)

SGSI Information Security Management System (Sistema de Gestión de Seguridad de la Información)

TLS Transport Layer Security (Seguridad de la Capa de Transporte)

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La seguridad informática es uno de los pilares fundamentales para las empresas de desarrollo de software, donde la protección de la información y la continuidad operativa son esenciales para garantizar la confianza de sus clientes y el cumplimiento normativo. Con el crecimiento de las amenazas cibernéticas y el aumento de ataques dirigidos a infraestructuras tecnológicas, las organizaciones enfrentan el reto de fortalecer sus estrategias de seguridad para mitigar riesgos y evitar impactos negativos en sus operaciones. La falta de medidas adecuadas puede traducirse en pérdidas económicas significativas, sanciones legales o un deterioro de la reputación corporativa, factores que comprometen la sostenibilidad del negocio.

En este contexto, la gestión de riesgos de seguridad informática se convierte en un proceso clave para identificar vulnerabilidades y definir estrategias de mitigación efectivas. La aplicación de metodologías de evaluación de riesgos permite analizar tanto la infraestructura tecnológica como el factor humano, elementos críticos en la protección de activos. Alinearse con normativas internacionales como ISO 27001 y 22301 proporciona un marco estructurado para gestionar incidentes y mejorar la resiliencia organizacional, evitando así interrupciones prolongadas que pueden generar altos costos y pérdida de confianza por parte de los usuarios y socios estratégicos.

Las empresas de desarrollo de software, debido a la naturaleza de sus procesos y la constante innovación tecnológica, requieren modelos de seguridad adaptables y dinámicos. Desde la detección de brechas de seguridad hasta la implementación de políticas efectivas, es imprescindible contar con un enfoque integral que combine buenas prácticas con la automatización de procesos de monitoreo y respuesta ante amenazas. La adopción de este enfoque no solo reduce la superficie de exposición a ataques, sino que también contribuye a minimizar las consecuencias financieras derivadas de incidentes graves, como fugas de información o interrupciones del servicio.

Se propone un modelo de políticas que han sido basadas en metodologías de análisis de seguridad, valoración y tratamiento de riesgos y vulnerabilidades mediante normativas internacionales. A través de este enfoque, se busca optimizar la detección temprana de riesgos, fortalecer la postura de seguridad y garantizar la continuidad del negocio en un entorno de amenazas en constante evolución.

En las siguientes secciones, se detallarán los aspectos metodológicos junto con las estrategias propuestas para mejorar la seguridad informática en empresas dedicadas a la creación de software.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedentes

Una empresa con más de 9 años de antigüedad dedicada al desarrollo de software de aplicaciones móviles y web, ubicada en la ciudad de Guayaquil cuenta con alrededor de 15 colaboradores. Esta organización forma parte de un grupo empresarial más amplio y no solo brinda soporte a las demás empresas del grupo, sino que a su vez extiende sus servicios a otras organizaciones en el país.

La creciente complejidad de las amenazas cibernéticas que actualmente enfrentan las organizaciones impacta de manera inherente al análisis costo-beneficio de las estrategias de sostenibilidad y reputación [1]. Sin un plan robusto para el análisis de riesgos, la seguridad de la información en las actividades de desarrollo de software se ven comprometidas,

exponiendo a la empresa a ciberataques y vulnerabilidades críticas en la nube entre las que se encuentran: accesos no autorizados a máquinas virtuales e imágenes ISO, ataques DDoS e interrupciones de servicios [2]. Un análisis de riesgo y propuesta de políticas de seguridad permitirán identificar y evaluar sistemáticamente las amenazas del entorno y las vulnerabilidades descritas, proporcionando una base sólida para la toma de decisiones informadas [3].

Ante lo mencionado, se busca contribuir al diseño de políticas de seguridad fundamentadas en estándares y normas internacionales, que permitan evaluar y mitigar riesgos potenciales, fomentando un entorno de confianza y resiliencia. Al implementar estas medidas, se aspira a minimizar los impactos negativos asociados con posibles brechas de seguridad, fortaleciendo así la protección de la organización.

La solución planteada ofrecerá directrices claras para evaluar y mitigar riesgos y vulnerabilidades en sus operaciones, adoptando políticas que se alineen a estándares globales, mejorando la capacidad de la empresa para enfrentar amenazas cibernéticas, protegiendo su infraestructura tecnológica. Por otro lado, es especialmente útil para pequeñas y medianas empresas de soluciones tecnológicas u organizaciones que integran servicios de la nube en sus operaciones, facilitando que sus esfuerzos se centren en ofrecer soluciones innovadoras y de calidad, manteniéndose

competitivas y seguras. Autores como Braz y Bacchelli que han analizado las perspectivas de desarrolladores de software [4] y Annunziata, Lambiaze, Palomba y Ferrucci que abordan el análisis de riesgos con respecto al manejo de proyectos y grupos [5] describen lo crucial que es tomar en cuenta todos los roles y actores que intervienen en el proceso de diseño, implementación y soporte de aplicaciones de software, incluyendo servicios relacionados en la nube. Específicamente, esto permitirá la mitigación de los riesgos asociados a la infraestructura de la organización, reduciendo pérdidas económicas y mejorando la reputación corporativa, mientras se fomenta un entorno de confianza y resiliencia de manera interna.

1.2 Descripción del problema

La institución presentada enfrenta graves desafíos en la seguridad de sus actividades de desarrollo, despliegue y soporte, ya que no cuentan con un adecuado plan integral de protección de la información. Se han generado una variedad de incidentes que han comprometido la integridad y confidencialidad, tales como: accesos no autorizados a sistemas críticos, segmentación insuficiente de permisos relacionados con el perfil del colaborador y ausencia de políticas efectivas que han dado como resultado la propagación de Malware al departamento de desarrollo. Además, existe una deficiencia en el procedimiento de desvinculación de colaboradores, así como la inadecuada utilización de licencias de software y equipos de

cómputo para fines distintos a los laborales que pueden implicar infracciones legales y de seguridad.

Dados los antecedentes mencionados junto con la sofisticación de ciberataques, obsolescencia de sistemas, rápida adopción de tecnologías disruptivas sin una correcta dirección en los lineamientos de seguridad de la información, muchas personas de la organización se ven afectados. Algunas de estas personas son: directivos, gerentes, colaboradores, proveedores y clientes, quienes experimentan las consecuencias de esta obsolescencia que impacta en la continuidad del negocio, provocando pérdidas económicas, daño a la reputación y un aumento en la probabilidad de ocurrencia de incidentes de seguridad.

1.3 Solución propuesta

La solución propuesta consiste en el diseño de políticas de seguridad alineadas con las normativas internacionales ISO 27001 e ISO 22301, que establecen metodologías para la gestión de la seguridad de la información y la continuidad del negocio. La ISO 27001 proporciona un sistema de gestión para identificar, evaluar y mitigar riesgos relacionados con la infraestructura tecnológica, mientras que la ISO 22301 se enfoca en la planificación y gestión de la continuidad operativa en caso de contingencias. Estas normas son especialmente relevantes dado el entorno actual, donde las amenazas cibernéticas son cada vez más sofisticadas y las

organizaciones deben estar preparadas para enfrentarlas de manera efectiva [6].

Se diseñarán políticas específicas para la gestión de acceso, protección de datos y continuidad del negocio, alineadas con los estándares internacionales. Estas políticas establecerán controles rigurosos de acceso a sistemas críticos, protocolos claros para el manejo de información sensible y planes de recuperación ante desastres, garantizando la protección de los activos más valiosos de la organización. El análisis de riesgos y vulnerabilidades en conjunto con las políticas permitirán brindar a la alta dirección una base sólida para la toma de decisiones informadas.

En el desarrollo del presente proyecto, uno de los autores de este documento forma parte de la organización en cuestión, y se ha evaluado que es factible diseñar políticas de seguridad tecnológicas, con recursos económicos limitados y tomando en cuenta un tiempo límite de 3 a 4 meses. La clave radica en emplear herramientas de software de código abierto, así como metodologías y normativas internacionales como la ISO 22301 y la ISO 27001. Estas metodologías ofrecen recomendaciones y guías relevantes para el monitoreo, la implementación de controles de seguridad y el proceso de mejora continua dentro de la organización [7]. Esto facilitará optimizar los recursos disponibles y asegurar medidas eficientes.

Además, se cuenta con la colaboración de los distintos sectores de la organización y el compromiso de la alta dirección, lo que garantizará que las medidas adoptadas sean sostenibles a largo plazo, priorizando procesos claves del departamento TI. Esto permitirá avanzar de manera efectiva en la implementación en la propuesta. Por último, la combinación de estos factores técnicos, junto con la disponibilidad de tiempo y recursos, respalda la viabilidad del proyecto, asegurando su éxito en el entorno actual.

La principal ventaja de esta solución es la reducción significativa de los riesgos cibernéticos y la mejora en la capacidad de respuesta ante amenazas. Al adoptar las normativas ISO 27001 e ISO 22301, la empresa no solo fortalecerá su infraestructura tecnológica, sino que también asegurará la continuidad de sus operaciones frente a incidentes críticos, minimizando los impactos financieros y reputacionales [8]. Esta alternativa facilitará de forma holística, el cumplimiento de requisitos legales y regulatorios, lo que es especialmente relevante para organizaciones que manejan datos sensibles. Además, el diseño de políticas de seguridad propuesto se alinea no solo con los estándares internacionales ISO 27001 e ISO 22301, sino también con la Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador. Ya que se busca fortalecer la necesidad de implementar medidas técnicas y organizativas adecuadas para garantizar la seguridad, confidencialidad y tratamiento lícito de los datos personales, especialmente en entornos donde se manejan datos sensibles.

1.4 Objetivo general

Diseñar políticas que aseguren las buenas prácticas de protección de la información y continuidad del negocio, basados en normas internacionales, para evaluar los riesgos y vulnerabilidades de las actividades realizadas por una empresa de desarrollo de software.

1.5 Objetivos específicos

- Identificar el entorno de la empresa y las actividades críticas que requieren protección.
- Evaluar los riesgos y vulnerabilidades asociados a la infraestructura de los activos de la organización.
- Proponer un diseño de políticas de seguridad que incluyan procedimientos para la gestión de acceso, uso, almacenamiento de datos y continuidad del negocio, fundamentados en las normativas ISO 27001 e ISO 22301.

1.6 Metodología

El presente trabajo será de carácter descriptivo. Para ello, se llevó a cabo un levantamiento de información que incluyo entrevistas, revisiones documentales, análisis de procesos, incidentes previos ocurridos en la organización, activos y recursos en la nube. A su vez, se efectuó un análisis cualitativo que se complementó con una perspectiva comparativa respecto

a las normativas internacionales ISO 27001 e ISO 22301. En este enfoque se seleccionó y adapto los estándares y controles más relevantes a las necesidades específicas de la organización. La recopilación de datos se basó en entrevistas estructuradas dirigidas a dos líderes del equipo de tecnología y el Gerente General. Para ello, se empleó una lista de preguntas con una variedad de interrogantes, tales como: abiertas, cerradas y que empleen una escala de Likert para medir la perspectiva actual de la compañía. Asimismo, se aplicó un análisis de registros de los planes y políticas de seguridad existentes, referentes al uso de hardware y software, la protección de credenciales y el resguardo de la infraestructura de los servicios utilizados en la nube. Además, se buscó conocer acerca de los planes de contingencia y de respuesta ante incidentes.

El diseño de investigación propuesto será no experimental transversal, ya que se desarrollará una evaluación integral de la situación actual de la seguridad de la información y planes de continuidad del negocio en la empresa de software, es decir durante un único momento en el tiempo. Las actividades incluyeron la elaboración de políticas que regulen la gestión de accesos, el uso y almacenamiento de datos. Además, se definieron procedimientos claros para la desvinculación de colaboradores, la correcta utilización de recursos de hardware y software, y se establecieron directrices de seguridad en las actividades de diseño, implementación y soporte de aplicaciones.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Seguridad de la información

Actualmente, el ecosistema digital evoluciona constantemente y exige una implementación continua para mantenerse al día con las tecnologías de rápido desarrollo, que están redefiniendo la seguridad informática [9]. En otras palabras, la seguridad informática es un elemento esencial cuyo objetivo es proteger tanto los datos como la infraestructura tecnológica, garantizando que la información confidencial y operativa, esté protegida contra accesos no autorizados, pérdidas, alteraciones y ataques maliciosos. Definir directrices holísticas y eficaces no solo resguarda los recursos digitales, sino también potencia la resiliencia organizacional, mejora la reputación y fomenta un ambiente de confianza de todos los involucrados de la organización [10]

2.1.1 Normativa ISO 27001: Gestión de la seguridad de la información

La norma ISO 27001 establece un marco global para la gestión de la seguridad de la información, permitiendo a las organizaciones identificar, evaluar y mitigar riesgos relacionados con sus activos informáticos de acuerdo con la *Figura 1.2*. En el contexto de los servicios gubernamentales, la implementación de esta norma es esencial para garantizar la seguridad de la información personal y las transacciones electrónicas, como se evidencia en los proyectos de servicios móviles en los gobiernos locales de latinoamérica, los cuales deben cumplir con estándares internacionales de protección de datos y seguridad [8].

Además, la integración de técnicas de inteligencia de fuentes abiertas (OSINT) con ISO 27001 permite mejorar la evaluación de riesgos y la gestión de la seguridad de la información [6]. Esta combinación optimiza el análisis de vulnerabilidades, especialmente en áreas críticas como la gestión de recursos humanos y las relaciones con proveedores, asegurando una respuesta efectiva ante posibles amenazas y fortaleciendo el Sistema de Gestión de Seguridad de la Información (SGSI) de las organizaciones.

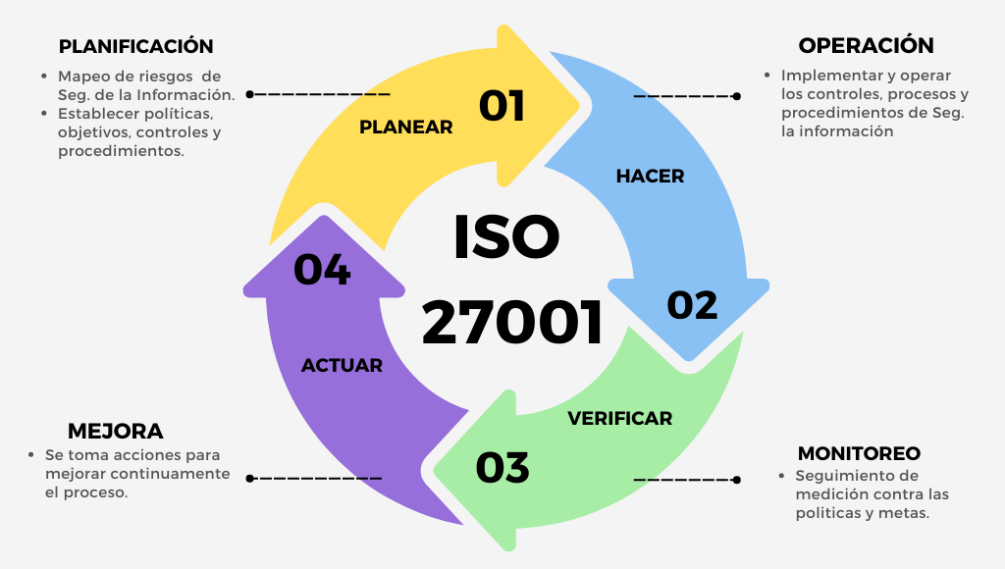

Figura 1.2: Ciclo PHVA (ISO 27001)

2.2 Gestión de continuidad del negocio

La gestión de la continuidad del negocio es fundamental para garantizar que los servicios de TI puedan recuperarse y continuar operando frente a incidentes, reduciendo el impacto en los procesos críticos de la organización. Un plan de contingencia ineficiente conlleva un peligro considerable, dificultando la reacción de respuesta ante eventos disruptivos que podrían provocar pérdidas importantes y evidenciando fallas en la gestión de la seguridad informática [11].

Por ello, el plan de continuidad del negocio (BCP), exige un enfoque integral que abarque tantos aspectos internos enfocados en el ámbito tecnológico, y externos como: desastres naturales, terremotos o inundaciones. Sin embargo, existe una carencia de soluciones por la falta de un plan de recuperación robusto y de procedimientos de continuidad

bien definidos aumentando significativamente la vulnerabilidad de la organización ante cualquier incidente imprevisto. La gestión de la continuidad (BCM) se orienta a mitigar el impacto de estos eventos disruptivos, permitiendo a la organización responder y recuperarse de manera eficaz, mientras se evalúan y optimizan los riesgos y costos asociados a posibles interrupciones [12].

2.2.1 Normativa ISO 22301: Sistema de continuidad del negocio

La norma ISO 22301 ofrece un marco de referencia para gestionar la continuidad del negocio y la resiliencia organizacional, siguiendo el ciclo de Planear, Hacer, Verificar y Actuar (PHVA) de la *Figura 2.2*, proporcionando pautas que ayuden a las compañías en la detección y manejo de posibles amenazas que puedan paralizar sus operaciones. Esta norma define la habilidad de una entidad de continuar con la entrega de productos y/o servicios dentro de tiempos aceptables durante la interrupción, haciendo énfasis en la importancia de la resiliencia, ejecutando un análisis de impacto del negocio considerando el nivel corporativo, el nivel del sistema y el retorno económico, para establecer estrategias de recuperación frente a desastres del sistema de información, a través de la realización de evaluaciones integrales y la creación de planes de recuperación de desastres (DRP) [13].

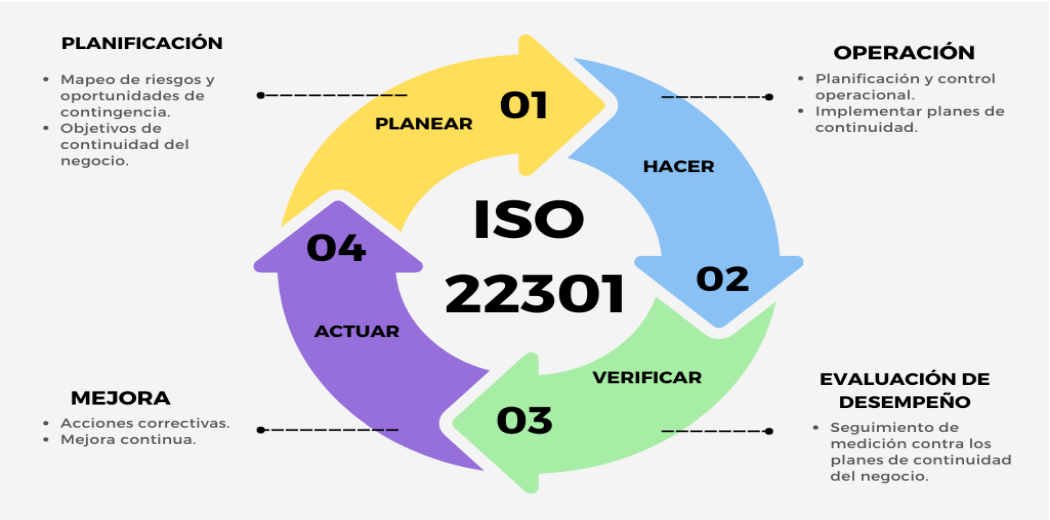

Figura 2.2: Ciclo PHVA (ISO 22301)

2.3 Soluciones propuestas en la industria

2.3.1 Casos de estudio de soluciones efectivas

La implementación de seguridad en sistemas de información ha transformado diversas actividades y procesos en las organizaciones. En la industria del desarrollo de software, las vulnerabilidades son comunes en la mayoría de las aplicaciones, y las técnicas tradicionales de detección suelen enfrentar desafíos recurrentes, como los falsos positivos o la incapacidad de identificar todas las vulnerabilidades [14]. Para abordar estos problemas, existen soluciones automatizadas que extraen vulnerabilidades utilizando bases de datos conocidas con información estática, combinadas con datos provenientes de proyectos de código abierto en C/C++ (como

Linux Kernel, Mozilla, Xen, httpd y Glibc). Estas soluciones permiten agregar información de vulnerabilidades de otros proyectos de código abierto como Cassandra, MongoDB, MySQL, Neo4J, Postgres y Django. Además, se han desarrollado paneles de control para facilitar el análisis de estas bases de datos [15].

Estas soluciones se complementan con otras investigaciones y conjuntos de datos en la industria. Por ejemplo, Reis y Abreu [16] crearon un conjunto de datos a partir de proyectos en GitHub, identificando 682 vulnerabilidades reales en 248 proyectos escritos en lenguajes populares. Además, Bhandari desarrolló CVEfixes, un conjunto de datos con vulnerabilidades y sus correcciones extraídas de la base de datos Nacional de Vulnerabilidades (NVD), lo que permite predecir y reparar vulnerabilidades [17].

Además, para las empresas de desarrollo de software es importante que adapten certificaciones de estándares respecto a ciberseguridad en un entorno comercial caracterizado por el desarrollo ágil y la integración de operaciones. Este enfoque no solo se centra en las propiedades del producto final, sino que evalúa los procesos utilizados en su desarrollo y operación. Tal estrategia permite a las organizaciones aumentar la confianza en la seguridad de sus sistemas, destacando la necesidad de establecer criterios claros para la certificación en un panorama digital en rápida evolución [18].

2.3.2 Retos de la seguridad para aplicaciones web y móviles

El desarrollo de aplicaciones web y móviles enfrenta numerosos retos en términos de seguridad, especialmente ante la creciente complejidad de las tecnologías y la diversidad de amenazas cibernéticas. La Open Web Application Security Project (OWASP) destaca las diez vulnerabilidades más críticas que pueden comprometer la seguridad de las aplicaciones, tales como inyecciones y problemas de autenticación [19]. Además, el auge de las tecnologías móviles, especialmente en plataformas como Android, introduce nuevos riesgos, ya que muchos usuarios almacenan información sensible en sus dispositivos.

El desarrollo ágil de software, aunque efectivo para responder rápidamente a las necesidades cambiantes de las organizaciones, presenta dificultades al integrar prácticas de seguridad de manera adecuada. A pesar de la implementación de metodologías como Scrum, XP y DevOps, que facilitan entregas rápidas y cambios continuos, la alineación de la agilidad con las políticas de seguridad sigue siendo un reto. El estudio “Security Practices in Agile Software Development” clasifica 252 actividades de seguridad extraídas de 35 investigaciones, organiza estas actividades en prácticas específicas dentro de cuatro dominios clave: gobernanza, inteligencia, ciclo de vida del desarrollo de seguridad y despliegue. La mayoría de las

actividades identificadas se relacionan con la estrategia y métricas de seguridad (12.7%), seguidas por pruebas de seguridad (10.7%), modelos de ataque (10.3%) y características de seguridad y diseño (10.3%). Estos resultados subrayan la necesidad de combinar actividades técnicas con iniciativas organizacionales, como la planificación de la seguridad, las pruebas de seguridad y la integración de requisitos de seguridad desde las primeras etapas del desarrollo. Además, se pueden utilizar estándares internacionales como las normas ISO para guiar la implementación de estas prácticas y garantizar que los procesos de desarrollo sean seguros, sin comprometer la agilidad [20

CAPITULO 3

IDENTIFICACIÓN DEL ENTORNO DE LA EMPRESA Y ACTIVOS CRÍTICOS

3.1 Análisis del entorno

Para el desarrollo del presente proyecto en una empresa de desarrollo de software, se llevó a cabo un levantamiento de información que incluyó entrevistas, revisiones documentales, análisis de procesos, revisión de incidentes previos ocurridos en la organización, así como la identificación de activos y recursos en la nube.

La recopilación de datos se basó en entrevistas estructuradas con dos líderes del equipo de tecnología y el Gerente General. Para ello, se utilizó una lista de preguntas que incluyó tanto interrogantes abiertas como cerradas, así como preguntas con escala de Likert para medir la perspectiva actual de la compañía. Además, se realizó una revisión documental sobre los activos de información y las actividades críticas de la

empresa, con el fin de identificar aquellos elementos clave relacionados con la seguridad de la información. Este proceso abarcó el estudio del uso de hardware y software, la protección de credenciales y el resguardo de la infraestructura de los servicios en la nube. También se investigaron los planes de contingencia y las estrategias de respuesta ante incidentes.

El alcance se centrará en la evaluación de riesgos y amenazas, así como en el diseño de las políticas de seguridad bajo estándares internacionales, dejando la implementación y evaluación de su aplicación para trabajos posteriores. Se realizará un análisis exhaustivo exclusivamente de los activos y procesos críticos, con el objetivo de identificar aquellos elementos clave para garantizar la protección de la información y la continuidad operativa del negocio, asegurando que las medidas de seguridad propuestas estén alineadas con las necesidades específicas de la organización.

3.2 Identificación de activos críticos

Como resultado del uso de diversas herramientas para identificar los activos de información, tal como la revisión de documentos históricos de inventarios, se han determinado clasificaciones de activos de información de la Tabla 1, los cuales están directa o indirectamente relacionados con la seguridad tecnológica y la operatividad de la compañía.

Tabla 1: Listado de activos críticos de la empresa

LISTA DE ACTIVOS CRÍTICOS			
TIPO DE ACTIVO	**DESCRIPCIÓN**	**UBICACIÓN**	**CANTIDAD**
Activo de Hardware	Laptops y PCs	Físico	16
Activo de Software	Licencia de administrador de contraseñas	Nube	1
Activo de Software	Servidores del entorno de desarrollo	Nube	4
Activo de Software	Servidores del entorno de QA	Nube	2
Activo de Software	Servidores del entorno de producción	Nube	5
Activo de Software	Servidores de respaldo	Nube	5
Activo de Software	Servidor de almacenamiento de videos	Nube	1
Activo de datos	Repositorios de código fuente	Nube	9
Activo de datos	Datos en equipos informáticos	Nube/Local	1
Activo de datos	Ficheros	Nube	4
Activo de datos	Bases de datos de proyectos	Nube/Local	6
Activo de redes	Router	Físico	2
Activo de redes	Firewall	Nube	1
Activo de redes	Red WLAN	Físico	1
Activo de redes	Red de telefonía	Físico	1
Activo auxiliares	Generador eléctrico	Físico	1
Activo auxiliares	UPS	Físico	1

Activo auxiliares	Equipo de climatización	Físico	1

3.3 Determinación y clasificación de procesos

Mediante una revisión de documentos, diálogos con el Gerente y tomando en cuenta la experiencia de uno de los miembros del equipo dentro de la organización, se lograron identificar los procesos principales y críticos dentro de la empresa de la Tabla 2, las mismas que están directamente relacionadas con la seguridad de la información y son fundamentales para el adecuado funcionamiento de la empresa.

Tabla 2: Procesos principales y críticos dentro de la empresa.

PROCESOS	DESCRIPCIÓN
Capacitación de nuevo personal	El proceso de capacitación para el nuevo personal ya sea pasante o profesional, tiene una duración de entre 1 y 2 semanas, y tiene como objetivo facilitar su integración efectiva al equipo. Durante este período, se le proporciona una formación intensiva en las tecnologías utilizadas, así como en la metodología ágil Scrum. Además, se cubren aspectos clave como el ciclo de vida del

	software, las buenas prácticas de desarrollo, herramientas y procesos internos que se emplean en la organización. También se procede con la entrega de equipos necesarios para la realización de sus actividades con una carta firmada de recepción de equipos. La capacitación se realiza de manera presencial o remota, adaptándose a las circunstancias y necesidades del nuevo integrante.
Desvinculación del personal	Cuando un colaborador deja la organización, debe realizar la entrega de todos los equipos y materiales proporcionados al inicio de sus actividades, tales como laptop, teléfonos móviles, cargadores, periféricos (mouse, monitor, micrófono, memorias, Raspberry Pi o cualquier otro hardware). Además, el colaborador debe firmar una carta de entrega de equipos, en la cual se especifica el estado en que se devuelven los artículos.
Subida de actualizaciones de software	Para subir cambios autorizados en el código fuente, el autor primero debe realizar un pull request hacia la rama de desarrollo (develop).

	Este pull request es revisado por el encargado de calidad, quien realiza las revisiones y pruebas necesarias en conjunto con el líder de proyecto. Dependiendo del caso, se pueden solicitar cambios adicionales o el pull request es aprobado siendo necesaria la aprobación de 2 o más personas. Una vez aprobado, el equipo de desarrollo procede a subir la actualización al servidor de desarrollo. Después de realizar las pruebas en el entorno de desarrollo, si todo funciona correctamente, se repite el proceso con un nuevo pull request hacia la rama main para la integración final de los cambios.
Revisión de código y pruebas	La aprobación de cambios y su despliegue hacia los entornos de desarrollo y producción debe ser realizada por al menos dos personas: el encargado de calidad (QA) y el líder de proyecto. El encargado de calidad es responsable de realizar las pruebas unitarias y el control de

	calidad del código, asegurando que los cambios cumplan con los estándares técnicos y no introduzcan errores en el sistema. Por otro lado, el líder de proyecto o un superior se enfoca en aspectos más amplios como la usabilidad, experiencia del usuario y rendimiento del sistema.
Creación de backups de DB	Se deben crear scripts en cada servidor para realizar backups periódicos de las bases de datos y recursos como archivos críticos utilizados, ejecutándose de 1 a 3 veces por día. Además, cada proyecto debe contar con un servidor de backup independiente, con un volumen de espacio desplegado en la nube. En este servidor se deben almacenar de manera automática los backups de bases de datos encriptadas para garantizar la seguridad y disponibilidad de la información.
Planificación y monitoreo de Sprint	El líder de proyecto o encargado es responsable de generar o preparar las historias de usuario, tareas o bugs en el

	backlog, los cuales también pueden ser creados por los colaboradores. El primer día del sprint, se presentan las historias y tareas a desarrollar al equipo, y se evalúan aspectos como el peso, la duración, los entregables y los responsables de cada tarea. Durante el sprint, cada 1 o 2 días se realizan revisiones de avances y logros. Al finalizar el sprint, se realiza la revisión final y la entrega del producto incrementado, donde se obtiene retroalimentación del cliente o partes interesadas.
Gestión de tickets y resolución de incidencias	Los clientes de un software en producción pueden notificar cualquier bug o requerimiento mediante tickets generados a través de una aplicación de terceros como Zendesk, Freshdesk o Groove o incluso via correo. Estos tickets se convierten en un canal de comunicación directa, con el líder de proyecto, quien también recibe las evidencias y detalles del incidente.

	Dependiendo de la gravedad o importancia de la incidencia, se evalúa y clasifica la urgencia del ticket. En función de esto, se procede a comunicar al cliente y a agendar la actualización o corrección del problema en una fecha u hora tentativa.
Rollback en casos de incidencias críticas	Se implementa un proceso de rollback para revertir los últimos cambios realizados en alguno de los proyectos mediante Git. Si el rollback no es suficiente para resolver la incidencia, se recurre a uno de los backups de bases de datos disponibles. Se busca deshacer modificaciones recientes que puedan haber afectado el rendimiento o la seguridad.

CAPÍTULO 4

EVALUACIÓN DE LOS RIESGOS Y VULNERABILIDADES

La compañía enfrenta una serie de desafíos significativos relacionados con la seguridad de la información, lo que pone en riesgo tanto la integridad de sus sistemas como la confidencialidad de los datos manejados. A lo largo de su trayectoria, en el departamento de desarrollo se han experimentado múltiples incidentes que evidencian la falta de un plan integral de protección.

Para ello, es esencial evaluar la compañía con la implementación de un análisis de riesgo, donde podremos plasmar los hallazgos tomando en consideración pilares fundamentales como la TRIADA (Confidencialidad, integridad y disponibilidad), reflejada en la *Figura 3.4*.

Figura 3.4: Pilares de la Seguridad Informática (Autores)

Al considerar estos factores podremos calcular los niveles de impacto, probabilidad y riesgo para proteger lo que se considera más crítico para la empresa como en la *Figura 4.4*.

Figura 4.4: Evaluación de Riesgos (Autores)

En la tabla 3, para una empresa desarrolladora de software, la confidencialidad implica proteger el código fuente, datos de clientes y documentación interna, asegurando que solo personal autorizado tenga acceso. La integridad garantiza que activos de información como código, los datos y la documentación no sean alterados sin autorización. La disponibilidad asegura que herramientas, servidores y repositorios estén operativos para el desarrollo y entrega del software al cliente.

Tabla 3: Valoración TRIADA

TRIADA					
CONFIDENCIALIDAD		INTEGRIDAD		DISPONIBILIDAD	
NIVEL	CRITERIO	NIVEL	CRITERIO	NIVEL	CRITERIO
ALTO (5)	La información está disponible solo para los empleados y procesos autorizados. En caso de ser utilizada por un tercero puede conllevar a un impacto negativo operativo, legal y económico.	ALTO (5)	La pérdida de información conlleva un impacto negativo operativo, legal, económico a nivel catastrófico.	ALTO (5)	La no disponibilidad de la información genera un impacto negativo severo en los ámbitos operativo, legal y económico. La no disponibilidad no debe superar las 2 horas.
MEDIO (3-4)	La información está disponible para todos los empleados y procesos. En caso de ser utilizada por un tercero puede conllevar a un impacto negativo en los procesos de la empresa.	MEDIO (3-4)	La pérdida de información conlleva un impacto negativo legal, económico u operativo a nivel moderado.	MEDIO (3-4)	La no disponibilidad de la información genera un impacto negativo moderado en los ámbitos operativo, legal y económico. La no disponibilidad no debe superar las 6 horas.
BAJO (1-2)	La información puede ser consultada o utilizada por cualquier persona dentro o fuera de la organización, sin que esto implique daños a la empresa o a terceros.	BAJO (1-2)	La pérdida de información no conlleva un impacto significante para la organización	BAJO (1-2)	La no disponibilidad de la información puede afectar las operaciones normales de la organización pero no posee un impacto en los ámbitos legales y económicos. La no disponibilidad no debe superar las 24 horas.

La evaluación de amenazas y vulnerabilidades es esencial en la seguridad informática para gestionar riesgos de manera efectiva. En la Tabla 4 se propone una escala de cinco niveles, donde 1 representa una amenaza o vulnerabilidad baja y 5 muy alta, según criterios definidos por los autores.

Tabla 4: Escala de valoración de amenazas y vulnerabilidades

Valoración de amenazas y vulnerabilidades			
VALORACIÓN	NIVEL	AMENAZA	VULNERABILIDAD
1-2	BAJO	Posee experiencia y recursos limitados para llevar a cabo un ataque. Busca obtener información sensible e interrumpir brevemente los recursos, pero sus efectos son mínimos. Puede afectar a pocos o ningún área de la organización.	Representa una preocupación leve o mínima, su remediación puede mejorarse aunque no resulta indispensable.
3	MEDIO	Dispone de experiencia y recursos moderados para ejecutar uno o pocos ataques, con el objetivo de obtener, modificar o comprometer la información sensible o los recursos de la organización. Sus acciones podrían afectar parcialmente a la infraestructura y los servicios de la empresa.	Supone una preocupación moderada debido a la complejidad con la que puede ser explotada, la gravedad de sus posibles consecuencias y su nivel de exposición limitado.
4	ALTO	Cuenta con un alto nivel de experiencia y dispone de los recursos suficientes para llevar a cabo numerosos ataques. Tiene la capacidad de comprometer o paralizar funciones esenciales de la organización.	Genera gran preocupación por la facilidad con la que puede ser explotada, la gravedad de sus posibles consecuencias y su alta exposición.
5	MUY ALTO	Posee un nivel de experiencia avanzado y dispone de los recursos necesarios para ejecutar ataques continuos de forma sostenida. Puede obstaculizar de manera significativa o incluso anular la función principal de la organización.	Está altamente expuesta, y su explotación aparte de ser sencilla podría generar consecuencias graves.

En la gestión de riesgos, es crucial medir el impacto de posibles amenazas en las operaciones. Se puede observar en la Tabla 5 una clasificación del nivel de afectación, donde 1 representa un impacto insignificante, con mínima o nula interrupción, y 5 un impacto catastrófico, con graves consecuencias para la viabilidad de la empresa. Esto nos ayuda a priorizar estrategias de mitigación y reforzar medidas de seguridad para reducir la exposición a amenazas.

Tabla 5: Escala de valoración de Impacto

Valoración de impacto		
VALORACIÓN	NIVEL	CRITERIO
1-2	Insignificante-Menor	Impacto leve que puede requerir atención, pero no representa un riesgo crítico
3	CRITICO	Impacto notorio que afecta resultados importantes, pero manejables con recursos adicionales.
4	MAYOR	Impacto severo que causa interrupciones críticas o pérdidas importantes, requiriendo intervención urgente.
5	CATASTROFICO	Impacto extremo que causa daños irreparables o pérdidas masivas, comprometiendo la viabilidad del proyecto u organización.

Como se muestra en la Tabla 6, la probabilidad de ocurrencia de eventos de seguridad se evalúa en una escala de 1 a 5, donde 1 indica una probabilidad remota o poco probable, y 5 una probabilidad constante o inminente. Este enfoque ayuda a determinar la recurrencia de los riesgos y a definir medidas para reducir su impacto.

Tabla 6: Escala de valoración de Probabilidad

Valoración de Probabilidad		
VALORACIÓN	NIVEL	CRITERIO
1-2	Improbable- Posible	Eventos con baja probabilidad de ocurrencia, pero que no pueden descartarse completamente
3	Ocasional	Eventos que pueden suceder de manera intermitente o en circunstancias específicas.
4	Moderador	Eventos que tienen una alta probabilidad de ocurrencia en condiciones normales.
5	Constante	Eventos que ocurren de manera constante o recurrente, casi seguros en un plazo corto.

El valor del riesgo se calcula mediante el producto de los valores de impacto y probabilidad. Este cálculo determina el nivel que de acuerdo con la Tabla 7 se clasifica en tres categorías: bajo, medio y alto. Esta evaluación permite priorizar los riesgos en función de su gravedad y frecuencia, facilitando la toma de decisiones sobre las medidas preventivas y correctivas necesarias para proteger los activos de la empresa desarrolladora de software.

Tabla 7: Escala de niveles de riesgo

Nivel de Riesgo		
VALORACIÓN	NIVEL	CRITERIO
1-4	El riesgo es BAJO	Riesgo menor, con impacto y/o frecuencia reducida. Es manejable sin intervenciónsignificativa.
5-14	El riesgo es MEDIO	Riesgo moderado, con impacto notable o frecuencia ocasional. Requiere atenciónpara mitigarlo.
15-25	El riesgo es ALTO	Riesgo crítico, con alta probabilidad o impacto severo. Necesita intervención inmediata y prioritaria.

4.1 Identificación de riesgos y vulnerabilidades

La identificación de amenazas y vulnerabilidades en los activos de la empresa resultó en un proceso detallado de encuestas, entrevista y la revisión de documentación relevante. Los hallazgos, sustentados por los autores consultados, permiten obtener una comprensión profunda de los riesgos asociados a cada activo, lo que facilita la creación de estrategias de mitigación personalizadas. En la Tabla 8 se detalla la lista de activos y sus respectivos hallazgos, ofreciendo un panorama completo de los riesgos asociados.

Tabla 8: Identificación de riesgos y vulnerabilidades de activos

Nº	Descripción	Hallazgos	Amenaza	Vulnerabilidad
1	Laptops y PCs	Algunos colaboradores han utilizado equipos de la empresa para actividades personales o recreativas, lo que ha expuesto la red corporativa a infecciones o accesos no autorizados	Uso indebido de equipos corporativos para actividades personales.	Los dispositivos corporativos carecen de restricciones técnicas o políticas adecuadas para prevenir actividades personales, lo que aumenta la exposición a riesgos de ciberseguridad.
2	Licencia de administrador de contraseñas	Los colaboradores a cargo desconocen prácticas seguras para compartir las contraseñas	Accesos no autorizados e intercepción de información	Envío de contraseñas a través de medios no cifrados o protegidos como correo electrónico, mensajes de texto o aplicaciones de mensajería sin protección adecuada.
3	Servidores del entorno de desarrollo	La configuración posee ajustes predeterminados o	Inyección de malware y	Existencia de puertos y servicios innecesarios o no configurados

		inseguros como puertos y servicios abiertos, contraseñas por defecto	explotación de puertos abiertos	
4	Servidores del entorno de QA	Se detectó presencia de datos sensibles o de producción dentro de este entorno para la realización de pruebas	Exposición de información a personal no autorizado	No existe un correcto aislamiento de los datos o bases utilizadas entre producción y QA
5	Servidores del entorno de producción	No se encontró un plan definido de recuperación ante desastres para la restauración rápida de los servicios en producción	Interrupciones prolongadas en los servicios y pérdidas de datos críticos	Ausencia de procedimientos documentados y estandarizados ante desastres
6	Servidores de respaldo	No se implementa cifrado en algunas copias de seguridad	Robo o exposición de datos	Dependencia única a la protección y medidas de seguridad del proveedor
7	Servidor de almacenamiento de videos	Los recursos están centralizados en una sola máquina virtual en la nube	Ataques DDoS que afecte la disponibilidad de los recursos	Limitada replicación debido a un único servidor
8	Repositorios de código fuente	Los repositorios contienen	Consumo de recursos en la nube	No existe un monitoreo para detectar uso

		credenciales o información sensible de configuración	causando sobrecostos o interrupciones	indebido y exposición de credenciales en código fuente
9	Datos en equipos informáticos	Uso de diferentes tipos de hardware y software en los equipos	Ataques a sistemas y equipos no actualizados	Dificultad para mantener actualizados los sistemas operativos y aplicaciones
10	Ficheros Multimedia	Los datos almacenados (videos, imágenes) en la nube suelen accederse desde múltiples ubicaciones y dispositivos por parte de los empleados	Empleados o colaboradores con intenciones maliciosas que aprovechan el acceso	No existe limitación adecuada de los permisos según la ubicación o el dispositivo.
11	Bases de datos en producción	No hay registros de auditorías para monitorear y registrar quién accede o realiza cambios en los datos	Ataques internos de empleados malintencionados	Ausencia de mecanismos de control, visibilidad y trazabilidad
12	Router	El dispositivo está configurado con las reglas de seguridad estándar, sin	Accesos no autorizados y ataques DoS	Falta de personalización de las reglas de seguridad y

		personalización u optimización según las necesidades específicas.		desactualización del firmware
13	Firewall	El tráfico y las alertas generadas ante posibles amenazas no cuentan con la supervisión continua del personal	Ataques DDoS que hacen ineficaz al firewall	Existen limitaciones en la visibilidad y en las alertas automáticas para una respuesta eficiente a incidentes.
14	Red WLAN	Los registros de mantenimiento no están documentados y no existen auditorías de seguridad de la red	Ataques cibernéticos y robos de datos	Ausencia de medidas de seguridad como cifrado y autenticación para la red local
15	Red de telefonía	Los equipos de telefonía no son sometidos a mantenimiento e inspección	Interrupción de comunicación por problemas técnicos	No existen protocolos para detectar y prevenir fallos
16	Generador eléctrico	En el inventario solo se cuenta con una unidad, lo que podría resultar insuficiente para cubrir todos los	Interrupción o fallo inesperado por sobrecarga	Dependencia de un único generador

		dispositivos necesarios durante las operaciones en caso de una falta de suministro eléctrico		
17	UPS	Falta de pruebas regulares para verificar la autonomía de la batería.	Desastres naturales y variaciones de voltaje	Baterías en mal estado o envejecidas que no garantizan el suministro necesario
18	Equipo de climatización	No se encontraron registros de inspecciones técnicas o de funcionamiento del equipo.	Fallo inesperado del equipo e Interrupción de actividades de empleados	Incumplimiento de normativas de mantenimiento preventivo

4.2 Valoración de riesgos y vulnerabilidades

La valoración de riesgos y vulnerabilidades es un proceso clave para la gestión de riesgos, que permite identificar, analizar y priorizar amenazas que pueden afectar los activos de la compañía. A través de la matriz de riesgo implementada se evaluó el impacto, probabilidad y nivel de riesgo, con el propósito de mitigar las amenazas identificadas.

Los resultados de la evaluación de la matriz de riesgo fueron extraídos de las fórmulas de la *Figura 5.4*, representados en un mapa de calor de 5X5 constituida de forma cualitativa, estableciendo rangos por la probabilidad y el impacto de los ejes de la tabla 4 y tabla 5. Esto facilita la compresión visual de los diversos riesgos, permitiendo combinar los dos factores en un solo gráfico, colocando colores al estilo semáforo e incluyendo el nivel de riesgo inherente, es decir, riesgo existente antes de aplicar cualquier control o medida de mitigación a los riesgos encontrados.

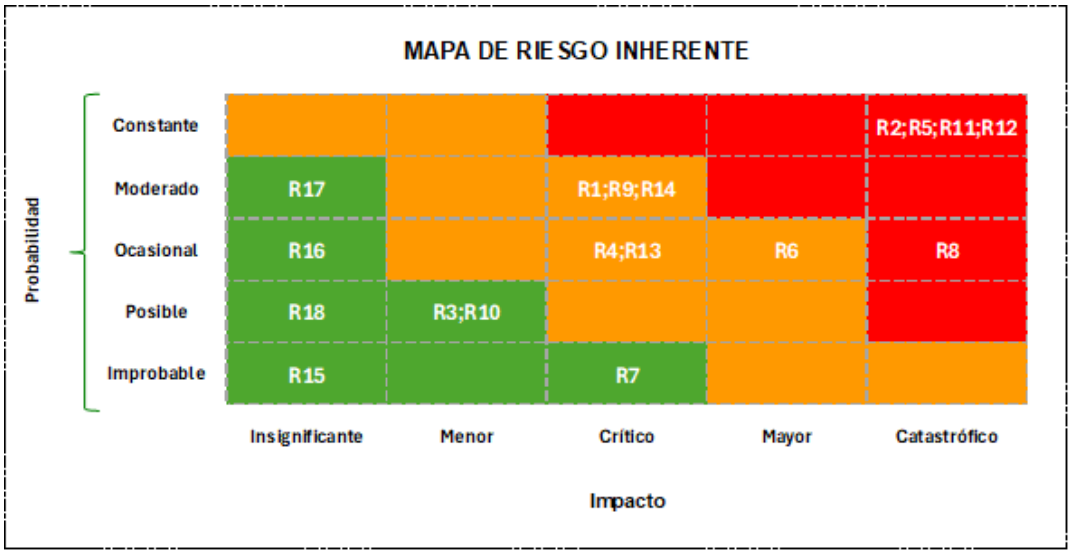

Figura 5.4: Mapa de Riesgo Inherente de Seguridad de la Información

4.3 Tratamiento de riesgos

Para el tratamiento definimos las acciones necesarias para abordar los riesgos identificados en la organización. En este proceso, se deben considerar diversas estrategias para reducir el impacto de las amenazas y

vulnerabilidades, garantizando la continuidad y estabilidad de los procesos. Las principales estrategias de tratamiento incluyen evitar, aceptar, transferir y mitigar el riesgo, cada una adecuada a diferentes circunstancias y niveles de exposición. En la Tabla 9 se reflejan estas estrategias junto con su descripción detallada, lo que proporciona un marco claro para seleccionar y aplicar la estrategia más apropiada según el tipo y la magnitud del riesgo.

Tabla 9: Estrategias de tratamiento de riesgos

OPCIONES DE TRATAMIENTO	
Método	**Descripción**
EVITAR	No realizar la actividad o evitar la situación que genera el riesgo.
ACEPTAR	Asumir el riesgo y sus consecuencias, cuando el impacto es bajo o se considera manejable.
TRANSFERIR	Movilizar el riesgo a un tercero, delegando su gestión o las posibles consecuencias a una entidad externa.
MITIGAR	Reducir la probabilidad de ocurrencia o el impacto del riesgo mediante controles o medidas específicas.

Los controles de seguridad son medidas clave para proteger la infraestructura y los activos de la empresa contra amenazas y vulnerabilidades. Se aplicaron las definiciones de acuerdo con la ISO 27002, en donde los controles se dividen en tres tipos principales: preventivo, detectivo y correctivo. Los controles preventivos buscan evitar que los incidentes de seguridad ocurran, los detectivos tienen como objetivo identificar y alertar sobre posibles incidentes en tiempo real, y los correctivos se aplican para restaurar la normalidad después de un incidente de seguridad. En la Tabla 10, se exponen estos tipos de controles junto con sus descripciones, proporcionando una guía para implementar una estrategia de seguridad efectiva.

Tabla 10: Tipos de controles de seguridad

OPCIONES DE CONTROLES	
Nombre	**Descripción**
PREVENTIVO	Evita que ocurran incidentes de seguridad.
DETECTIVO	Identifica y alerta sobre incidentes de seguridad o anomalías en curso.
CORRECTIVO	Minimiza el impacto y restaura la normalidad después de un incidente de seguridad.

El tratamiento adecuado de los riesgos es esencial para garantizar la protección de los activos. “La estrategia de identificación se basó en la evaluación de amenazas y vulnerabilidades y despues de los controles, demostrando mitigación En la Tabla 11, se detalla cómo, dependiendo del riesgo inherente calculado se establece una estrategia de tratamiento de riesgos, el tipo de control que se aplica y la medida a implementar según lo estipulado con la ISO 27001. Además, se incluye una breve descripción de cada tratamiento, lo que proporciona claridad sobre cómo abordar cada tipo de riesgo y cómo garantizar que se mantengan los estándares de seguridad.

Tabla 11: Tratamiento de los riesgos de activos

Descripción	Nivel	Método	Tipo de control	Controles a implementar (27001)	Descripción del tratamiento
Laptops y PCs	**MEDIO**	MITIGAR	Preventivo	Términos y condiciones de empleo para uso de equipos (6.2)	Realizar políticas sobre el uso de equipos de trabajo y concientizar sobre ellas.
Licencia de administrador de contraseñas	**ALTO**	MITIGAR	Preventivo	Información de autenticación (5.17)	Realizar políticas y asesoramiento al personal sobre el tratamiento de adecuado de la

					información de autenticación.
Servidores del entorno de desarrollo	**BAJO**	MITIGAR	Preventivo	Gestión de la configuración (8.9)	Aplicar y documentar configuraciones seguras al software, servicios y redes
Servidores del entorno de QA	**MEDIO**	MITIGAR	Preventivo	Clasificación de la información (5.12)	Clasificar la información en función de la confidencialidad, integridad y disponibilidad. Restringir y prevenir el uso indebido de datos de alta confidencialidad.
Servidores del entorno de producción	**ALTO**	MITIGAR	Preventivo	Preparación de las TIC para la continuidad del negocio (5.30)	Establecer las bases para garantizar la continuidad operativa de los servicios de tecnología de la

					información y comunicación (TIC) en caso de interrupciones, asegurando la disponibilidad, recuperación y sostenibilidad de los sistemas críticos para el negocio.
Servidores de respaldo	**MEDIO**	MITIGAR	Preventivo	Enmascaramiento de datos (8.11)	Aplicar mecanismos de encriptación y anonimización, controles de acceso a las copias y monitoreo continuo.
Servidor de almacenamiento de videos	**BAJO**	MITIGAR	Preventivo	Separación de los entornos de desarrollo, prueba y producción (8.31)	Definir lineamientos para separar los entornos de desarrollo, prueba y producción,

					garantizando la seguridad de los sistemas de información y reduciendo riesgos de cambios no autorizados, errores o accesos indebidos.
Repositorios de código fuente	**ALTO**	MITIGAR	Preventivo	Aceso al código fuente (8.4)	Gestión de identidad de acceso y a las aplicaciones. Depuración o cifrado de credenciales y datos sensibles en repositorios. Política para gestión de credenciales y accesos en código fuente.

Datos en equipos informáticos	**MEDIO**	MITIGAR	Preventivo	Instalación de software en sistemas operativos (8.19)	Establecer política de instalación y versionamiento de software y sistemas operativos autorizados. Seguir un proceso de autorización y revisión en instalaciones y actualizaciones.
Ficheros Multimedia	**BAJO**	MITIGAR	Correctivo	Restricción de acceso a la información (8.3)	Restringir el acceso a los activos conforme los roles o permisos y en conformidad con la política de control de acceso que se establezca.
Bases de datos en producción	**ALTO**	MITIGAR	Detectivo	Actividades de supervisión (8.16)	Implementar supervisión continua de accesos y

					actividades en las bases para informar de eventos como modificaciones y uso de datos críticos.
Router	**ALTO**	MITIGAR	Preventivo/Detectivo	Seguridad de redes (8.20)	Revisión y configuración del router. Establecer mantenimientos, actualizaciones y pruebas de seguridad periódicas.
Firewall	**MEDIO**	MITIGAR	Preventivo/Detectivo	Seguridad de los servicios de red (8.21)	Automatizar respuesta de seguridad sin intervención humana. Centralizar alertas en una sola plataforma. Capacitación de gestión de incidentes a

					personal conforma a la política de seguridad.
Red WLAN	**MEDIO**	MITIGAR	Preventivo	Seguridad de redes (8.20)	Establecer políticas de uso aceptable de red, auditorias y evaluaciones periódicas.
Red de telefonía	**BAJO**	ACEPTAR	Correctivo	Uso aceptable de la información y otros activos asociados (5.10)	Se acepta el riesgo ya que el impacto potencial de una falla es bajo y la probabilidad de que ocurra un incidente es mínima.
Generador eléctrico	**BAJO**	TRANSFERIR	Preventivo	Preparación de las TIC para la continuidad del negocio (5.30)	Debido a su bajo impacto el riesgo es transferido al área ténica de mobiliarios y equipos.
UPS	**BAJO**	TRANSFERIR	Preventivo	Preparación de las TIC para la	Debido a su bajo impacto el riesgo

				continuidad del negocio (5.30)	es transferido al área ténica de mobiliarios y equipos.
Equipo de climatización	**BAJO**	TRANSFERIR	Preventivo/Corrective	Preparación de las TIC para la continuidad del negocio (5.30)	Debido a su bajo impacto y probabilidad el riesgo es transferido al área ténica de mobiliarios y equipos.

El mapa de calor de los riesgos residuales de la *Figura 6.4* es una herramienta clave para visualizar el impacto de los riesgos que permanecen después de implementar los tratamientos especificados. Una vez que se toman en cuenta las estrategias y controles, se observa una disminución tanto en la probabilidad como en el impacto de los riesgos.

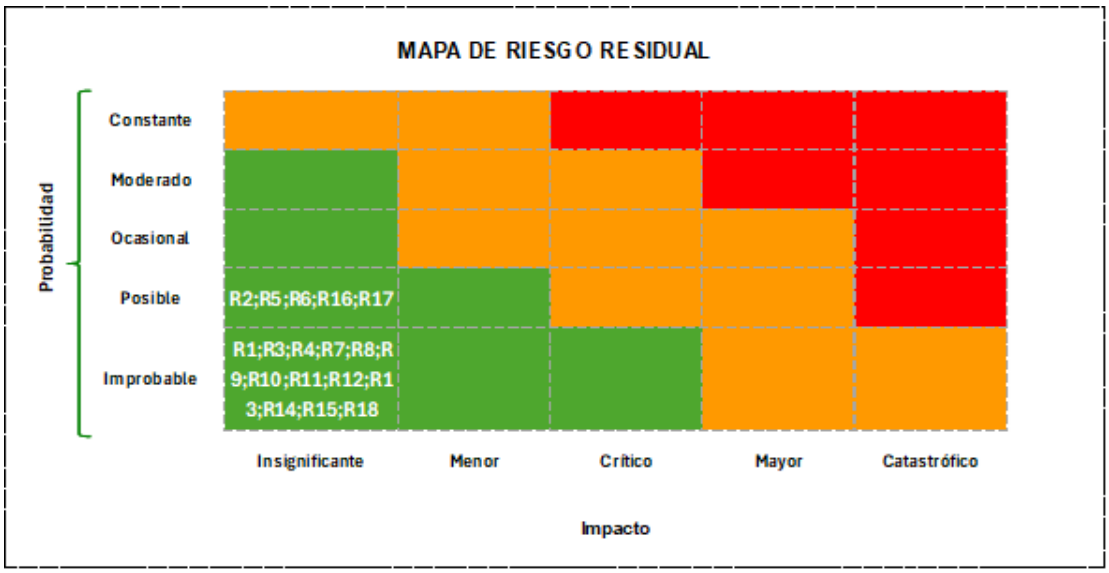

Figura 6.4: Mapa de Riesgo Residual de Seguridad de la Información

4.4 Impacto en la continuidad del negocio

El análisis de impacto en el negocio (BIA) es un proceso crucial para entender cómo los riesgos pueden afectar la continuidad operativa de una empresa. En este estudio, se analizarán los procesos de una empresa de desarrollo de software, enfocándose en los diferentes tipos de impacto que podrían comprometer su funcionamiento. En la Tabla 12 se presenta una escala de impacto que abarca los aspectos financieros, reputacionales, legales y operacionales, desde un impacto insignificante hasta uno catastrófico, con el fin de evaluar cómo las interrupciones pueden afectar la estabilidad y sostenibilidad del negocio. Este análisis proporcionará una base sólida para la planificación de contingencias.

Tabla 12: Valoración BIA

VALORACIÓN BIA					
Valoración	Nivel	Impacto financiero	Impacto reputacional	Impacto legal	Impacto operacional
1	Insignificante	$0 a $1,000	El incidente no genera afectaciones en la imagen corporativa ni en la confianza de los clientes.	No genera ninguna afectación a nivel normativo ni compromete la reputación de la organización. No se requiere acción regulatoria ni correctiva.	No impacta las operaciones y la empresa puede continuar funcionando con total normalidad.
2	Menor	$1,001 a $20,000	La afectación se restringe a un grupo reducido de clientes, sin generar repercusión externa significativa.	No genera incumplimientos normativos ni requiere acciones regulatorias. La operación de la empresa continúa sin afectaciones legales o de cumplimiento.	Afecta un proceso de control interno. Se requieren medidas correctivas, pero no hay un impacto significativo en la continuidad operativa.
3	Crítico	$20,001 a $40,000	La situación trasciende el ámbito interno y se difunde en medios de comunicación sectoriales o de alcance restringido, sin generar una crisis reputacional.	Puede generar observaciones en auditorías y posibles sanciones por parte de organismos reguladores. Aunque el impacto es manejable, la empresa deberá tomar medidas correctivas para evitar consecuencias mayores.	Afecta un proceso interno de la organización, lo que genera inconvenientes operativos, pero no interrumpe por completo la operación. Se requiere intervención para resolverlo, pero la empresa puede continuar con sus actividades.
4	Mayor	$40,001 a $80,000	El incidente es reportado en plataformas digitales, medios de comunicación y foros específicos de quejas, aumentando el riesgo de una escalada reputacional.	Puede derivar en multas impuestas por organismos reguladores, pero sin llegar a generar restricciones operativas. Aunque representa un impacto financiero y de cumplimiento, la empresa puede continuar sus actividades tras cumplir con las sanciones.	Afecta un proceso crítico de la organización, lo que tiene un impacto directo y significativo en el cliente. Esto puede paralizar operaciones clave y requiere una pronta resolución.
5	Catastrófico	Más de $80,000	La situación se difunde ampliamente en redes sociales y medios de comunicación masivos, comprometiendo la imagen de la empresa y generando una pérdida de confianza de clientes y socios estratégicos.	Requiere un pronunciamiento público por parte de los organismos reguladores y puede resultar en la imposición de múltiples restricciones. Esto puede afectar gravemente la operación de la empresa, generando un impacto significativo en su cumplimiento normativo y reputación.	Impacta directamente en el tiempo de respuesta comprometido con el cliente para la entrega de un producto o servicio, lo que provoca retrasos significativos y puede afectar la satisfacción del cliente. Requiere una resolución urgente para evitar consecuencias graves.

En el marco de análisis de impacto al negocio, evaluamos los tiempos de recuperación e interrupción para garantizar la continuidad de las operaciones críticas. Se utilizaron métricas clave como el RTO (Recovery Time Objective), que define el tiempo máximo tolerable para la recuperación de un proceso tras una interrupción, y el RPO (Recovery Point Objective), que establece el punto máximo de pérdida de datos aceptable en caso de un fallo. Además, se tomó en cuenta el MTPD (Maximum Tolerable Period of Disruption), que determina el tiempo máximo que una operación puede estar interrumpida antes de que su

impacto se vuelva catastrófico. Las respectivas escalas establecidas se presentan a continuación en la Tabla 13.

Tabla 13: Valoración de tiempos de impacto y recuperación

VALORACIÓN TIEMPOS RECUPERACIÓN/INTERRUPCIÓN				
Valoración	Criticidad	RTO	RPO	MTPD
5	Crítico	Los servicios tecnológicos o activos requieren una configuración de alta disponibilidad, con un margen de hasta 2 horas para interrupciones perceptibles.	Los servicios tecnológicos o activos requieren que los datos estén disponibles en todo momento, con un margen para pérdidas de hasta 2 horas.	La interrupción de este servicio o activo causa una paralización total de las operaciones esenciales de la empresa. Debe resolverse en un plazo máximo de 4 horas para evitar pérdidas graves y afectaciones críticas en la continuidad del negocio.
4	Prioridad alta	Los servicios tecnológicos o activos deben ser restaurados en menos de 4 horas para minimizar interrupciones y garantizar la continuidad operativa.	Los servicios tecnológicos o activos solo pueden aceptar la pérdida de datos de las últimas 4 horas, asegurando que la mayoría de la información permanezca íntegra	La interrupción afecta significativamente la entrega de servicios o productos, generando posibles pérdidas financieras o incumplimientos contractuales. Aunque la empresa puede operar de forma limitada, es fundamental restablecer el servicio en un máximo de 8 horas para evitar impactos severos.
3	Prioridad media	Los servicios tecnológicos o activos pueden tolerar una interrupción de hasta 8 horas, tras lo cual deben ser restablecidos para evitar repercusiones significativas en la operación.	Los servicios o activos solo pueden tolerar la pérdida de datos generados o modificados en un periodo máximo de 8 horas, con impacto controlado en la operación.	La interrupción genera inconvenientes operativos moderados, pero la empresa puede continuar sus funciones con planes alternativos. Sin embargo, el restablecimiento debe realizarse en un máximo de 24 horas para evitar retrasos en las operaciones y afectaciones en la productividad del equipo.
2	Prioridad media	Los servicios tecnológicos o activos pueden permanecer interrumpidos por hasta 16 horas sin afectar de manera crítica la operación, aunque podrían presentarse impactos parciales en la continuidad del negocio.	Los servicios tecnológicos o activos pueden operar con la pérdida de información generada o modificada en las últimas 24 horas, sin afectar gravemente la continuidad del negocio	La interrupción tiene un impacto menor en la operatividad diaria y puede resolverse en un plazo más amplio sin afectar gravemente el negocio. Se recomienda restablecer el servicio en un máximo de 48 horas para evitar acumulación de tareas o afectaciones menores en el flujo de trabajo.
1	Insignificante	Lo servicios o activos no están sujetos a tiempos estrictos de recuperación y pueden tolerar disrupciones más prolongadas que 24 horas sin un impacto crítico.	Los activos tecnológicos o activos no están sujetos a estrictas políticas de retención de datos y pueden tolerar pérdidas más prolongadas que 24 horas sin un impacto inmediato en la operatividad	La interrupción no tiene un impacto relevante en las operaciones y puede resolverse en cualquier momento sin urgencia. Estos servicios o activos pueden permanecer fuera de servicio por más de 72 horas sin generar consecuencias significativas en la empresa.

Es fundamental analizar los procesos clave de la empresa para identificar sus riesgos asociados. En la Tabla 14 se presenta una lista detallada de los procesos críticos de la empresa, acompañada de los hallazgos obtenidos durante la investigación, las amenazas que podrían afectarlos y las vulnerabilidades inherentes.

Tabla 14: Identificación de riesgos y vulnerabilidades de procesos

N.º	Proceso	Hallazgos	Amenaza	Vulnerabilidad
1	Capacitación de nuevo personal	No existe un proceso formal de evaluación y seguimiento posterior a la capacitación inicial, lo que puede generar brechas en el conocimiento de los nuevos empleados sobre prácticas de seguridad de la información y políticas internas.	Un empleado recién ingresado con conocimientos insuficientes sobre seguridad informática puede cometer errores que expongan información confidencial, provoquen configuraciones inseguras o faciliten ataques de ingeniería social.	Falta de verificación sobre la correcta asimilación de las políticas de seguridad, manejo de datos sensibles y uso seguro de herramientas internas por parte del nuevo personal.
2	Desvinculación del personal	No existe un procedimiento formalizado para la	Un excolaborador con acceso no revocado podría filtrar	Excolaboradores podrían mantener credenciales activas

		revocación inmediata de accesos a sistemas y servicios internos tras la desvinculación del personal.	información sensible, modificar código de manera malintencionada o realizar acciones que comprometan la seguridad y continuidad de la empresa.	o accesos no revocados a plataformas internas, repositorios de código, servicios en la nube o herramientas corporativas.
3	Subida de actualizaciones de software	No existe un control automatizado para verificar que las actualizaciones no contengan credenciales, información sensible o vulnerabilidades antes de ser desplegadas en los entornos de desarrollo y producción.	Un atacante interno o un desarrollador sin malas intenciones podría introducir código con vulnerabilidades explotables, filtración de credenciales en el repositorio o malas configuraciones que comprometan la seguridad del sistema.	Dependencia exclusiva de revisiones manuales para detectar errores de seguridad, lo que aumenta el riesgo de que credenciales, configuraciones inseguras o vulnerabilidades sean introducidas en el código.
4	Revisión de código y pruebas	El proceso de revisión de código no incluye una evaluación exhaustiva de las	La inclusión de bibliotecas vulnerables o maliciosas en el proyecto puede abrir	Las dependencias de software de terceros pueden contener

		dependencias externas utilizadas en el proyecto, lo que podría generar vulnerabilidades si se utilizan bibliotecas o componentes desactualizados o maliciosos.	puertas a ataques como la ejecución remota de código, inyecciones, o explotación de vulnerabilidades específicas de las bibliotecas, comprometiendo la integridad y seguridad de la aplicación y los datos.	vulnerabilidades conocidas que no son detectadas si no se realiza un análisis riguroso y continuo de las actualizaciones de dichas bibliotecas.
5	Creación de backups de DB	No se realizan pruebas periódicas de restauración de los backups, lo que podría llevar a la falsa suposición de que los datos son recuperables en caso de desastre.	En caso de un incidente de pérdida de datos o fallo del sistema, si los backups no pueden ser restaurados correctamente, la empresa podría sufrir pérdida de datos crítica, interrupción de servicios o un largo tiempo de inactividad, afectando la continuidad del negocio	La falta de pruebas regulares de restauración de backups puede generar una falsa sensación de seguridad, ya que no se valida si los archivos de respaldo están completos, intactos y pueden ser restaurados efectivamente en caso de necesidad.

			y la confianza del cliente.	
6	Planificación y monitoreo de Sprint	No se realiza una revisión formal de seguridad en las historias de usuario, tareas o bugs del backlog, lo que puede permitir que vulnerabilidades de seguridad se pasen por alto durante el ciclo de desarrollo.	Una historia de usuario o tarea que involucre información sensible o la integración con sistemas externos podría ser mal implementada o contener vulnerabilidades de seguridad, permitiendo a un atacante comprometer la aplicación, robar información o ejecutar ataques como inyecciones o escalada de privilegios.	La ausencia de una evaluación de seguridad en las fases tempranas de planificación y durante la revisión de avances incrementales puede llevar a que no se identifiquen riesgos de seguridad en el código o en las funcionalidades solicitadas por el cliente.
7	Gestión de tickets y resolución de incidencias	No existe un protocolo claro para la gestión segura de los tickets que contengan información sensible, como datos	La exposición de información sensible a través de los tickets podría ser aprovechada por atacantes internos o externos para robar	La falta de un manejo adecuado de la información sensible en los tickets puede resultar en la exposición no

		personales del cliente o detalles de configuración del sistema.	datos, realizar ataques de ingeniería social, o comprometer la seguridad del sistema a través de la explotación de vulnerabilidades mencionadas en los tickets.	autorizada de datos confidenciales, tanto por parte de los empleados como a través de canales inseguros (correo electrónico, aplicaciones de terceros sin encriptación, etc.).
8	Rollback en casos de incidencias críticas	El proceso de rollback en ambiente de producción, depende exclusivamente de los cambios recientes gestionados a través de Git, sin un control adicional para verificar que las versiones previas no tengan vulnerabilidades conocidas o configuraciones inseguras.	Restaurar una versión anterior con vulnerabilidades conocidas podría exponer la aplicación a ataques cibernéticos, como inyecciones SQL, acceso no autorizado o ejecución de código malicioso, comprometiendo la seguridad y la integridad del sistema. Además, si los backups utilizados no están actualizados o	El rollback podría restaurar versiones anteriores que contienen vulnerabilidades o configuraciones inseguras que ya han sido identificadas, pero no solucionadas, lo que podría permitir la explotación de estos fallos si no se realiza una validación adecuada.

			correctamente cifrados, podría comprometerse la confidencialidad de los datos restaurados.	

El mapa de calor del riesgo inherente presentado en la *Figura 7.4*, proporciona una visualización clara de los riesgos a los que están expuestos los procesos de la empresa. A través de este análisis, se identificaron los estados de los procesos clave en términos de continuidad del negocio, observándose que, en su mayoría, los riesgos presentan un impacto crítico o mayor y probabilidades altas de ocurrir. Este mapa de calor destaca la vulnerabilidad de los procesos más esenciales, lo que subraya la necesidad de una atención urgente para aplicar estrategias efectivas que aseguren la perpetuidad operativa.

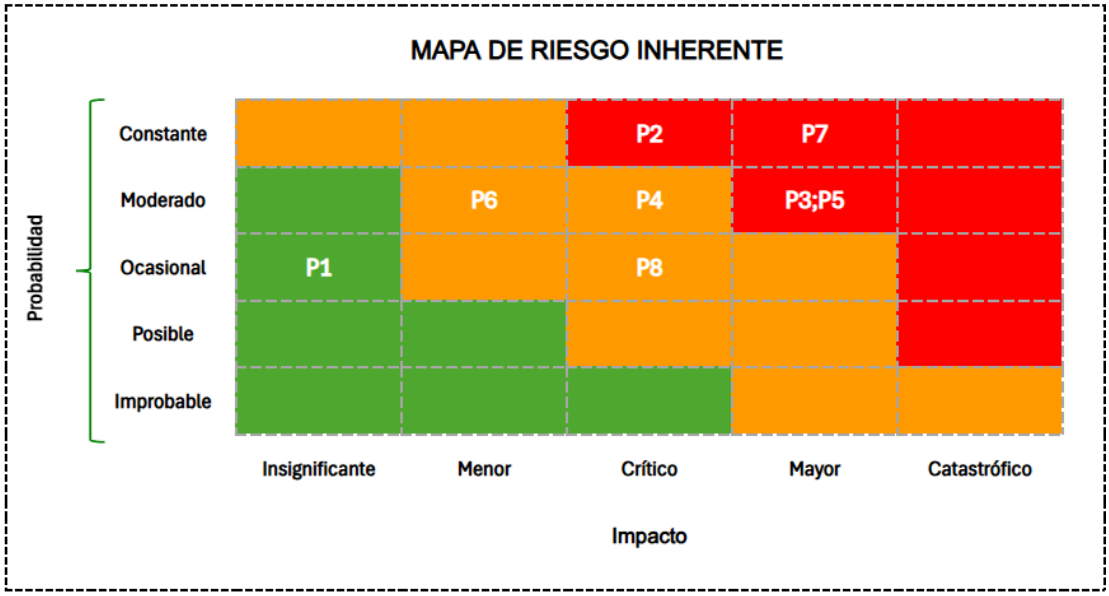

Figura 7.4: Mapa de Riesgo Inherente de Continuidad del Negocio

En el tratamiento de riesgos dentro del contexto de la ISO 22301 para la continuidad del negocio, es fundamental garantizar que los procesos críticos de la empresa se mantengan operativos ante cualquier interrupción. En la tabla 15, se presenta cómo, en función del riesgo inherente a cada proceso, calculado en base al impacto financiero, reputacional, legal y operacional y la probabilidad de ocurrencia, se determinan controles, acciones o políticas que aseguran la continuidad de los procesos esenciales y la capacidad de recuperación ante eventos disruptivos.

Tabla 15: Tratamiento de los riesgos de procesos

Proceso	Nivel	Método	Tipo de control	ISO 22301	Controles/Acciones/Políticas a implementar
Capacitación de nuevo personal	**BAJO**	MITIGAR	Preventivo	7.2 Competencia	Implementar un programa continuo de evaluaciones y capacitaciones a empleados para que mantengan un nivel adecuado de conocimientos en seguridad, continuidad del negocio y políticas internas a lo largo del tiempo.
Desvinculación del personal	**ALTO**	MITIGAR	Preventivo	6.1 Acciones para abordar los riesgos y las oportunidades	Establecer política de desvinculación de personal.
Subida de actualizaciones de software	**ALTO**	MITIGAR	Preventivo	6.1 Acciones para abordar los riesgos y las oportunidades	Establecer política de analisis de codigo fuente.
Revisión de código y pruebas	**MEDIO**	MITIGAR	Preventivo	6.1 Acciones para abordar los riesgos y las oportunidades	Establecer política de análisis y monitoreo de código fuente.

Creación de backups de DB	**ALTO**	MITIGAR	Preventivo	8.5 Programa de ejercicios y puebas	Realizar pruebas periódicas de restauración para garantizar la efectividad de recuperación ante desastres.
Planificación y monitoreo de Sprint	**MEDIO**	MITIGAR	Preventivo	8.1 Planificación y control operacional	Implementar la revisión de seguridad en el backlog para garantizar que se identifiquen y mitiguen riesgos desde las primeras etapas del desarrollo.
Gestión de tickets y resolución de incidencias	**ALTO**	MITIGAR	Preventivo	8.1 Planificación y control operacional	Establecer directrices para la gestión segura de tickets, asegurando que solo el personal autorizado pueda gestionar la información sensible.
Rollback en casos de incidencias críticas	**MEDIO**	MITIGAR	Preventivo	8.4 Planes y procedimientos para la continuidad del Negocio	Establecer plan de continuidad del negocio - DRP (Plan de recuperación de desastres), donde debe brindar orientación e información para ayudar a los equipos a responder en una interrupción y ayudar a la organización en la respuesta y recuperación

El mapa de riesgo residual en el contexto del Estudio BIA, orientado a procesos, proporciona una visión clara de los riesgos que aún persisten tras aplicar las acciones y controles recomendados. Tal como se ilustra en la *Figura 8.4*, una vez que se han implementado las estrategias de tratamiento y mitigación para cada proceso crítico, se observa una reducción tanto en la probabilidad como en el impacto. Al visualizar estos riesgos residuales, se asegura que los procesos esenciales se mantengan operativos y resilientes ante posibles interrupciones, minimizando el impacto en la estabilidad organizacional.

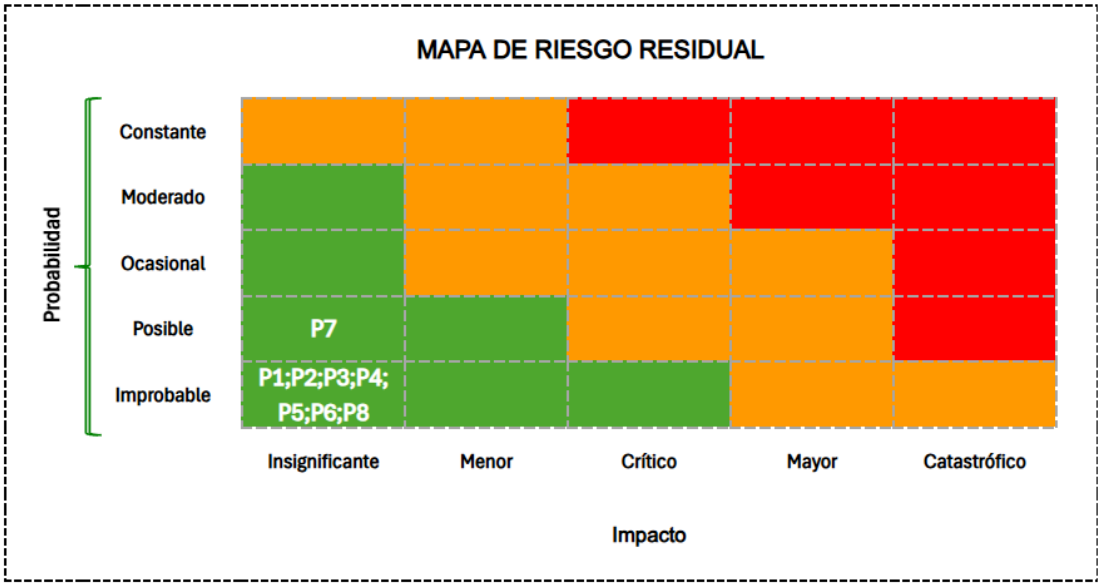

Figura 8.4: Mapa de Riesgo Inherente de Continuidad del Negocio

CAPÍTULO 5

DISEÑO DE ACCIONES Y POLÍTICAS FUNDAMENTADAS EN LAS NORMATIVAS ISO 27001 E ISO 22301

Tras la evaluación de los riesgos y vulnerabilidades identificadas en la infraestructura tecnológica y los procesos de la empresa de desarrollo de software, es fundamental establecer un marco de seguridad que permita mitigar los riesgos críticos y garantizar la continuidad operativa. En este capítulo, se diseñan políticas y acciones alineadas con las normativas ISO 27001 e ISO 22301, con el objetivo de fortalecer la seguridad de la información y la resiliencia del negocio ante posibles incidentes.

5.1 Aplicación de las normativas ISO 27001 e ISO 22301

La ISO 27001 proporciona un marco para la gestión de la seguridad de la información, asegurando la confidencialidad, integridad y disponibilidad de los datos. Por otro lado, la ISO 22301 establece las bases para un sistema de gestión de continuidad del negocio, permitiendo a la empresa mantener sus operaciones ante eventos disruptivos.

A partir del análisis de riesgos, se definen políticas específicas para la protección de la información, control de accesos, gestión de incidentes y recuperación ante desastres. Asimismo, se establecen estrategias para garantizar la disponibilidad de los servicios críticos y la capacidad de respuesta ante posibles interrupciones. A continuación, se detalla la aplicación práctica de las normativas definiendo lineamientos claros para su implementación y monitoreo continuo.

5.2 Políticas de seguridad de la información

5.2.1 Infraestructura de tecnologías de la información

En esta sección, se establecen las directrices para la gestión y protección de la infraestructura de tecnologías de la información. Estas políticas garantizan la disponibilidad, integridad y seguridad de los sistemas, redes y servidores utilizados en la organización.

- Se deben establecer y mantener servidores de desarrollo, prueba y producción completamente separados, pero con

configuraciones y ambientes similares respecto al sistema operativo y dependencias.

- Los servidores deben utilizar sistema operativo con la versión más reciente y estable, que cuente con los últimos parches comprobados y autorizados por el líder de desarrollo de tecnologías de la información o líder del proyecto.
- Los servidores deben utilizar software con las versiones más estables y actualizadas, comprobadas y autorizadas por el líder de desarrollo de tecnologías de la información o líder del proyecto.
- El acceso a cada entorno debe ser restringido y regulado según el rol del usuario. Se debe aplicar el principio de privilegio mínimo, de acuerdo con el tipo de usuario desarrollador o líder de proyecto.
- Cualquier cambio en el entorno de producción debe ser aprobado previamente por el líder de proyecto mediante un proceso formal de gestión de cambios mediante correos electrónicos, tickets o mediante pull requests con Github.
- Se deben registrar mediante logs todos los accesos e interacciones con los entornos, incluyendo direcciones ip y comandos ejecutados.

- Las pruebas de nuevas funcionalidades o correcciones de errores deben realizarse en el entorno de desarrollo o prueba sin ninguna conexión con los sistemas en producción.
- Se deben utilizar contenedores para la gestión de los proyectos en entornos de desarrollo y prueba, asegurando la portabilidad, aislamiento y consistencia.
- Todos los routers, firewalls y switches deben ser configurados por el personal encargado de redes antes de comenzar a estar operativos. Se deben deshabilitar protocolos y servicios inseguros como Telnet, FTP, SNMP y HTTP.
- El acceso a la configuración de los routers debe estar restringido solo a personal autorizado por el líder de tecnologías de la información.
- El SSID de las redes Wi-Fi corporativas no debe ser público, y las redes para empleados y visitantes deben estar segmentadas.
- Se deben aplicar parches de seguridad y actualizaciones de firmware en routers, firewalls y switches al menos cada tres meses o cuando se detecten vulnerabilidades críticas.
- Todas las configuraciones y cambios realizados en la infraestructura de red deben ser documentados y auditados.

- No se permite el uso de redes Wi-Fi públicas o VPNs no autorizadas para acceder a sistemas críticos de la empresa.
- Se debe realizar una auditoría de red cada seis meses para evaluar configuraciones, accesos y cumplimiento de las políticas establecidas.
- Se deben revisar los logs de eventos y tráfico de red mediante herramientas SIEM para detectar posibles intentos de intrusión, al menos 2 veces por semana.

5.2.2 Desarrollo de tecnologías de la información

En esta sección, se definen las políticas para el desarrollo de tecnologías de la información, asegurando que los sistemas y aplicaciones sean diseñados con estándares de calidad, seguridad y eficiencia, minimizando vulnerabilidades y riesgos.

- La información de clientes o de softwares utilizada en entornos de prueba debe ser clasificada según su nivel de confidencialidad, integridad y disponibilidad, y se debe asegurar que los datos de alta confidencialidad sean protegidos o sustituidos.
- Las credenciales y datos sensibles almacenados en repositorios deben ser depurados, cifrados o utilizados mediante variables de entorno no versionadas.

- Se deben implementar herramientas de escaneo del código fuente como GitLeaks, GitGuardian, SecretLint para detectar, depurar o tratar credenciales expuestas.
- Todas las librerías y dependencias utilizadas en el desarrollo de las aplicaciones deben provenir de fuentes confiables y estar debidamente actualizadas y autorizadas por el líder del proyecto.
- Las aplicaciones no deben revelar información de carácter sensible en mensajes de error y se deben registrar los errores en archivos de logging o en bases de datos.
- Las APIs deben implementar autenticación, autorización y restricciones adecuadas por cada endpoint de acuerdo con el criterio del líder de proyecto.
- No se deben exponer al público en general archivos que muestren los métodos, parámetros o lógica requeridos para el funcionamiento de los proyectos y servidores.
- Las aplicaciones móviles no deben contener datos confidenciales en la memoria más tiempo del necesario (tiempo que dure la operación), y la memoria se debe borrar explícitamente después de su uso.
- En lo posible no almacenar las contraseñas o tokens reusables de seguridad en el dispositivo. En el caso de

requerirlo no se deben guardar en texto claro por lo contrario deben ser almacenadas únicamente en formato cifrado AES-256 o SHA-256 como mínimo.

- El código fuente de la aplicación debe ofuscarse para que el mismo no sea visible al usuario en el caso que se realicen procesos de ingeniería inversa.

5.2.3 Autenticación de usuarios

En esta sección, se establecen las políticas para la autenticación de usuarios, garantizando que el acceso a los sistemas y datos sea seguro, controlado y acorde con los principios de confidencialidad y protección de la información.

- Se deben utilizar protocolos de autenticación seguros como OAuth2, OpenID Connect o MFA para el acceso a las aplicaciones y servicios utilizados por el personal.
- La administración de identidades del personal debe realizarse a través de un sistema de gestión de identidades y accesos (IAM) con auditoría y trazabilidad de accesos tales como: Active Directory, Gravitee Identity Management o Red Hat Identity Management.

- Se deben implementar mecanismos de bloqueo de cuenta y CAPTCHA en los sistemas de autenticación de los proyectos en producción.
- Se deben implementar administradores de contraseñas como ProtonPass, 1Password, Bitwarden o Lastpass para almacenar claves de APIS, tokens y credenciales de servicios de desarrollo y producción.
- Las credenciales nunca deben almacenarse en texto plano en bases de datos o archivos de configuración.
- Las credenciales se deben revocar inmediatamente cuando un usuario cambia de rol, es dado de baja o ya no requiere ciertos permisos.
- Se deben realizar monitoreos periódicos sobre los accesos para identificar cuentas inactivas o privilegios innecesarios, al menos 3 veces al año.
- El cierre de sesión por inactividad tras un periodo de tiempo corto debe ser 5 minutos para aplicaciones que manejan información de alto riesgo como datos de pago o información personal. Para aplicaciones con menor riesgo, se considera aceptable que la sesión se cierre tras un periodo de inactividad de 40 minutos.

5.2.4 Información sensible

En esta sección, se definen las directrices para la gestión y protección de la información sensible, asegurando su confidencialidad, integridad y acceso restringido solo a personas autorizadas.

- No almacenar las claves de usuario en variables permanentes de memoria. La clave del usuario es utilizada únicamente en el proceso de autenticación y no requiere ser guardada en memoria. Luego del proceso de autenticación la clave debe ser inicializada con “null” o utilizar un token de autenticación.
- Los parámetros sensibles que requieren ser enviados hacia otras aplicaciones deben estar cifrados y se los transmitirá únicamente mediante el método POST. Estos parámetros no deben ser visibles para el usuario final.
- Para la ejecución de transacciones financieras como compras, débitos a tarjetas y contratación de servicios, se recomienda un segundo factor de autenticación para verificar la autenticidad del usuario en el sistema antes de ejecutar la transacción.

5.2.5 Bases de Datos

En esta sección, se definen las directrices para la administración segura de las bases de datos, asegurando la confidencialidad, disponibilidad y precisión de la información almacenada.

- No permitir el acceso directo a la base de datos de las aplicaciones mediante usuario root, este acceso debe ser restringido solo para usuarios autorizados.
- Se debe implementar un sistema de monitoreo continuo que registre logs de accesos, consultas, modificaciones y eliminaciones de datos críticos en la base de datos.
- Se deben generar alertas automáticas que se envíen al líder del proyecto para accesos sospechosos, cambios masivos de datos o consultas no autorizadas sobre información sensible.
- El acceso a los registros de los logs debe estar restringido a personal autorizado, y estos deben almacenarse por un período mínimo de 12 meses.
- Se deben realizar revisiones periódicas de los logs y reportes de auditoría para identificar actividades inusuales o potenciales brechas de seguridad en las bases de datos.
- Está prohibido utilizar información de bases de datos de producción en ambientes de desarrollo y pruebas.

5.2.6 Criptografía

En esta sección, se establecen las directrices para el uso de criptografía, asegurando la protección de la información mediante técnicas de cifrado.

- Los datos utilizados en entornos de prueba deben anonimizarse o encriptarse
- Toda información clasificada como sensible o crítica debe ser cifrada en reposo en las bases de datos y en tránsito utilizando algoritmos robustos como AES-256, SHA-256 o TLS 1.2.
- Es mandatorio el uso de certificados digitales emitidos por una entidad externa CA reconocida, para exponer una web al internet; es decir se deben utilizar protocolos seguros basados en TLS para su publicación (HTTPS).
- Los respaldos de bases de datos y archivos críticos deben estar cifrados y almacenados en ubicaciones seguras con control de acceso.
- Está prohibido almacenar claves criptográficas en código fuente o archivos de configuración.
- Se debe utilizar cifrado de extremo a extremo en aplicaciones que transmitan información confidencial o personal de usuarios.

5.2.7 Auditorias

En esta sección, se definen las directrices para la realización de auditorías, permitiendo evaluar el cumplimiento de las políticas de seguridad y detectar posibles vulnerabilidades en los sistemas de información.

- Se deben realizar auditorías de seguridad de la información al menos una vez al año para evaluar el cumplimiento de las políticas, normativas y controles establecidos orientadas a las ISO 27001 y 22301.
- Todas las auditorías deben ser realizadas por personal independiente y autorizado, ya sea interno o externo.
- Se deben establecer procedimientos para que los hallazgos de auditoría sean remediados en un tiempo máximo definido por criticidad.
- Todas las aplicaciones en entorno de prueba y producción deben contar con mecanismos de logging para registrar eventos relevantes en archivos de texto almacenados en el mismo servidor de ejecución.
- Ningún usuario deberá modificar, desactivar y detener los registros de logs establecidos en las aplicaciones.
- Todo registro de log debe considerar registrar la actividad de los usuarios, con la siguiente información básica: Identificador

de Usuario, Terminal Id (Dirección IP o Hostname), Fecha y Hora (Timestamp), Opción o recurso utilizado, Acción, Código de retorno.

5.2.8 Administración de Personal

En esta sección, se establecen las políticas para la gestión del personal, asegurando que todos los empleados cumplan con las normas de seguridad de la información y reciban la capacitación adecuada para mitigar riesgos.

- Todo el equipo de desarrollo debe recibir formación continua de al menos 1 o 2 veces al año en buenas prácticas de seguridad y manejo de vulnerabilidades.
- Se prohíbe compartir contraseñas o credenciales de acceso entre empleados, contratistas o terceros, sin la autorización del líder de proyecto o líder de tecnologías de la información y se debe solicitar mediante un proceso formal vía correo electrónico.
- Todos los dispositivos corporativos deben estar configurados con cifrado de disco completo (BitLocker, FileVault) y contar con software de seguridad actualizado.
- Toda instalación de software en laptops y dispositivos móviles de la empresa debe estar debidamente autorizada por el líder de proyecto y evidenciado mediante correo electrónico.

- En caso de extravío o robo de un dispositivo, el empleado debe notificar de inmediato al área de TI, y es mandatorio aplicar un procedimiento de borrado remoto de datos.
- Todas las cuentas de empleados deben ser desactivadas inmediatamente tras la finalización del contrato o cambio de rol.
- Los empleados deben reportar cualquier incidente de seguridad al área de tecnologías de manera inmediata, sin temor a represalias.

5.2.9 Servicios en la Nube

En esta sección, se definen las políticas para el uso de servicios en la nube, garantizando que los datos y aplicaciones almacenados en plataformas externas de proveedores sean protegidos según los estándares de seguridad establecidos.

- Para cada proyecto se debe implementar un pipeline de integración y despliegue continuo (CI/CD) mediante Gitlab, para los entornos de prueba y producción.
- Se deben realizar pruebas de penetración y escaneo de vulnerabilidades a los servidores en la nube al menos 1 vez al año.

- Todo proveedor de servicio en la nube debe garantizar un nivel de disponibilidad del servicio de al menos 99.8 %.
- La infraestructura de servidores en la nube debe contar con los siguientes controles mínimos de seguridad: Antivirus, Antimalware, Firewalls, Intrusion Prevention Systems (IPS).
- Se deben implementar protocolo seguro (HTTPS) en todas las conexiones entre el cliente y los servicios.
- La comunicación a los servicios de administración de las plataformas de la nube como SSH, Escritorio Remoto RDP entre otros debe realizarse a través de un enlace seguro y privado VPN. No se deben publicar a todos los usuarios de internet.

5.3 Acciones y Políticas para la Gestión de la Continuidad del Negocio

5.3.1 Plan de continuidad del Negocio (BCP)

El plan de continuidad de negocio es un conjunto de procedimientos documentados con información para su uso durante un incidente, con el objetivo de que la organización continue sus operaciones más críticas con los recursos mínimo-requeridos, teniendo en cuenta el impacto y afectación, donde el costo de recuperación juega un papel importante para la continuidad.

El Plan de continuidad del negocio deberá estar formado por los siguientes planes:

- **Plan de emergencia:** donde la respuesta a la emergencia sea inmediata ante cualquier desastre. Ejemplo: Plan de evacuación.
- **Plan de Gestión de Crisis:** donde se detallan estrategias para garantizar una respuesta sistemática ante crisis.
- **Plan de Recuperación de Desastre (DRP):** gestión inicial para asegurar la operación de actividades esenciales con los recursos mínimos aceptables.

5.3.2 Plan de Recuperación de Desastres (DRP)

Se establecerá un Plan de desastre que garantice una respuesta inmediata ante cualquier desastre que afecte la continuidad del negocio. Este plan incluirá:

- Activación de protocolos de contingencia para mitigar interrupciones en servidores, bases de datos y entornos de desarrollo.
- Equipos de respuesta ante incidentes, con roles asignados para restauración de servicios y comunicación con clientes.
- Planes de respaldo y recuperación para código fuente, repositorios y datos críticos, asegurando la integridad del desarrollo.
- Simulacros y pruebas periódicas de recuperación ante fallos en infraestructura Cloud y servidores locales.
- Evaluaciones posts-incidentes para mejorar estrategias y optimizar tiempos de respuesta.

El Plan de Gestión de Crisis establece estrategias para garantizar una respuesta estructurada y eficaz ante incidentes que puedan afectar la operatividad de la empresa. Este plan incluye:

- Activación del Comité de Gestión de Crisis, encargado de coordinar y tomar decisiones estratégicas.
- Protocolos de respuesta escalonada, priorizando la continuidad de los servicios críticos y la comunicación con clientes.

- Planes de contingencia para infraestructura tecnológica, incluyendo recuperación de servidores, bases de datos y código fuente.
- Gestión de la comunicación interna y externa, asegurando transparencia y control en la difusión de información.
- Evaluación post-crisis para identificar fallos, optimizar estrategias y fortalecer la resiliencia organizacional.

El Plan de Recuperación de Desastre (DRP) define las acciones necesarias para restablecer las operaciones esenciales de la empresa con los recursos mínimos aceptables tras un incidente grave. Este plan incluye:

- Identificación de sistemas críticos para priorizar la recuperación de entornos de desarrollo, repositorios de código y bases de datos.
- Estrategias de recuperación rápida, incluyendo activación de servidores de respaldo y restauración de copias de seguridad.
- Procedimientos de continuidad operativa para mantener servicios esenciales con infraestructura temporal o en la nube.

- Roles y responsabilidades asignadas dentro del equipo técnico para ejecutar acciones de mitigación y restauración.
- Pruebas periódicas del DRP para evaluar su eficacia y optimizar los tiempos de recuperación.

5.3.3 Réplicas

Para las réplicas en un DRP, son esenciales para garantizar la continuidad de las operaciones frente a eventos catastróficos. Estas replicas permiten que la información y los sistemas sean duplicados en ubicaciones alternativas, asegurando en que si algún momento existe falla en el sitio principal, la empresa pueda seguir funcionando.

- Tipos de réplicas:

Al momento de elegir un tipo de réplica para la implementación de la continuidad de la operación, se deben tomar en cuenta varios factores como: costo, el giro de negocio y el objetivo a cubrir. Los tipos de replicas más comunes son:

Tabla 16: Tipos de replicaciones

Tipo de replica	Descripción	RPO
Activa - Activa	Ambas ubicaciones operan simultáneamente, permitiendo una recuperación instantánea.	Casi cero
Activa-Pasiva	Una ubicación primaria activa la réplica de datos a un sitio secundario, que se activa en situaciones de falla.	Minutos a horas
Asíncrona	La replicación se realiza con cierto retraso, lo que puede causar perdida de datos recientes en caso de falla	Minutos a horas

5.3.4 Pruebas

- Se deben realizar pruebas de restauración de bases de datos al menos una vez al año o tras cualquier cambio significativo en la infraestructura tecnológica. Se deben considerar distintos escenarios, como:
    - Pruebas de restauración de datos (recuperación desde copias de seguridad).

  - Simulación de desastres para validar la respuesta organizacional.
  - Pruebas de conmutación (failover y failback) en infraestructuras redundantes.
- Se debe desarrollar un cronograma de pruebas con el personal involucrado, asegurando mínima interrupción a las operaciones. Cada prueba debe tener objetivos claros, incluyendo métricas como:
  - Tiempo de recuperación (RTO – Recovery Time Objective).
  - Punto de recuperación (RPO – Recovery Point Objective).
  - Disponibilidad y consistencia de datos restaurados.

- Se debe registrar el resultado de cada prueba, identificando fallos, tiempos de recuperación y áreas de mejora.
- Se debe conservar la documentación en un repositorio seguro y accesible para auditorías internas y externas solo a personal autorizado.
- Si se detectan deficiencias durante las pruebas, se deben actualizar los planes de recuperación y los procedimientos operativos.

- Se deben capacitar regularmente a los equipos involucrados en la ejecución de las pruebas y planes de respuesta.

5.4 Proceso de mejora continua

Una vez establecidas las políticas de seguridad y continuidad del negocio, es fundamental implementar un proceso de mejora continua que garantice su efectividad a lo largo del tiempo. La integración de un ciclo de mejora continua permite evaluar el desempeño de las políticas implementadas, identificar áreas de mejora y realizar ajustes que optimicen la resiliencia y protección de la empresa ante nuevas amenazas y cambios operacionales. Esto no solo permite mantener la vigencia y aplicabilidad de las políticas, sino que también impulsa la evolución constante de las estrategias de seguridad, asegurando que la empresa pueda adaptarse a un entorno tecnológico y de riesgos en constante cambio.

El mantenimiento y la actualización constante de las políticas de seguridad y continuidad del negocio establecidas en el presente trabajo no solo aseguran el cumplimiento con normativas como ISO/IEC 27001 e ISO 22301, sino que también fomentan una cultura organizacional basada en la seguridad y la prevención. A través de auditorías, pruebas de simulación y la capacitación continua del personal, se fortalece la postura de seguridad de la empresa, garantizando su estabilidad y crecimiento

sostenible en un entorno dinámico y competitivo. Además, estas acciones permiten detectar y corregir posibles deficiencias antes de que se conviertan en vulnerabilidades críticas, reduciendo así la exposición a amenazas y mejorando la capacidad de respuesta ante incidentes.

CONCLUSIONES

En base a los resultados del análisis del entorno organizacional, se logró identificar actividades críticas, que sustentan la operatividad de la empresa, tales como análisis de procesos, gestión de información documental y comunicación con partes interesadas. Estas actividades presentaron una alta dependencia de los sistemas informáticos, por lo que requerían una protección prioritaria de la información y la continuidad del negocio.

En relación con la evaluación, permitió obtener una visión integral de los riesgos y vulnerabilidades, tanto tecnológicos como humanos, que podrían afectar la confidencialidad, integridad y disponibilidad de los activos de la información. Entre los hallazgos más relevantes que se pudieron identificar, fueron la carencia de controles de acceso robustos, falla de configuración en los sistemas críticos, ausencia de políticas efectivas y la falta de la concienciación en la seguridad por parte de la organización.

Con base en los hallazgos encontrados, se propuso un diseño de políticas de seguridad alineadas con las normas ISO 27001 e ISO 22301, que permitió establecer un marco sólido para la protección de la información y la continuidad del negocio. Las políticas de seguridad abordaron aspectos fundamentales como la autenticación de usuarios, protección de información sensible en la infraestructura tecnológica, elaboración de un Plan de Continuidad del Negocio (BCP), incorporando medidas de

emergencia y un enfoque de mejora continua, garantizando una gestión estructurada de la seguridad de la información.

Como resultado, se logró un modelo de seguridad robusto que no solo mitiga riesgos, sino que también fortalece la resiliencia de la empresa frente a incidentes y desastres. La integración de ambas normativas facilitó la protección de la información y la continuidad operativa, alineando la seguridad con los objetivos estratégicos de la organización.

RECOMENDACIONES

Se sugiere implementar programas de formación continua para el personal, enfocados en la seguridad de la información y la continuidad del negocio. La concienciación del equipo sobre buenas prácticas y procedimientos de respuesta ante incidentes es fundamental para reducir el riesgo de errores humanos y mejorar la resiliencia organizacional.

Se recomienda establecer un proceso de revisión y actualización continua de las políticas de seguridad diseñadas bajo ISO 27001 e ISO 22301. Esto permitirá adaptar las medidas de protección a los cambios en la infraestructura tecnológica, la evolución de las amenazas y las actualizaciones normativas.

Es conveniente realizar una evaluación continua de la seguridad de los servicios en la nube utilizados por la empresa, asegurando el cumplimiento de estándares de cifrado, control de accesos y monitoreo de actividad. Además, resulta esencial establecer acuerdos con los proveedores para garantizar la protección de los datos alojados en sus plataformas.

Se considera importante que la alta dirección respalde y fomente continuamente la aplicación de las políticas de seguridad y continuidad del negocio, destinando los recursos necesarios para su implementación y

mejora continua. Un liderazgo comprometido fortalecerá la cultura organizacional de seguridad.

BIBLIOGRAFÍA

[1] S. Bartha, R. Ballantine, y D. Aspinall, «Measuring Cyber Essentials Security Policies», en Proceedings of the 17th Cyber Security Experimentation and Test Workshop, en CSET '24. New York, NY, USA: Association for Computing Machinery, 2024, pp. 17-26. doi: 10.1145/3675741.3675747.

[2] M. T. Nguyen y Pavel. B. Khorev, «Information risks in the cloud environment and cloud-based secure information system model», en 2019 International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE), 2019, pp. 1-6. doi: 10.1109/REEPE.2019.8708845.

[3] A. F. P. Anacona, F. J. Pino, S. L. Buitrón, M. Rodríguez, y M. Piattini, «Esquema de certificación por conformidad de requisitos del estándar ISO/IEC 29110 para la calidad de las empresas software», en 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 2020, pp. 1-6. doi: 10.23919/CISTI49556.2020.9141029.

[4] L. Braz y A. Bacchelli, «Software security during modern code review: the developer's perspective», en Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, en ESEC/FSE 2022. New York, NY, USA: Association for Computing Machinery, 2022, pp. 810-821. doi: 10.1145/3540250.3549135.

[5] G. Annunziata, S. Lambiase, F. Palomba, y F. Ferrucci, «SERGE – Serious Game for the Education of Risk Management in Software Project Management», en Proceedings of the 46th International Conference on Software Engineering: Software Engineering Education and Training, en ICSE-SEET '24. New York, NY, USA: Association for Computing Machinery, 2024, pp. 264-273. doi: 10.1145/3639474.3640085.

[6] H. AlKilani y A. Qusef, «OSINT Techniques Integration with Risk Assessment ISO/IEC 27001», en International Conference on Data Science, E-Learning and Information Systems 2021, en DATA'21. New York, NY, USA: Association for Computing Machinery, 2021, pp. 82-86. doi: 10.1145/3460620.3460736.

[7] M. H. Hersyah y Derisma, «A Literature Review on Business Continuity Based on ISO 22301, Six Sigma and Customer Satisfaction Evaluation», en 2018 International Conference on Information Technology Systems and Innovation (ICITSI), 2018, pp. 392-397. doi: 10.1109/ICITSI.2018.8696075.

[8] L. Zhang, X. Fang, Y. Chen, Y. Song, y S. Qian, «Research on business continuity rating model in cloud environment», en 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2021, pp. 1702-1705. doi: 10.1109/IAEAC50856.2021.9390871.

[9] P. Sharma y H. Gupta, «Emerging Cyber Security Threats and Security Applications in Digital Era», en 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future

Directions) (ICRITO), 2024, pp. 1-6. doi: 10.1109/ICRITO61523.2024.10522181.

[10] S. A. Grishaeva y V. I. Borzov, «Information Security Risk Management», en 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 2020, pp. 96-98. doi: 10.1109/ITQMIS51053.2020.9322901.

[11] N. M. A. A. Aziz y D. I. Jambari, «Information Management Procedures for Business Continuity Plan Maintenance», en 2019 International Conference on Electrical Engineering and Informatics (ICEEI), 2019, pp. 489-495. doi: 10.1109/ICEEI47359.2019.8988804.

[12] P. Gomes, G. Cadete, y M. Mira da Silva, «Using Enterprise Architecture to Assist Business Continuity Planning in Large Public Organizations», en 2017 IEEE 19th Conference on Business Informatics (CBI), 2017, pp. 70-78. doi: 10.1109/CBI.2017.30.

[13] L. Zhang, X. Fang, Y. Chen, Y. Song, y S. Qian, «Research on business continuity rating model in cloud environment», en 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2021, pp. 1702-1705. doi: 10.1109/IAEAC50856.2021.9390871.

[14] M. C. Sánchez, J. M. C. de Gea, J. L. Fernández-Alemán, J. Garceran, y A. Toval, «Software vulnerabilities overview: A descriptive study», Tsinghua Sci. Technol., vol. 25, n.o 2, pp. 270-280, 2020, doi: 10.26599/TST.2019.9010003.

[15] J. D. Pereira, J. H. Antunes, y M. Vieira, «A Software Vulnerability Dataset of Large Open Source C/C++ Projects», en 2022 IEEE 27th Pacific Rim International Symposium on Dependable Computing (PRDC), 2022, pp. 152-163. doi: 10.1109/PRDC55274.2022.00029.

[16] S. Reis y R. Abreu, «SECBENCH: A Database of Real Security Vulnerabilities. », en SecSE@ ESORICS, 2017, pp. 69-85.

[17] G. Bhandari, A. Naseer, y L. Moonen, «CVEfixes: automated collection of vulnerabilities and their fixes from open-source software», en Proceedings of the 17th International Conference on Predictive Models and Data Analytics in Software Engineering, en PROMISE 2021. New York, NY, USA: Association for Computing Machinery, 2021, pp. 30-39. doi: 10.1145/3475960.3475985.

[18] V. Lotz, «Cybersecurity Certification for Agile and Dynamic Software Systems – a Process-Based Approach», en 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2020, pp. 85-88. doi: 10.1109/EuroSPW51379.2020.00021.

[19] M. Agreindra Helmiawan, E. Firmansyah, I. Fadil, Y. Sofivan, F. Mahardika, y A. Guntara, «Analysis of Web Security Using Open Web Application Security Project 10», en 2020 8th International Conference on Cyber and IT Service Management (CITSM), 2020, pp. 1-5. doi: 10.1109/CITSM50537.2020.9268856.

[20] A. Selva-Mora y C. Quesada-López, «Security Practices in Agile Software Development: A Mapping Study», en Proceedings of the 7th

ACM/IEEE International Workshop on Software-Intensive Business, en IWSiB ’24. New York, NY, USA: Association for Computing Machinery, 2024, pp. 56-63. doi: 10.1145/3643690.3648241.