Implementación de políticas y procedimientos para minimizar riesgos de pérdida de datos sensibles por configuraciones incorrectas en empresas de desarrollo de software, aplicadas a Culturasoft S.A.S

Yorguin Augusto López Ortiz

Asesor

Eduard Antonio Mantilla Torres

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Especialización en Seguridad Informática

2025

Dedicatoria

Dedico este trabajo a mi familia, especialmente a mis hijos quienes se han convertido en el motor para construir un ejemplo que sea útil en sus vidas.

Agradecimientos

Quiero expresar mi más sincero agradecimiento a mis tutores y profesores de la Universidad Nacional Abierta y a Distancia (UNAD) por su guía y apoyo durante el desarrollo de este proyecto. Agradezco también a mis compañeros de estudio, con quienes compartí este viaje académico, por su colaboración y amistad. Un especial reconocimiento a los expertos y profesionales que, a través de sus conocimientos y experiencias, enriquecieron este trabajo. Finalmente, gracias a Culturasoft S.A.S. por brindarme la oportunidad de aplicar mis conocimientos en un entorno real y por el valioso acceso a los recursos necesarios para llevar a cabo esta investigación.

Resumen

Este proyecto busca establecer políticas y procedimientos de seguridad para reducir los riesgos derivados de configuraciones erróneas en el desarrollo de software. Se centra en la empresa CulturaSoft S.A.S., donde se detectaron fallos significativos que ponían en peligro la protección de datos sensibles. El proyecto aplicado adopta un enfoque basado en normativas internacionales como ISO/IEC 27001 e ISO/IEC 27002, complementado con herramientas de auditoría como Nessus y OpenVAS. Las fases del proyecto incluyen la identificación de configuraciones erróneas, el análisis de políticas existentes, el diseño de estrategias personalizadas y su implementación efectiva. Además, se subraya la importancia de la formación del personal en prácticas seguras y la promoción de una cultura organizacional enfocada en la seguridad. El proyecto ha permitido fortalecer la postura de seguridad de Culturasoft S.A.S., reduciendo riesgos inmediatos y estableciendo una base para mejoras continuas. Este esfuerzo posiciona a la empresa como un referente en seguridad de la información, alineándola con las mejores prácticas internacionales y los requerimientos de sus clientes.

***Palabras clave**:* Auditoría, Implementación, Información, Seguridad, Software.

Abstract

This work aims to implement security policies and procedures to minimize risks associated with misconfigurations in software development projects. It focuses on CulturaSoft S.A.S., a company where critical issues compromising sensitive data security were identified. The research adopts an approach based on international standards such as ISO/IEC 27001 and ISO/IEC 27002, complemented by auditing tools like Nessus and OpenVAS. The project phases include identifying misconfigurations, analyzing existing policies, designing customized strategies, and ensuring their effective implementation. Additionally, the importance of staff training in secure practices and promoting an organizational culture focused on security is emphasized. The project has strengthened CulturaSoft S.A.S.'s security posture, reducing immediate risks and establishing a foundation for continuous improvement. This effort positions the company as a reference in information security, aligning it with international best practices and client requirements

Keywords: Audit, Implementation, Information, Security, Software.

Tabla de contenido

Introducción....13

Planteamiento del problema....15

Descripción del problema....15

Importancia del problema....15

Planteamiento de la pregunta problema....16

Justificación....17

Objetivos....19

Objetivo general....19

Objetivos específicos....19

Marco Referencial....20

Antecedentes....20

Marco conceptual....22

Marco teórico....25

Marco legal....28

Marco contextual....30

Diseño Metodológico....34

Fase 1: Identificación de Configuraciones Incorrectas y Riesgos Asociados....34

Fase 2: Análisis de Políticas Existentes en Empresas Similares....35

Fase 3: Diseño de Políticas y Procedimientos Personalizados 36

Fase 4: Implementación y Evaluación de Políticas y Procedimientos.....36

Configuraciones Incorrectas en Proyectos de Desarrollo de Software.....39

Tipos comunes de Configuraciones Incorrectas 40

Permisos y Control de Acceso.....40

Configuración de Servidores 41

Configuración de Aplicaciones 41

Diagnóstico de la situación actual 41

Análisis del entorno de desarrollo de CulturaSoft S.A.S 42

SSDLC – Ciclo de desarrollo seguro en CulturaSoft 42

Entornos ágiles y su relación con el SSDLC 45

Entornos de Desarrollo 46

Análisis GAP de brechas en seguridad de datos ISO/IEC 27001 48

Métricas 57

Análisis de Políticas y Procedimientos Actuales en Seguridad de Datos.....59

Análisis 59

Recomendaciones 62

Análisis Detallado de Variables Clave 63

Identificación de Variables Clave 63

Evaluación del Impacto de las Variables Clave 65

Priorización de Variables Clave 71

Diseño de Políticas y Procedimientos para la Seguridad de Datos 76

Diseño de Políticas y Procedimientos 76

Metodología para Priorizar Políticas Basadas en Impacto Potencial. 76

Políticas y Procedimientos de Seguridad para CulturaSoft S.A.S. 80

Procedimientos Operativos Estándar (SOPs) 83

Mecanismos de Validación y Socialización 84

Resultados Preliminares de Validación de Hipótesis. 85

Análisis General de los Resultados Preliminares 88

Implementación y Evaluación de Políticas de Seguridad. 89

Implementación Gestión de Acceso y Control de Permisos. 89

Proceso de Gestión de Accesos 89

Explicación del proceso. 90

Implementación Gestión de Configuración y Cambios. 91

Proceso de Gestión de Configuración de Cambios 91

Mecanismos de Implementación 93

Indicadores de Éxito 94

Respuesta a Incidentes de Seguridad. 95

Proceso de Respuesta a Incidentes 95

Capacitación y Evaluación 97

Conclusiones.....99

Recomendaciones.....103

Referencias.....104

Lista de Tablas

Tabla 1 *Requisitos Obligatorios* 49

Tabla 2 *Declaración de Aplicabilidad SoA* 52

Tabla 3 *Métricas* 58

Tabla 4 *Proceso de Gestión de Accesos* 90

Tabla 5 *Tabla de Gestión de Cambios* 93

Tabla 6 *Registro de Incidentes* 96

Lista de Figuras.

Figura 1 *Personal Desarrollo CulturaSoft*.....44

Figura 2 *Personal Desarrollo CulturaSoft*.....44

Figura 3 *Pantallazo de la Plataforma Azure DevOps*.....46

Figura 4 *Ambientes de Desarrollo de CulturaSoft,*.....48

Figura 5 *Gráfico cumplimiento Requisitos SGSI*.....59

Figura 6 *Estructura del Proceso de Gestión de Configuración de Cambios*.....92

Figura 7 *Control de Cambios del Proyecto*.....93

Figura 8 *Automatización de Implementación de parches y funcionalidades*.....94

Figura 9 *Capacitación a funcionarios - Controles de Seguridad*.....98

Figura 10 *Proceso de Evaluación a Desarrolladores*.....98

Lista de Apéndices

Apéndice A *Carta de Autorización*..... 106

Apéndice B *Acuerdo de Confidencialidad*..... 109

Introducción

En el entorno digital actual, la protección de datos sensibles se ha convertido en un imperativo estratégico para empresas de desarrollo de software, independientemente de su tamaño o sector de operación. La creciente dependencia de tecnologías como la computación en la nube, los modelos de Software como Servicio (SaaS) y los entornos ágiles de desarrollo ha incrementado exponencialmente la complejidad de los sistemas informáticos, lo que a su vez ha ampliado la superficie de ataque disponible para actores malintencionados. En este contexto, las configuraciones incorrectas en los sistemas y aplicaciones han emergido como una de las principales causas de vulnerabilidades de seguridad, representando un riesgo significativo para la integridad, confidencialidad y disponibilidad de la información crítica.

Este proyecto tiene como objetivo central implementar políticas y procedimientos efectivos para minimizar los riesgos asociados con la pérdida de datos sensibles debido a configuraciones incorrectas en empresas de desarrollo de software. El enfoque se centra específicamente en Culturasoft S.A.S., una empresa ubicada en Bucaramanga, Colombia, que desarrolla soluciones tecnológicas innovadoras para sus clientes. Culturasoft opera en un entorno competitivo donde la seguridad de la información no solo es un requisito regulatorio, sino también un factor crítico para mantener la confianza de sus clientes y socios comerciales. Sin embargo, un análisis inicial reveló que la empresa enfrenta importantes desafíos en términos de seguridad de la información, particularmente en áreas como la gestión de accesos, la respuesta a incidentes y la documentación de políticas, lo que la hace vulnerable a brechas de seguridad potencialmente devastadoras.

La relevancia de este proyecto radica en la necesidad crítica de fortalecer la postura de seguridad de Culturasoft mediante la estandarización de procedimientos, la capacitación continua

del personal y la evaluación sistemática de riesgos. Las configuraciones incorrectas no solo comprometen la seguridad de los datos, sino que también pueden resultar en interrupciones del servicio, pérdida de productividad y daños reputacionales significativos. Según estudios recientes, como el informe de IBM Security (2020), el costo promedio de una brecha de datos alcanzó los 3.86 millones de dólares, con las configuraciones incorrectas siendo una de las principales causas de estas violaciones. Además, normativas internacionales como el Reglamento General de Protección de Datos (GDPR) en Europa y la Ley de Privacidad del Consumidor de California (CCPA) imponen sanciones severas a las organizaciones que no protegen adecuadamente la información sensible de sus usuarios.

El marco conceptual del proyecto se fundamenta en tres ejes principales: la gestión de riesgos, la seguridad de la información y las mejores prácticas en la configuración de sistemas y software. La gestión de riesgos implica la identificación, evaluación y mitigación de amenazas que podrían afectar negativamente a la organización, mientras que la seguridad de la información abarca un conjunto integral de medidas diseñadas para proteger los datos contra accesos no autorizados, uso indebido, divulgación, alteración y destrucción. Este proyecto busca no solo abordar las configuraciones incorrectas, sino también fomentar una cultura organizacional proactiva y responsable en la protección de datos, alineándose con estándares internacionales como ISO/IEC 27001 e ISO/IEC 27002.

Planteamiento del Problema

Descripción del Problema

Las configuraciones incorrectas en los sistemas de software son una causa común de vulnerabilidades de seguridad que pueden llevar a la exposición y pérdida de datos sensibles. Estas configuraciones erróneas pueden incluir permisos mal configurados, servidores mal asegurados, y aplicaciones mal configuradas, lo que facilita el acceso no autorizado a datos críticos. La creciente complejidad de los entornos de TI y la presión por implementar soluciones rápidamente contribuyen a estos errores (Smith, 2023).

Importancia del Problema

Los problemas de configuración incorrecta han resultado en numerosas brechas de seguridad significativas. Por ejemplo, un estudio realizado por IBM reveló que el costo promedio de una brecha de datos fue de 3.86 millones de dólares en 2020, con la configuración incorrecta siendo una de las principales causas (IBM Security, 2020). Además, la pérdida de datos puede dañar la reputación de una empresa y resultar en sanciones legales y regulatorias, especialmente bajo regulaciones como el GDPR en Europa y el CCPA en California.

Algunos de los factores que contribuyen al problema son:

- Falta de Capacitación: Muchos empleados de TI y desarrolladores no reciben capacitación adecuada en seguridad de la información, lo que aumenta el riesgo de errores de configuración.
- Ausencia de Estándares: La falta de estándares y procedimientos claros para la configuración de sistemas y aplicaciones contribuye a inconsistencias y errores.
- Errores Humanos: La naturaleza humana es propensa a errores, especialmente cuando se trabaja bajo presión o con sistemas complejos.

Un análisis de múltiples estudios académicos y reportes de la industria resalta la prevalencia y el impacto de las configuraciones incorrectas:

- Según el informe "Top Threats to Cloud Computing" de la Cloud Security Alliance, las configuraciones incorrectas son una de las principales amenazas en entornos de nube.
- Un estudio de Verizon sobre brechas de datos en 2021 encontró que el 13% de las brechas eran atribuibles a errores de configuración.

Diferentes empresas del sector han presentado esta problemática en sus proyectos de desarrollo de software, En 2019, Capital One sufrió una brecha de seguridad que expuso datos de 100 millones de clientes debido a una configuración incorrecta en su infraestructura de nube en Amazon Web Services (AWS), En 2021, una configuración incorrecta en los servidores de Microsoft dejó expuestos datos de 250 millones de registros de soporte al cliente

La implementación de políticas y procedimientos efectivos es crucial para minimizar los riesgos asociados con la pérdida de datos sensibles debido a configuraciones incorrectas. Un enfoque integral que incluya la capacitación del personal, la estandarización de procedimientos, y el uso de herramientas de monitoreo y auditoría puede ayudar a mitigar estos riesgos y proteger la información crítica de la empresa

Planteamiento de la Pregunta Problema

¿Cómo la implementación de políticas y procedimientos necesarios puede minimizar los riesgos asociados con la pérdida de datos sensibles debido a configuraciones incorrectas en la empresa CulturaSoft S.A.S?

Justificación

El desarrollo de este proyecto es de vital importancia debido a la creciente amenaza de pérdida de datos sensibles en el ámbito de la tecnología de la información, especialmente en empresas que operan bajo el modelo SaaS. Las configuraciones incorrectas son una de las principales causas de brechas de seguridad, exponiendo a las empresas a riesgos significativos que pueden comprometer la integridad, disponibilidad y confidencialidad de la información (Chen, Desmet & Huygens, 2014). La implementación de políticas y procedimientos sólidos y bien definidos es esencial para mitigar estos riesgos y garantizar un entorno seguro para los datos y aplicaciones.

Además, la conformidad con normativas y estándares internacionales de seguridad de la información, como ISO/IEC 27001 e ISO/IEC 27002, es cada vez más demandada por clientes y socios comerciales (ISO/IEC 27002, 2013). Cumplir con estas normativas no solo mejora la postura de seguridad de la empresa, sino que también fortalece su reputación y confianza en el mercado. Un estudio de la Ponemon Institute (2021) destaca que las organizaciones que adoptan marcos de seguridad robustos experimentan una reducción significativa en el costo de las brechas de datos, lo cual justifica la inversión en este tipo de proyectos.

La implementación de procedimientos y políticas adecuadas también contribuye a la eficiencia operativa. Las configuraciones incorrectas no solo representan riesgos de seguridad, sino que también pueden llevar a interrupciones del servicio y pérdida de productividad (Andress, 2014). Establecer un marco claro para la configuración y gestión de los sistemas permite a empresas con proyectos de software operar de manera más eficiente y con menor riesgo de incidentes imprevistos. Esto es especialmente crítico en un entorno SaaS, donde la disponibilidad y confiabilidad del servicio son factores clave para el éxito.

Finalmente, este proyecto tiene un impacto positivo en la cultura organizacional de las empresas del sector. La formación y concienciación del personal en temas de seguridad es fundamental para crear una cultura proactiva y responsable en la protección de datos (Whitman & Mattord, 2018). Un personal bien capacitado y consciente de las mejores prácticas en seguridad reduce significativamente la probabilidad de errores humanos que puedan llevar a configuraciones incorrectas y, por ende, a brechas de seguridad. La capacitación continua y la implementación de políticas claras fortalecen la resiliencia de la organización frente a amenazas de seguridad emergentes (Schneier, 2015).

El desarrollo de este proyecto no solo aborda una necesidad crítica de mejorar la seguridad de los datos, sino que también aporta beneficios tangibles en términos de conformidad normativa, eficiencia operativa y fortalecimiento de la cultura organizacional. La inversión en políticas y procedimientos de seguridad robustos es una medida proactiva que posiciona a la empresa en una mejor situación para enfrentar los desafíos de seguridad actuales y futuros.

Objetivos

Objetivo General

Implementar políticas y procedimientos efectivos mediante la evaluación de riesgos, la capacitación del personal, la implementación de herramientas de monitoreo y auditoría, y la estandarización de procedimientos de configuración para prevenir la pérdida de datos sensibles debido a configuraciones incorrectas en proyectos de desarrollo de software en la empresa Culturasoft S.A.S. en Bucaramanga, Colombia.

Objetivos Específicos

Identificar las configuraciones incorrectas que afectan la seguridad de los datos en proyectos de desarrollo de software para minimizar riesgos asociados a la exposición de información de los clientes.

Analizar las políticas y procedimientos existentes en empresas de desarrollo de software para minimizar riesgos de pérdida de datos sensibles.

Diseñar políticas y procedimientos personalizados para minimizar riesgos de pérdida de datos sensibles debido a configuraciones incorrectas.

Evaluar la efectividad de las políticas y procedimientos diseñados para CULTURASOFT S.A.S. sobre configuraciones de software para minimizar riesgos de exposición de datos de los clientes.

Marco Referencial

Antecedentes

Las configuraciones incorrectas en sistemas de software han sido una fuente recurrente y crítica de vulnerabilidades de seguridad en la industria tecnológica durante las últimas décadas. Este problema ha evolucionado en complejidad y alcance con el avance de las tecnologías de la información, afectando tanto a grandes corporaciones como a pequeñas y medianas empresas.

Un caso emblemático que marcó un antes y después en la percepción de este riesgo fue la brecha de seguridad de Capital One en 2019 (Pozzi, 2019), donde una mala configuración en su infraestructura de nube Amazon Web Services (AWS) expuso datos personales y financieros de más de 100 millones de clientes. Este incidente no solo representó pérdidas económicas significativas para la institución financiera, sino que también evidenció cómo errores aparentemente menores pueden tener consecuencias devastadoras.

El estudio realizado por IBM Security (2020) sobre el costo de las violaciones de datos reveló que los problemas de configuración son responsables de una proporción considerable de estos incidentes, con un impacto promedio de 3.86 millones de dólares por evento. Este hallazgo coincidió con otros estudios de la industria que comenzaron a destacar las configuraciones incorrectas como una de las principales causas de vulnerabilidades en entornos cloud.

En el contexto colombiano, empresas como CulturaSoft S.A.S. enfrentan desafíos similares al intentar proteger sus activos digitales mientras mantienen la competitividad en el mercado. La falta de estandarización en procesos y la presión por implementar soluciones rápidamente son factores que contribuyen a la aparición de configuraciones inseguras (Gutierrez, 2023).

La evolución hacia modelos de Software como Servicio (SaaS) ha incrementado exponencialmente la superficie de ataque potencial. Según el informe "Top Threats to Cloud Computing" de la Cloud Security Alliance (2020), las configuraciones incorrectas ocupan el primer lugar entre las amenazas más críticas en entornos cloud, superando incluso a amenazas como el acceso no autorizado o el malware.

El análisis comparativo de múltiples estudios académicos e informes industriales revela un patrón preocupante:

- El 13% de las brechas de datos reportadas en 2021 fueron atribuidas directamente a errores de configuración (Verizon DBIR, 2021)
- Las organizaciones que no implementan revisiones regulares de configuración tienen un 60% más de probabilidades de sufrir una violación de datos
- El tiempo promedio para detectar una configuración incorrecta es de 207 días Casos notables adicionales incluyen:

- La exposición de 250 millones de registros de soporte técnico de Microsoft en 2021 debido a servidores mal configurados
- La brecha de datos de Estée Lauder en 2020, que expuso 440 millones de registros por una base de datos Elasticsearch sin protección
- La filtración de datos de MGM Resorts en 2023, resultado de una API mal configurada

Estos antecedentes demuestran la necesidad crítica de establecer políticas y procedimientos robustos que mitiguen estos riesgos. Organizaciones que han implementado marcos formales de gestión de configuraciones han reportado reducciones significativas en

incidentes de seguridad, destacando la importancia de abordar este problema de manera estructurada y proactiva.

La experiencia de empresas que han transitado hacia modelos más maduros de seguridad muestra que la combinación de herramientas automatizadas, procesos documentados y capacitación continua del personal es fundamental para minimizar el riesgo de configuraciones incorrectas. Esta lección aprendida será crucial para guiar la implementación en empresas como CulturaSoft S.A.S.

Marco Conceptual

El marco conceptual de este proyecto se fundamenta en varios pilares fundamentales que permiten comprender y abordar de manera integral la problemática de las configuraciones incorrectas en entornos de desarrollo de software. Estos conceptos clave están interrelacionados y forman la base teórica para el diseño e implementación de políticas y procedimientos efectivos.

Gestión de Riesgos de Seguridad Informática La gestión de riesgos se define como el proceso sistemático de identificación, evaluación y control de los riesgos que podrían afectar negativamente a la organización (Castillo, 2024). En el contexto de este proyecto, la gestión de riesgos contempla varios elementos críticos:

1. Identificación de Activos de Información:
    - Bases de datos de clientes
    - Código fuente de aplicaciones
    - Infraestructura de servidores
    - Documentación técnica

2. Análisis de Amenazas y Vulnerabilidades:

    - Configuraciones incorrectas
    - Acceso no autorizado
    - Divulgación indebida de información
    - Alteración de datos

3. Evaluación del Impacto:

    - Severidad: Baja, Media, Alta, Crítica
    - Probabilidad de ocurrencia
    - Matriz de riesgos

Seguridad de la Información La seguridad de la información comprende el conjunto de medidas y prácticas destinadas a proteger los datos contra accesos no autorizados, uso indebido, divulgación, alteración y destrucción (Ciberseguridad.com, 2024). Para CulturaSoft S.A.S., esto implica:

Modelo CIA (Confidencialidad, Integridad, Disponibilidad):

- Mecanismos de autenticación y cifrado
- Control de integridad de datos
- Planes de continuidad del negocio

Capas de Seguridad:

- Perimetral

- De red
- De aplicación
- De datos

Mejores Prácticas en Configuración de Sistemas y Software Las mejores prácticas en configuración incluyen:

1. Principios Fundamentales:
    - Principio de mínimo privilegio
    - Separación de ambientes
    - Control de cambios documentado
2. Estándares de Configuración:
    - CIS Benchmarks
    - Políticas de contraseñas seguras
    - Configuración de firewalls y DMZs
3. Procesos de Verificación:
    - Escaneo de vulnerabilidades
    - Auditorías regulares
    - Monitoreo continuo

Políticas y Procedimientos de Seguridad Las políticas establecen directrices generales mientras que los procedimientos detallan pasos específicos:

La política debe contemplar dentro de su estructura Objetivo, Alcance, Responsabilidades, Requisitos, Indicadores de cumplimiento y procedimientos operativos como son la gestión de accesos, control de cambios, respuesta a incidentes y copias de seguridad.

Cultura de Seguridad Organizacional La creación de una cultura de seguridad implica:

Elementos Clave: Compromiso de la alta dirección, Capacitación continua, Comunicación efectiva, Métricas de desempeño y contemplar mecanismos de Implementación como: Programas de inducción, Simulaciones de incidentes, Evaluaciones periódicas, Reconocimientos y sanciones

Estos conceptos están interrelacionados y forman la base para el desarrollo de soluciones efectivas en seguridad de la información. La gestión de riesgos provee el marco para identificar y priorizar problemas, mientras que la seguridad de la información establece los objetivos específicos de protección. Las mejores prácticas en configuración aseguran la implementación técnica adecuada, y las políticas con sus respectivos procedimientos garantizan la operatividad y consistencia. Finalmente, la cultura organizacional permite la adopción efectiva y sostenible de todas estas medidas.

Marco Teórico

El marco teórico que sustenta este proyecto se fundamenta en diversos conceptos y teorías relacionadas con las prácticas de seguridad de la información en entornos de software como servicio (SaaS). Las configuraciones incorrectas representan una de las principales causas de vulnerabilidades de seguridad, situación que puede derivarse de múltiples factores incluyendo errores humanos, falta de conocimiento técnico adecuado o la ausencia de procedimientos claros y estandarizados (Zscaler, 2023).

La gestión de configuraciones en entornos SaaS requiere un enfoque integral que considere tanto los aspectos técnicos como los procesos organizacionales. Gutierrez enfatiza en 2023 que las empresas que operan bajo este modelo enfrentan desafíos únicos debido a la naturaleza dinámica y distribuida de sus infraestructuras tecnológicas. La implementación de políticas y procedimientos de seguridad constituye un componente fundamental en esta ecuación, donde las políticas establecen las directrices generales para la protección de la información mientras que los procedimientos detallan los pasos específicos necesarios para materializar dichas directrices en la práctica operativa diaria (Gutierrez, 2023).

Las herramientas de auditoría y análisis juegan un papel crucial en la identificación y corrección de configuraciones incorrectas. Soluciones como Nessus, OpenVAS y Nmap permiten realizar evaluaciones sistemáticas de las infraestructuras tecnológicas, detectando puntos débiles y áreas susceptibles de mejora (Smith & colaboradores, 2023). Estas herramientas no solo facilitan la identificación de vulnerabilidades existentes, sino que también contribuyen a establecer métricas objetivas sobre el estado de seguridad de los sistemas, lo cual es fundamental para el monitoreo continuo y la mejora progresiva de las posturas de seguridad.

El concepto de mínimo privilegio emerge como un principio fundamental en la gestión de accesos y permisos dentro de los sistemas de software. Castillo señala en 2024 que la implementación efectiva de este principio requiere no solo la definición clara de roles y responsabilidades sino también la creación de mecanismos de control que aseguren el cumplimiento continuo de esta política (Castillo, 2024). Este enfoque reduce significativamente la superficie de ataque potencial al limitar el acceso a recursos críticos únicamente a aquellos usuarios que realmente lo requieren para el desempeño de sus funciones.

La respuesta a incidentes de seguridad representa otro pilar fundamental en la construcción de una postura de seguridad robusta. El marco teórico desarrollado por Ciberseguridad.com en 2024 destaca la importancia de establecer procedimientos claros y bien documentados para la gestión de incidentes, asegurando que la organización pueda responder de manera efectiva ante cualquier eventualidad (Ciberseguridad.com, 2024). Este proceso incluye desde la detección inicial del incidente hasta su resolución final, pasando por etapas críticas de análisis, clasificación y escalado según la severidad del evento.

El análisis de riesgos constituye un elemento transversal que permea todos los aspectos de la seguridad de la información. La metodología propuesta por IBM en 2023, basada en el marco del NIST, proporciona una estructura sistemática para identificar, evaluar y tratar los riesgos asociados con la seguridad de la información (IBM, 2023). Este enfoque permite priorizar las acciones de mitigación según su impacto potencial y probabilidad de ocurrencia, optimizando así la asignación de recursos y esfuerzos en materia de seguridad.

La integración de estos conceptos teóricos en un marco coherente permite abordar de manera integral la problemática de las configuraciones incorrectas en entornos de desarrollo de software. La combinación de principios fundamentales de seguridad, herramientas de auditoría especializadas y procedimientos bien definidos crea una base sólida para el desarrollo e implementación de políticas efectivas de seguridad de la información (TechOne & Sanchez, 2023).

La formación y concientización del personal emerge como un componente crucial en este marco teórico. Smith y colaboradores destacan en 2023 que los factores humanos representan una de las principales fuentes de configuraciones incorrectas, subrayando la necesidad de implementar programas de capacitación continuos que mantengan al personal actualizado sobre

las mejores prácticas en seguridad de la información (Smith & colaboradores, 2023). Esta dimensión humana del problema complementa los aspectos técnicos y procedimentales, creando un enfoque holístico que aborda las causas raíz de las configuraciones defectuosas.

Marco Legal

El marco legal que sustenta este proyecto se encuentra alineado con normativas y estándares internacionales que establecen los lineamientos fundamentales para la gestión de la seguridad de la información. Estas regulaciones no solo proporcionan un marco estructurado para la implementación de medidas de seguridad, sino que también definen las responsabilidades y obligaciones de las organizaciones en la protección de datos sensibles (Cynthus, 2023).

La norma ISO/IEC 27001 se constituye como uno de los pilares fundamentales en la gestión de la seguridad de la información, estableciendo requisitos para implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Esta normativa es especialmente relevante para empresas como CulturaSoft S.A.S., ya que proporciona un enfoque sistemático para identificar, evaluar y tratar los riesgos asociados con la seguridad de la información (IBM, 2023). La adopción de este estándar no solo mejora la postura de seguridad de la organización, sino que también demuestra su compromiso con prácticas reconocidas internacionalmente.

El estándar ISO/IEC 27002 complementa la norma ISO/IEC 27001 al proporcionar directrices detalladas sobre controles de seguridad específicos que deben implementarse para proteger la información. Este documento sirve como referencia fundamental para el diseño e implementación de políticas y procedimientos de seguridad, asegurando que las medidas adoptadas estén alineadas con las mejores prácticas de la industria (Ciberseguridad.com, 2024).

La combinación de estos dos estándares permite a las organizaciones no solo cumplir con requisitos normativos, sino también fortalecer su capacidad para proteger activos críticos.

El marco del NIST SP 800-30 representa otro componente crucial en el ámbito legal y regulatorio, proporcionando una metodología estructurada para la evaluación de riesgos en sistemas de información. Este marco establece procedimientos claros para identificar, estimar y analizar riesgos, lo cual es fundamental para priorizar las acciones de mitigación y asignar recursos de manera efectiva (IBM, 2023). La implementación de esta metodología permite a las organizaciones desarrollar una comprensión profunda de sus riesgos de seguridad y tomar decisiones informadas sobre cómo abordarlos.

El Reglamento General de Protección de Datos (GDPR) de la Unión Europea establece requisitos estrictos para la protección de datos personales, imponiendo obligaciones significativas a las organizaciones que manejan información de ciudadanos europeos. Este reglamento no solo define principios fundamentales para el tratamiento de datos personales, sino que también establece sanciones severas para el incumplimiento, lo cual subraya la importancia crítica de implementar medidas adecuadas de protección de datos (Cynthus, 2023). La Ley de Privacidad del Consumidor de California (CCPA) establece regulaciones similares para el mercado estadounidense, creando un marco legal que protege los derechos de los consumidores respecto a sus datos personales.

La implementación de estos marcos regulatorios requiere un enfoque integral que considere tanto los aspectos técnicos como organizacionales de la seguridad de la información. El marco COBIT 5, aunque principalmente enfocado en la gobernanza de TI, proporciona un conjunto valioso de directrices para alinear las prácticas de seguridad con los objetivos empresariales, asegurando que las inversiones en seguridad generen valor tangible para la

organización (IBM, 2023). Este enfoque integral es especialmente relevante en entornos de desarrollo de software, donde la complejidad técnica debe equilibrarse con la necesidad de cumplimiento normativo.

La aplicación práctica de estas normativas y estándares requiere la implementación de procesos documentados y verificables que aseguren el cumplimiento continuo de los requisitos legales y regulatorios. Esto incluye no solo la definición de políticas formales, sino también la implementación de mecanismos de monitoreo y auditoría que permitan verificar el cumplimiento de manera regular (Ciberseguridad.com, 2024). La falta de documentación adecuada y la ausencia de procesos formalizados representan riesgos significativos de incumplimiento, lo cual puede resultar en sanciones legales y daños reputacionales.

La convergencia de estos marcos regulatorios crea un entorno donde las organizaciones deben demostrar no solo el cumplimiento técnico de los requisitos, sino también la efectividad de sus controles de seguridad a través de auditorías y evaluaciones periódicas. Esta necesidad de verificación constante refuerza la importancia de implementar herramientas de monitoreo automatizado y procesos de auditoría estructurados que permitan mantener un estado de cumplimiento continuo (IBM, 2023). Además, la evolución constante del panorama regulatorio requiere que las organizaciones mantengan una postura proactiva en la actualización de sus políticas y procedimientos para adaptarse a nuevos requisitos y amenazas emergentes.

Marco Contextual

marco conceptual que sustenta este proyecto se fundamenta en varios pilares fundamentales que permiten comprender y abordar de manera integral la problemática de las configuraciones incorrectas en entornos de desarrollo de software. Estos conceptos clave están

interrelacionados y forman la base teórica para el diseño e implementación de políticas y procedimientos efectivos (Castillo, 2024).

La gestión de riesgos emerge como un elemento central en este marco conceptual, definiéndose como el proceso sistemático de identificación, evaluación y control de los riesgos que podrían afectar negativamente a la organización, especialmente en el contexto de la seguridad de la información. Este proceso incluye no solo la identificación de activos críticos como bases de datos de clientes y código fuente de aplicaciones, sino también el análisis de amenazas y vulnerabilidades específicas que podrían comprometer estos activos. La matriz de riesgos desarrollada permite priorizar las acciones de mitigación según su impacto potencial y probabilidad de ocurrencia, optimizando así la asignación de recursos y esfuerzos en materia de seguridad (IBM, 2023).

La seguridad de la información se constituye como otro pilar fundamental del marco conceptual, comprendiendo el conjunto de medidas y prácticas destinadas a proteger los datos contra accesos no autorizados, uso indebido, divulgación, alteración y destrucción. Este concepto se materializa a través del modelo CIA (Confidencialidad, Integridad, Disponibilidad), donde cada componente representa una dimensión crítica de la protección de la información. La implementación de mecanismos de autenticación y cifrado asegura la confidencialidad, mientras que los controles de integridad de datos garantizan que la información no sea alterada sin autorización, y los planes de continuidad del negocio aseguran su disponibilidad (Ciberseguridad.com, 2024).

Las mejores prácticas en configuración de sistemas y software forman un tercer componente crucial del marco conceptual, estableciendo estándares mínimos que deben cumplirse para mantener un entorno seguro. El principio de mínimo privilegio se erige como una

directriz fundamental, limitando el acceso a recursos críticos únicamente a aquellos usuarios que realmente lo requieren para el desempeño de sus funciones. La separación de ambientes de desarrollo, prueba y producción se convierte en una práctica esencial para minimizar el riesgo de exposición de datos sensibles durante las diferentes fases del ciclo de vida del software (TechOne & Sanchez, 2023).

Los procesos de auditoría y análisis juegan un papel crucial en la verificación continua del cumplimiento de estas mejores prácticas, proporcionando métricas objetivas sobre el estado de seguridad de los sistemas. Herramientas especializadas como Nessus, OpenVAS y Nmap permiten realizar evaluaciones sistemáticas de las infraestructuras tecnológicas, detectando puntos débiles y áreas susceptibles de mejora. Estas herramientas no solo facilitan la identificación de vulnerabilidades existentes sino que también contribuyen a establecer un sistema de monitoreo continuo que asegure el mantenimiento de los estándares de seguridad (Smith & colaboradores, 2023).

La formación y concientización del personal emerge como un componente transversal que permea todos los aspectos del marco conceptual. Los factores humanos representan una de las principales fuentes de configuraciones incorrectas, subrayando la necesidad de implementar programas de capacitación continuos que mantengan al personal actualizado sobre las mejores prácticas en seguridad de la información. Esta dimensión humana del problema complementa los aspectos técnicos y procedimentales, creando un enfoque holístico que aborda las causas raíz de las configuraciones defectuosas (Moest, 2023).

La integración de estos conceptos en un marco coherente permite abordar de manera integral la problemática de las configuraciones incorrectas en entornos de desarrollo de software. La combinación de principios fundamentales de seguridad, herramientas de auditoría

especializadas y procedimientos bien definidos crea una base sólida para el desarrollo e implementación de políticas efectivas de seguridad de la información. Esta integración teórico-práctica resulta especialmente relevante en el contexto actual donde la creciente complejidad de los sistemas y la presión por implementar soluciones rápidamente aumentan significativamente el riesgo de configuraciones defectuosas al momento de la implementación (Gutierrez, 2023).

Diseño Metodológico

La metodología que se propone está alineada con los objetivos generales y específicos definidos para garantizar una implementación efectiva de políticas y procedimientos que reduzcan los riesgos de pérdida de datos sensibles. Se combinan marcos normativos como ISO 27001 y NIST SP 800-30, herramientas de auditoría como Nessus y Nmap, y un enfoque de análisis GAP para asegurar un control exhaustivo de las configuraciones de software. El enfoque será mixto, combinando metodologías cuantitativas y cualitativas.

Fase 1: Identificación de Configuraciones Incorrectas y Riesgos Asociados

Objetivo Específico: Identificar las configuraciones incorrectas que afectan la seguridad de los datos en proyectos de desarrollo de software para minimizar riesgos asociados a la exposición de información de los clientes

1. Revisión Documental y Análisis de Casos:
    - Análisis de estándares relevantes (ISO 27001, ISO 27002, NIST SP 800-53) para identificar las mejores prácticas en seguridad de software.
    - Revisión de casos de pérdida de datos en otras empresas, identificando patrones y riesgos comunes.
2. Auditoría de Configuraciones Actuales (Nessus, Nmap y OpenVAS):
    - Nessus y OpenVAS: Escaneo de vulnerabilidades en servidores y sistemas críticos, detectando configuraciones débiles (por ejemplo, puertos abiertos innecesarios).
    - Nmap: Mapeo de la red para identificar hosts activos, servicios expuestos y configuraciones de acceso.
    - Indicadores de Riesgo:

    - Número de configuraciones incorrectas detectadas.
    - Severidad de las vulnerabilidades (baja, media, alta, crítica).

3. Análisis GAP:
    - Comparación entre las configuraciones actuales y las mejores prácticas definidas en los estándares ISO/NIST.
    - Identificación de brechas que podrían comprometer la seguridad de los datos.
4. Evaluación de Riesgos (NIST SP 800-30):
    - Identificación de activos críticos (por ejemplo, bases de datos de clientes).
    - Análisis de amenazas y vulnerabilidades específicas para cada activo.
    - Matriz de riesgos para priorizar las configuraciones incorrectas más críticas.

Fase 2: Análisis de Políticas Existentes en Empresas Similares

Objetivo específico: Analizar políticas y procedimientos implementados en empresas similares para minimizar riesgos de pérdida de datos sensibles.

1. Entrevistas y Encuestas:
    - Encuestas y entrevistas a expertos de empresas de desarrollo de software en Bucaramanga para identificar políticas y procedimientos exitosos relacionados con configuraciones seguras y protección de datos.
    - Evaluación de los procedimientos de respuesta a incidentes en uso.
2. Análisis Comparativo:
    - Comparación de las políticas revisadas con los requisitos normativos de ISO 27001 y las configuraciones actuales de CULTURASOFT.
    - Identificación de áreas de mejora para adoptar las mejores prácticas relevantes a la empresa.

Fase 3: Diseño de Políticas y Procedimientos Personalizados

Objetivo específico: Diseñar políticas y procedimientos personalizados para minimizar riesgos asociados con configuraciones incorrectas.

1. Definición de Políticas Personalizadas:
    - Elaboración de políticas de seguridad específicas para CULTURASOFT, alineadas con los resultados de las fases anteriores.
2. Desarrollo de Procedimientos Operativos Estándar (SOPs):
    - Redacción de SOPs detallados que cubran:
        - Procedimientos de configuración segura.
        - Procesos de auditoría y monitoreo continuo.
        - Respuesta rápida a incidentes de seguridad.
3. Validación de las Políticas:
    - Revisión de las políticas diseñadas con expertos internos y externos para asegurar su viabilidad y alineación con los objetivos organizacionales.

Fase 4: Implementación y Evaluación de Políticas y Procedimientos

Objetivo específico: Implementar y evaluar la efectividad de las políticas y procedimientos diseñados para CULTURASOFT S.A.S. sobre configuraciones de software para minimizar riesgos de exposición de datos de los clientes

1. Capacitación del Personal:
    - Programa de capacitación para todos los empleados, asegurando la comprensión de las nuevas políticas.
    - Uso de talleres, seminarios y módulos en línea para formar al personal en configuraciones seguras y gestión de incidentes.

- Indicadores de éxito:
    - Número de empleados capacitados.
    - Nivel de satisfacción con los contenidos de la capacitación (evaluado mediante encuestas).

2. Implementación Gradual de las Políticas:
    - Cronograma de implementación: Establecer un plan detallado con fechas y responsables para cada política y procedimiento.
    - Integración de herramientas de monitoreo (Nessus, OpenVAS) para asegurar el cumplimiento de las configuraciones seguras.
    - Métricas:
        - Porcentaje de políticas implementadas dentro del plazo.
        - Reducción de configuraciones incorrectas tras la implementación.
3. Monitoreo y Auditoría Continua:
    - Implementación de monitoreo continuo para detectar configuraciones incorrectas en tiempo real mediante herramientas como Nessus y Nmap.
    - Auditorías periódicas para asegurar el cumplimiento de los procedimientos establecidos.
4. Evaluación de Impacto:
    - Medición de la reducción de incidentes de seguridad tras la implementación de las políticas.
    - Análisis de tendencias en las vulnerabilidades detectadas antes y después de la implementación.
    - Indicadores de Impacto:

    - Número de incidentes evitados.
    - Porcentaje de reducción en la exposición de datos sensibles.

5. Encuestas de Satisfacción del Personal:
    - Evaluación del nivel de comprensión y adopción de las políticas mediante encuestas.
    - Identificación de áreas que requieran ajustes o mayor capacitación.
6. Plan de Mejora Continua:
    - Definición del plan de mejora continua que incluya revisión periódica de las políticas y procedimientos en función de los resultados de las auditorías y encuestas.
    - Actualización de políticas en caso de cambios en el entorno normativo o tecnológico.

Configuraciones Incorrectas en Proyectos de Desarrollo de Software

Las configuraciones incorrectas representan una de las amenazas más persistentes y dañinas en el ámbito de la seguridad informática, afectando cada etapa del ciclo de vida del desarrollo de software. Desde el diseño inicial hasta el despliegue y la operación, cada decisión de configuración tiene el potencial de fortalecer o debilitar la postura de seguridad de un sistema. Estas configuraciones abarcan un amplio espectro, desde errores simples, como no modificar configuraciones por defecto, hasta fallas más complejas, como la incorrecta implementación de controles de acceso o la exposición inadvertida de servicios sensibles.

En entornos modernos de desarrollo, que frecuentemente incluyen la adopción de tecnologías en la nube, la complejidad y dinamismo de los sistemas amplifican los riesgos asociados con configuraciones incorrectas. La computación en la nube, por ejemplo, ofrece ventajas como escalabilidad y flexibilidad, pero también introduce nuevas superficies de ataque. Las configuraciones predeterminadas en servicios en la nube, si no se revisan y ajustan adecuadamente, pueden dejar puertas abiertas que los atacantes pueden explotar. En este contexto, un informe de la Cloud Security Alliance titulado "Top Threats to Cloud Computing" destaca que las configuraciones incorrectas son una de las amenazas más críticas que enfrentan las organizaciones que migran a la nube (Cloud Security Alliance, 2020). Esta amenaza no solo se refiere a la configuración técnica de los recursos en la nube, sino también a cómo se manejan las identidades y accesos, la gestión de datos y la integración de aplicaciones.

Además, la transición a entornos de DevOps y la automatización continua en el desarrollo de software, mientras mejora la eficiencia, también puede aumentar el riesgo de errores de configuración. Los sistemas automatizados y las integraciones continuas requieren configuraciones precisas y coherentes; cualquier desajuste o error en los scripts de

automatización puede propagarse rápidamente a lo largo de todo el entorno de producción. Este riesgo es evidente en el "Data Breach Investigations Report" de Verizon, que señala que el 13% de las brechas de datos reportadas en 2021 fueron causadas directamente por errores de configuración (Verizon, 2021). Esto resalta la importancia de la configuración adecuada, no solo para proteger datos, sino también para asegurar que los procesos automatizados no introduzcan nuevas vulnerabilidades.

En cuanto a la gestión de permisos y credenciales, otro aspecto crítico es la creciente adopción de microservicios y arquitecturas distribuidas, donde la gestión adecuada de los secretos (como claves API y contraseñas) se vuelve aún más compleja. Los errores en la configuración de permisos pueden resultar en la exposición no solo de aplicaciones individuales, sino de toda la infraestructura subyacente, lo que podría permitir a los atacantes moverse lateralmente dentro del entorno comprometido.

Las configuraciones incorrectas son una preocupación transversal en todos los aspectos del desarrollo de software, especialmente en el contexto moderno donde la nube y la automatización están cada vez más presentes. La identificación y corrección temprana de estas configuraciones son esenciales para evitar que se conviertan en puntos de vulnerabilidad explotables por actores malintencionados, protegiendo así los datos y la integridad de los sistemas desarrollados.

Tipos comunes de Configuraciones Incorrectas

Permisos y Control de Acceso

Uno de los errores más comunes y críticos es la configuración incorrecta de permisos y control de acceso. Esto puede incluir la asignación de permisos excesivos a usuarios o roles que no requieren acceso a ciertos datos o funcionalidades, lo que facilita la posibilidad de accesos no

autorizados. Un estudio de (Verizon, 2021) encontró que el 13% de las brechas de datos eran atribuibles a errores de configuración, donde los permisos mal gestionados jugaron un papel significativo.

Configuración de Servidores

La configuración incorrecta de servidores es otra fuente importante de vulnerabilidades. Ejemplos de esto incluyen servidores web con configuraciones por defecto que no están debidamente aseguradas, o la falta de cifrado en la comunicación entre servidores. Este tipo de errores fue central en la brecha de seguridad sufrida por Capital One en 2019 (Capital One, 2019), donde una configuración incorrecta en su infraestructura de nube permitió la filtración de datos de más de 100 millones de clientes.

Configuración de Aplicaciones

Las aplicaciones, especialmente aquellas que interactúan con bases de datos o sistemas de terceros, también son susceptibles a configuraciones incorrectas. Esto puede incluir la exposición innecesaria de interfaces de administración, la falta de validación de entradas o la gestión inapropiada de claves de API y otras credenciales sensibles. Las configuraciones predeterminadas o la falta de personalización a las necesidades específicas del entorno de producción son aspectos que contribuyen a estas vulnerabilidades.

Diagnóstico de la Situación Actual

CulturaSoft S.A.S. es una empresa de desarrollo de software que se enfoca en la creación de soluciones tecnológicas innovadoras para sus clientes. Sin embargo, al igual que muchas empresas en el sector, CulturaSoft enfrenta desafíos en términos de seguridad de la información y protección de datos sensibles.

La empresa tiene desarrollos activos para clientes a nivel nacional siendo uno de esos proyectos INFIINITES el cual es una plataforma integrada de servicios, igualmente tiene proyectos que ya están en producción, pero sobre los cuales hay desarrollos activos como es el caso de SICMAWEB una solución para Empresas de Servicios Públicos domiciliarios que integra módulos Comercial, Financiero, Ventanilla única, Recurso Humano, Almacén y Activos fijos. Sobre los dos productos mencionados se desarrollará el proyecto aplicado.

Análisis del Entorno de Desarrollo de CulturaSoft S.A.S

CULTURASOFT S.A.S es una empresa joven enfocada en el desarrollo de software para lo cual ha implementado procesos y procedimientos enfocados al desarrollo de los diferentes componentes y la administración de los equipos con base en conceptos modernos.

El representante legal de la empresa manifiesta “Desde la administración se hace un gran esfuerzo para garantiza a nuestros clientes que el desarrollo de sus proyectos cumpla con estándares de calidad y seguridad, por esto se ha iniciado la implementación de ciclos de desarrollo seguro, DevOps y políticas de protección de datos desde la contratación del personal.”. En una revisión de los procesos de CULTURASOFT se ha identificado que la empresa no tiene un análisis de brecha con respecto a estándares como la ISO 27001.

SSDLC – Ciclo de Desarrollo Seguro en CulturaSoft

El Ciclo de Vida de Desarrollo de Software Seguro (SSDLC, por sus siglas en inglés) es un marco estructurado que guía el proceso de creación de software desde su concepción hasta su retiro. Este ciclo se compone de varias fases, cada una con objetivos específicos y actividades detalladas que aseguran la calidad y seguridad del producto final. La implementación de un SDLC seguro es crucial para las empresas que ofrecen servicios de software bajo el modelo SaaS, ya que garantiza la protección de datos y la integridad del sistema (Pressman, 2014).

1 Planificación y Análisis de Requisitos: En esta fase inicial, se identifican las necesidades del cliente y se definen los requisitos del software. Se realiza un análisis de riesgos para identificar posibles amenazas y vulnerabilidades desde el principio.

2 Diseño: Se elabora un diseño detallado del software, incluyendo la arquitectura del sistema y los componentes de seguridad necesarios. Esta fase incluye la creación de diagramas de flujo, modelos de datos y especificaciones técnicas.

3 Desarrollo: Los desarrolladores escriben el código del software siguiendo las especificaciones del diseño. Se implementan controles de seguridad como la validación de entradas, la gestión de sesiones y la encriptación de datos.

4 Pruebas: Se realizan pruebas exhaustivas para identificar y corregir errores y vulnerabilidades. Las pruebas incluyen pruebas unitarias, de integración, de sistema y de penetración.

5 Despliegue: El software se despliega en el entorno de producción. Se implementan medidas de seguridad adicionales, como la configuración de firewalls y sistemas de detección de intrusiones.

6 Mantenimiento: Se monitorea el software en busca de problemas y se realizan actualizaciones y parches de seguridad según sea necesario. Esta fase es continua y asegura que el software permanezca seguro y funcional a lo largo del tiempo CULTURASOFT en su proceso de desarrollo de Software contempla todos los requisitos

generales del SDLC teniendo en cuenta la planificación y análisis de requisitos, incluyendo en ellos aspectos de seguridad y requisitos arquitectónicos que contemplan aspectos de la seguridad contemplados en la ISO 27001, pero falta mayor implementación y control.

También se evidencia que no existe documentación al respecto y que el proceso no ha sido socializado en debida forma, si bien el personal ha sido enterado no se han definido roles ni se hay evidencia de las capacitaciones y socializaciones del proceso.

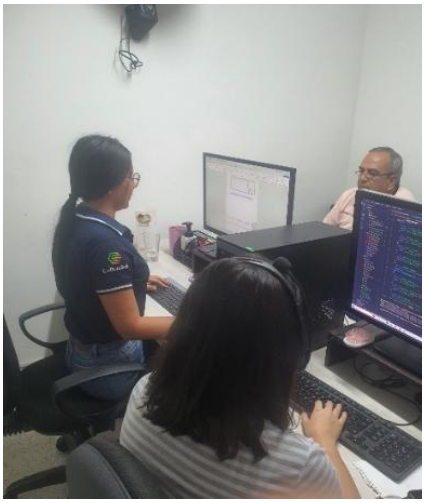
Figura 1

Personal Desarrollo CulturaSoft

Nota. Personal de desarrollo sin trabajando sin especificación de roles.

Figura 2

Personal Desarrollo CulturaSoft



Nota. Personal de documentación y soportes sin definición de roles.

Entornos ágiles y su Relación con el SSDLC

Los entornos ágiles de desarrollo se caracterizan por su flexibilidad y capacidad de adaptación a cambios rápidos. La metodología ágil se centra en la entrega continua de pequeñas mejoras incrementales, lo que permite a los equipos de desarrollo responder rápidamente a las necesidades del cliente y a los cambios en el mercado. Esta metodología se integra perfectamente con el SDLC, proporcionando un marco que asegura tanto la calidad como la seguridad del software (Schwaber, 2014).

1 Iteraciones Cortas: En lugar de seguir un ciclo de vida largo y lineal, los equipos ágiles trabajan en iteraciones cortas llamadas Sprint. Cada sprint incluye todas las fases del SDLC, desde la planificación hasta el despliegue.

2 Colaboración y Comunicación: La metodología ágil fomenta la colaboración constante entre los miembros del equipo y con los clientes. Las reuniones diarias y las revisiones de sprint aseguran que todos estén alineados y que los problemas se aborden rápidamente.

3 Entrega Continua: La entrega continua es un principio clave en los entornos ágiles. Los equipos liberan versiones funcionales del software al final de cada sprint, lo que permite una retroalimentación rápida y la implementación de mejoras de manera continua.

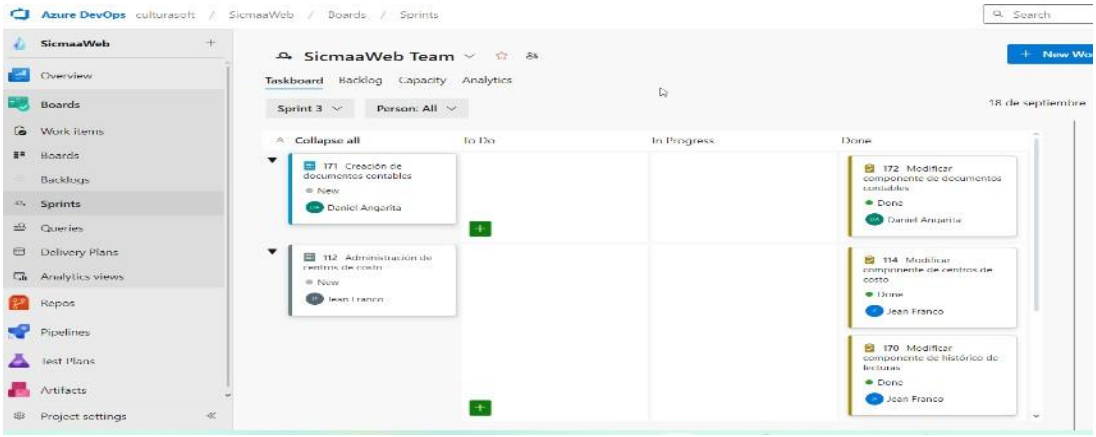
4 Integración de Seguridad: En un entorno ágil, la seguridad se integra en cada fase del desarrollo. Las pruebas de seguridad se realizan de manera continua y se implementan prácticas de desarrollo seguro desde el inicio.

CULTURASOFT ha implementado dos entornos ágiles los cuales se usan de acuerdo al proyecto y su estado, usa Scrum para proyecto nuevos en los cuales tiene el control de todo el ciclo de vida y Kanban para proyectos que están en mantenimiento y sobre los cuales solo

gestionan incidencia o tareas puntuales. Para el control de los dos entornos ágiles hace uso de la herramienta Azure DevOps.

Figura 3

Pantallazo de la Plataforma Azure DevOps



Nota. Captura de pantalla del software usado para el control de tareas.

Entornos de Desarrollo

La implementación de entornos de desarrollo es un proceso crítico para las empresas que ofrecen servicios SaaS. Un entorno de desarrollo bien configurado facilita el trabajo de los desarrolladores, mejora la calidad del software y reduce el tiempo de comercialización (Sommerville, 2011).

1 Entorno de Desarrollo Local: Este es el entorno donde los desarrolladores escriben y prueban su código. Incluye herramientas como editores de código, sistemas de control de versiones y entornos de ejecución locales.

2 Entorno de Pruebas: Aquí se realizan pruebas más exhaustivas del software. Este entorno replica el entorno de producción lo más fielmente posible para identificar y corregir problemas antes del despliegue.

3 Entorno de Integración Continua: En este entorno, el código se integra y se prueba de manera continua. Las herramientas de integración continua automatizan el proceso de construcción y prueba del software, asegurando que los cambios se integren sin problemas.

4 Entorno de Producción: Este es el entorno donde el software se despliega para su uso por parte de los clientes. Se implementan medidas de seguridad adicionales y se monitorea el rendimiento del software para asegurar su funcionamiento óptimo.

5 Entorno de Staging: Este entorno es una copia casi exacta del entorno de producción y se utiliza para realizar pruebas finales antes del despliegue. Permite a los equipos de desarrollo y operaciones verificar que todo funcione correctamente en un entorno que replica el de producción.

CULTURASOFT de los entornos expuestos anteriormente ha implementado:

Entrono de desarrollo: Cada proyecto tiene una rama Develop en la cual se realiza la interacción del desarrollo de cada uno de los integrantes del proyecto. Esta rama es clonada por el equipo y a partir de ella se crean ramas de trabajo, posteriormente cada colaborador solicita un Pull Request a Develop.

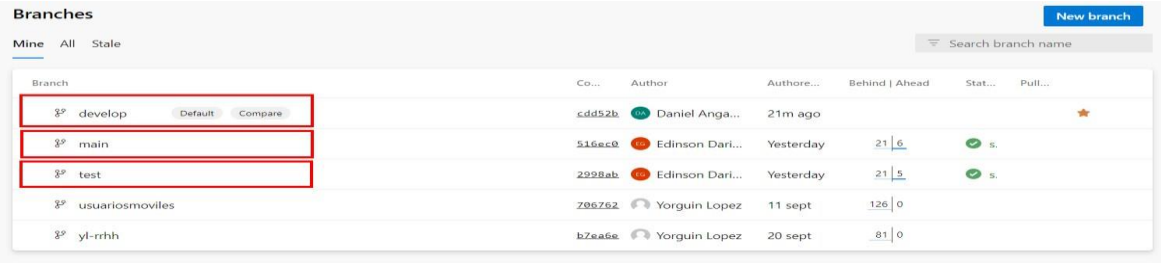
Entorno de Pruebas: Este entorno está configurado en la rama Test, la cual se despliega a un servidor de pruebas y sobre el cual los QA realizan el testeo de los componentes desarrollados antes de ser desplegado a producción.

Entorno de Producción: Este entono está separado en la rama Main y se despliega a un servidor de producción el cual está separado de los demás entornos.

Solo los entornos Test y Producción se despliegan al servidor y se hace manualmente.

Figura 4

Ambientes de Desarrollo de CulturaSoft



Nota. Captura de pantalla que muestra los ambientes de desarrollo establecidos.

Análisis GAP de Brechas En Seguridad de Datos ISO/IEC 27001

El análisis de brecha GAP (brecha en inglés) es una herramienta que permite medir el estado actual y el estado deseado de un proceso que para nuestro caso es la seguridad de la información enfocada a las configuraciones en desarrollo de software. Para CULTURASOFT se ha realizado en conjunto con el personal administrativo y del área de infraestructura la aplicación del análisis de brecha de acuerdo al estándar ISO/IEC 27001:2022. El formato aplicado se basa en los controles de la ISO/IEC 27001:2022.

La siguiente tabla muestra los requisitos obligatorios estándar establecidos para la ISO27001. Define los aspectos mínimos que se debe implementar el Sistema de Seguridad de la Información.

Tabla 1

Requisitos Obligatorios

Sección	Requisito ISO/IEC 27001	Estado
4	Contexto de la organización	
4.1	Contexto organizacional	
4.1.1	Determinar los objetivos del SGSI de la organización y cualquier cuestión que pueda comprometer su efectividad	Definido
4.2	Partes interesadas	
4.2.1	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, entre otros.	Definido
4.2.2	Determinar sus requisitos relevantes al respecto de la seguridad de la información y sus obligaciones.	Definido
4.3	Alcance del SGSI.	
4.3.1	Determinar y documentar el alcance del SGSI.	Limitado
4.4	SGSI.	
4.4.1	Establecer, implementar, mantener y mejorar continuamente un SGSI de conformidad con la norma.	Inicial
5	Liderazgo.	
5.1	Liderazgo & compromiso.	
5.1.1	La alta dirección debe demostrar liderazgo y compromiso en relación con el SGSI.	Definido
5.2	Política.	
5.2.1	Establecer la política de seguridad de la información.	Inexistente
5.3	Roles, responsabilidades y autoridades en la organización.	
5.3.1	Asignar y comunicar los roles y responsabilidades de la seguridad de la información.	Limitado
6	Planificación.	
6.1	Acciones para tratar con los riesgos y oportunidades.	
6.1.1	Diseñar / planificar el SGSI para satisfacer los requisitos, tratando con los riesgos & oportunidades.	Inicial
6.1.2	Definir y aplicar un proceso de apreciación de riesgos de seguridad de la información.	Inicial
6.1.3	Documentar y aplicar un proceso de tratamiento de riesgos de seguridad de la información.	Inicial
6.2	Objetivos & planes de seguridad de la información	

Sección	Requisito ISO/IEC 27001	Estado
6.2.1	Establecer y documentar los objetivos y planes de seguridad de la información.	Inicial
6.3	Planificación de cambios.	
6.3.1	Los cambios sustanciales al SGSI deben ser llevados a cabo de manera planificada.	Inicial
7	Soporte.	
7.1	Recursos.	
7.1.1	Determinar y proporcionar los recursos necesarios para el SGSI.	Inicial
7.2	Competencias.	
7.2.1	Determinar, documentar y poner a disposición las competencias necesarias.	Inicial
7.3	Concientización.	
7.3.1	Establecer un programa de concientización en seguridad.	Inicial
7.4	Comunicación.	
7.4.1	Determinar la necesidad para las comunicaciones internas y externas relevantes al SGSI.	Inicial
7.5	Información documentada.	
7.5.1	Proveer la documentación requerida por la norma, así como la requerida por la organización.	Inicial
7.5.2	Proveer títulos, autores, etc. para la documentación, adecuar el formato consistentemente, revisarlos y aprobarlos.	Inicial
7.5.3	Controlar la documentación adecuadamente.	Inicial
8	Operación.	
8.1	Planificación y control operacional.	
8.1.1	Planificar, implementar, controlar y documentar el proceso del SGSI para gestionar los riesgos (i.e. un plan de tratamiento de riesgos).	Inicial
8.2	Apreciación del riesgo de seguridad de la información	
8.2.1	(Re)hacer la apreciación, documentar los riesgos de seguridad de la información en forma regular y ante cambios o modificaciones	Inicial
8.3	Tratamiento del riesgo de seguridad de la información	
8.3.1	Implementar el plan de tratamiento de riesgos y documentar los resultados.	Inicial
9	Evaluación del desempeño.	
9.1	Seguimiento, medición, análisis y evaluación.	
9.1.1	Hacer seguimiento, medir, analizar y evaluar el SGSI y los controles.	Inicial

Sección	Requisito ISO/IEC 27001	Estado
9.2	Auditoría interna.	
9.2.1	Planificar y llevar a cabo auditorías internas del SGSI.	Inicial
9.3	Revisión por la dirección.	
9.3.1	Emprender revisiones por la dirección del SGSI regularmente.	Inicial
10	Mejora.	
10.1	Mejora continua.	
10.1.1	Mejorar continuamente el SGSI.	Inicial
10.2	No conformidad y acciones correctivas.	
10.2.1	Identificar, corregir y llevar a cabo acciones para prevenir la recurrencia de no conformidades, documentando las acciones.	Inicial

Nota. Requisitos de cumplimiento obligatorio. Adaptada de ISO/IEC 27001

La Declaración de Aplicabilidad (SoA, por sus siglas en inglés) es un documento fundamental en el marco de la norma ISO 27001, que se centra en el Sistema de Gestión de Seguridad de la Información (SGSI). La SoA no solo enumera los controles, sino que también justifica su inclusión o exclusión. Esto es crucial para demostrar que la organización ha realizado un análisis exhaustivo de riesgos y ha seleccionado los controles adecuados para mitigar esos riesgos.

Tabla 2

Declaración de Aplicabilidad SoA

Sección	Control de seguridad de la información	Estado	Notas
A5	Controles organizacionales		
A.5.1	Políticas para la seguridad de la información	Inicial	Existe una política inicial, pero se debe actualizar, hay nuevas funcionalidades
A.5.2	Roles y responsabilidades en la seguridad de la información	Inicial	Se han definido los roles, pero falta la implementación
A.5.3	Segregación de tareas	Limitado	Existe la segregación, pero falta control de esta
A.5.4	Responsabilidades de gestión	Inicial	En etapa inicial
A.5.5	Contacto con las autoridades	Inexistente	No se ha realizado nunca un contacto con autoridades
A.5.6	Contacto con grupos de interés especial	Inexistente	No se ha realizado nunca un contacto con autoridades
A.5.7	Inteligencia de amenazas	Definido	Se realiza y documenta
A.5.8	Seguridad de la información en la gestión de proyectos	Inicial	Existe un proceso inicial, falta más implementación
A.5.9	Inventario de activos de información y otros asociados a la misma	Definido	
A.5.10	Uso aceptable de activos de información y otros asociados a la misma	Definido	
A.5.11	Devolución de activos	Limitado	
A.5.12	Clasificación de la información	Inicial	
A.5.13	Etiquetado de la información	Inicial	
A.5.14	Intercambio de la información	Inicial	
A.5.15	Control de Acceso	Inexistente	
A.5.16	Gestión de la identidad	Inicial	Se realiza proceso de gestión de la identidad, pero falta implementación y control
A.5.17	Información de autenticación	Definido	Se ha definido la información de autenticación

Sección	Control de seguridad de la información	Estado	Notas
A.5.18	Derechos de acceso	Definido	
A.5.19	Seguridad de la información en la relación con proveedores	Inexistente	No existen muchos proveedores, no se ha dado importancia a este proceso
A.5.20	Requisitos de seguridad de la información en contratos con terceros	Definido	Se han definido los modelos de contratos
A.5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC (Tecnologías de Información y Comunicación)	Inexistente	No se ha contemplado
A.5.22	Gestión del cambio, revisión y monitoreo de los servicios del proveedor o suministrador	Inicial	Esta en proceso no están implementados
A.5.23	Seguridad de la información para el uso de servicios en la nube (cloud)	Definido	Se tiene servicio con Google Cloud y Amazon.
A.5.24	Planeamiento y preparación de la gestión de incidentes de seguridad de la información	Inexistente	
A.5.25	Evaluación y decisión en los eventos de seguridad de la información	Inexistente	
A.5.26	Respuesta a los incidentes de seguridad de la información	Inexistente	
A.5.27	Aprendizaje sobre los incidentes de seguridad de la información	Inexistente	
A.5.28	Recolección de evidencia	Inicial	
A.5.29	Seguridad de la información durante interrupciones	Inexistente	
A.5.30	Preparación de las TIC para la continuidad de negocio	Limitado	
A.5.31	Requisitos legales, estatutarios, regulatorios y contractuales	Definido	
A.5.32	Derechos de propiedad intelectual	Gestionado	
A.5.33	Protección de registros	Limitado	

Sección	Control de seguridad de la información	Estado	Notas
A.5.34	Privacidad y protección de la PII (Información Identificable Personal)	Definido	
A.5.35	Revisión independiente de la seguridad de la información	Limitado	
A.5.36	Cumplimiento con las políticas, reglas y normas de la seguridad de la información	Limitado	Es limitado, no se aplica siempre y falta control
A.5.37	Procedimientos operacionales documentados	Inexistente	No todos los procedimientos están documentados.
A6	Controles personales		
A.6.1	Revisión de antecedentes	Definido	Se ha definido la revisión de antecedes al personal antes de contratación
A.6.2	Términos y condiciones de empleo	Gestionado	Existen controles claros para la contratación y modelos de contratos legalmente aceptados
A.6.3	Concientización, educación y entrenamiento en seguridad de la información	Inicial	No se realiza inducción al respecto o es muy general
A.6.4	Proceso disciplinario	Gestionado	Se cuenta con manual de funciones y reglamento interno
A.6.5	Responsabilidades luego de la finalización o cambio de empleo	Definido	Está definido, pero no se aplica correctamente.
A.6.6	Acuerdos de confidencialidad o no revelación	Optimizado	Gestionado y optimizado
A.6.7	Trabajo remoto	Optimizado	Se hace uso de herramientas seguras y el control de tareas
A.6.8	Reportes de eventos de seguridad de la información	Gestionado	Se realiza el reporte oportuno y existen formatos y controles.
A7	Controles físicos		
A.7.1	Perímetros de seguridad física	Gestionado	
A.7.2	Entrada física	Gestionado	

Sección	Control de seguridad de la información	Estado	Notas
A.7.3	Seguridad de oficinas, despachos e instalaciones	Definido	
A.7.4	Supervisión de la seguridad física	Definido	
A.7.5	Protección contra amenazas físicas y ambientales	Inexistente	
A.7.6	Trabajo en áreas seguras	Limitado	
A.7.7	Escritorio y pantalla limpios	Gestionado	
A.7.8	Emplazamiento y protección de equipos	Gestionado	
A.7.9	Seguridad de activos fuera de las instalaciones	Gestionado	
A.7.10	Medios de almacenamiento	Gestionado	Existen copias de seguridad en nube automatizadas
A.7.11	Servicios de suministro	Definido	
A.7.12	Seguridad del cableado	Gestionado	
A.7.13	Mantenimiento de equipos	Gestionado	Debidamente organizado por periodos
A.7.14	Eliminación o reutilización segura de equipos	Gestionado	
A8	Controles tecnológicos		
A.8.1	Dispositivos terminales de usuario	Limitado	
A.8.2	Derechos de acceso privilegiado	Limitado	
A.8.3	Restricción de acceso a la información	Definido	
A.8.4	Acceso al código fuente	Gestionado	
A.8.5	Autenticación segura	Gestionado	Se hace uso de Microsoft para gestionar la autenticación
A.8.6	Gestión de la capacidad	Definido	
A.8.7	Protección contra código malicioso (malware)	Gestionado	
A.8.8	Gestión de vulnerabilidades técnicas	Definido	
A.8.9	Gestión de la configuración	Definido	
A.8.10	Borrado de información	Limitado	

Sección	Control de seguridad de la información	Estado	Notas
A.8.11	Enmascarado de datos	Limitado	
A.8.12	Prevención de filtración de datos	Limitado	
A.8.13	Respaldo de información	Gestionado	
A.8.14	Redundancia de las instalaciones de procesamiento de información	Limitado	
A.8.15	Registración	Definido	
A.8.16	Actividades de supervisión	Definido	
A.8.17	Sincronización de reloj.	Gestionado	
A.8.18	Uso de programas utilitarios privilegiados	Gestionado	
A.8.19	Instalación de software en sistemas operacionales	Limitado	
A.8.20	Seguridad en redes	Gestionado	
A.8.21	Seguridad de servicios de red	Gestionado	
A.8.22	Segregación de redes	Gestionado	
A.8.23	Filtrado web	Gestionado	
A.8.24	Uso de criptografía	Limitado	
A.8.25	Desarrollo seguro del ciclo de vida	Gestionado	Se ha definido y gestionado el proceso de desarrollo seguro
A.8.26	Requerimientos de seguridad en aplicaciones	Gestionado	Siempre se tiene en cuenta en requisitos arquitectónicos
A.8.27	Principios de arquitectura de sistemas e ingeniería seguras	Gestionado	
A.8.28	Generación de código seguro	Gestionado	
A.8.29	Prueba segura en el desarrollo y aceptación	Inicial	
A.8.30	Desarrollo tercerizado	No Aplica	
A.8.31	Separación de entornos de desarrollo, prueba y producción	Optimizado	Está definidos claramente y canalizado para su automatización mediante DevOps
A.8.32	Gestión de cambios	Optimizado	
A.8.33	Información de prueba	Limitado	

Sección	Control de seguridad de la información	Estado	Notas
A.8.34	Protección de sistemas de información durante pruebas de auditoría	Limitado	

Nota. Desarrollo de aplicabilidad SoA.

Métricas

El análisis situacional de CULTURASOFT basado en la encuesta aplicada ha permitido realizar métricas sobre el estado y la aplicabilidad del estándar ISO/IEC 27001:2023.

Tabla 3

Métricas

Estado	Significado	Proporción de requisitos del SGSI	Proporción de controles de seguridad de la información
? Desconocido	Controles que no han sido revisados	0%	0%
Inexistente	Ausencia de una políticas, controles y procedimientos legibles	4%	13%
Inicial	Desarrollo iniciado, requiere tiempo y esfuerzo para su aplicabilidad	75%	13%
Limitado	Se ha iniciado y está progresando, pero no está terminado	7%	18%
Definido	El desarrollo de los controles y su aplicabilidad está definido, pero aún no ha sido validado por la alta gerencia.	14%	22%
Gestionado	Desarrollo completo, ha iniciado operación reciente	0%	29%
Optimizado	El requisito de seguridad ha sido totalmente implementado, está siendo gestionado y monitoreado	0%	4%
No Aplica	Todos los requerimientos de la norma ISO/IEC 27001 si el SGSI va a ser certificado son obligatorios. De lo contrario pueden ser ignorados de acuerdo con decisiones de la gerencia.	0%	1%

Nota. En esta tabla se describe las convenciones y resultados de las tablas 1 y 2.

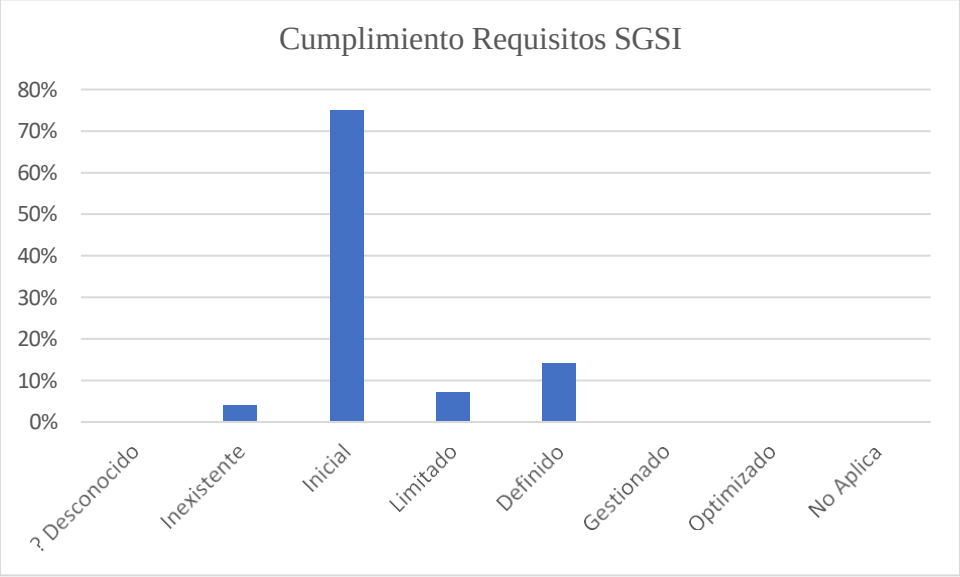
Análisis de Políticas y Procedimientos Actuales en Seguridad de Datos

Análisis

La métrica presentada evalúa el estado de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa CULTURASOFT, específicamente en términos de los requisitos de la norma ISO/IEC 27001 y los controles de seguridad de la información asociados. El análisis de estos datos muestra en qué fase se encuentra la empresa en cuanto a la implementación de su SGSI y sus controles, identificando áreas críticas y oportunidades de mejora.

Figura 5

Gráfico cumplimiento Requisitos SGSI



Nota. Relación de cumplimiento del SGSI

1. Estado Desconocido

- Proporción de Requisitos del SGSI: 0%
- Proporción de Controles de Seguridad de la Información: 0%

- Análisis: No hay controles o requisitos en esta categoría, lo cual es positivo ya que indica que todos los elementos del SGSI han sido evaluados o al menos están identificados.

2. Estado Inexistente

- Proporción de Requisitos del SGSI: 4%
- Proporción de Controles de Seguridad de la Información: 13%
- Análisis: Aquí se revela una brecha preocupante: el 13% de los controles de seguridad de la información están en un estado inexistente, lo que sugiere una falta total de políticas, procedimientos y controles en algunas áreas críticas de la seguridad. Además, un 4% de los requisitos del SGSI también carecen de implementación. Esto indica un área significativa de riesgo que debe abordarse de manera prioritaria.

3. Estado Inicial

- Proporción de Requisitos del SGSI: 75%
- Proporción de Controles de Seguridad de la Información: 13%
- Análisis: La mayor parte de los requisitos del SGSI (75%) están en una fase inicial de desarrollo. Aunque esto muestra un esfuerzo por avanzar en la implementación, sugiere que el SGSI aún no está completamente maduro. En términos de controles, el 13% también se encuentra en esta etapa, lo cual representa un buen punto de partida, pero requiere mejoras considerables para garantizar una seguridad adecuada.

4. Estado Limitado

- Proporción de Requisitos del SGSI: 7%

- Proporción de Controles de Seguridad de la Información: 18%
- Análisis: Una pequeña parte de los requisitos del SGSI (7%) y una mayor proporción de controles de seguridad (18%) están en una etapa de progreso, pero aún incompletos. Aunque se han tomado medidas, aún existe un riesgo considerable ya que la implementación no está finalizada.

5. Estado Definido

- Proporción de Requisitos del SGSI: 14%
- Proporción de Controles de Seguridad de la Información: 22%
- Análisis: Un 14% de los requisitos del SGSI ya están claramente definidos, pero no validados por la alta gerencia. En cuanto a los controles, el 22% se encuentra en este estado. Aunque esta es una señal de avance, la falta de validación y aprobación podría retrasar la operatividad y efectividad de estas medidas.

6. Estado Gestionado

- Proporción de Requisitos del SGSI: 0%
- Proporción de Controles de Seguridad de la Información: 29%
- Análisis: Ningún requisito del SGSI está completamente gestionado, lo cual es una brecha importante. Sin embargo, el 29% de los controles de seguridad están en esta fase, lo que indica que, aunque los controles han comenzado a operar, todavía hay un desfase con respecto a los requisitos del SGSI que no han llegado a esta etapa.

7. Estado Optimizado

- Proporción de Requisitos del SGSI: 0%
- Proporción de Controles de Seguridad de la Información: 4%

- Análisis: No hay ningún requisito del SGSI que haya sido optimizado, y solo el 4% de los controles de seguridad están en un estado plenamente gestionado y monitoreado. Esto sugiere que la empresa aún no ha alcanzado un nivel de madurez avanzada en la gestión de su seguridad, lo cual debería ser un objetivo clave.

8. No Aplica

- Proporción de Requisitos del SGSI: 0%
- Proporción de Controles de Seguridad de la Información: 1%
- Análisis: El 1% de los controles ha sido marcado como "No aplica", posiblemente debido a decisiones de la gerencia. Es importante que esta categoría se mantenga al mínimo, ya que la mayoría de los requisitos de ISO/IEC 27001 son obligatorios si se pretende obtener una certificación.

Recomendaciones

1. Brechas Críticas: La mayor preocupación radica en que un 13% de los controles de seguridad de la información están en estado inexistente, lo que indica una falta total de mecanismos de protección en ciertas áreas. Esto requiere atención urgente.

2. Madurez Baja: Aunque la mayoría de los requisitos del SGSI (75%) están en desarrollo, solo el 14% están claramente definidos. Esto significa que el SGSI aún no ha alcanzado una madurez suficiente. Un esfuerzo adicional es necesario para completar el desarrollo y alcanzar los estados "Gestionado" y "Optimizado".

3. Diferencias en la Implementación de Controles y Requisitos: Mientras que una buena parte de los controles están en fases gestionadas o definidas, los requisitos del

SGSI están retrasados en su implementación. Este desfase puede generar riesgos de desalineación entre las políticas y los controles.

4. Mejoras Recomendadas:

- Priorizar el cierre de las brechas en los controles inexistentes e iniciar su desarrollo inmediato.
- Acelerar la definición y validación de los requisitos del SGSI por parte de la alta gerencia para sincronizarlos con el estado de los controles.
- Fomentar la optimización de controles, enfocándose en las áreas más críticas de la empresa.

De acuerdo con la informacion analizada y al análisis de brecha realizado se concluye que CULTURASOFT, aunque ha realizado esfuerzos significativos para implementar buenas prácticas y modelo de seguridad tiene una brecha crítica y una de las principales fallas que no posee Políticas y Procedimiento de seguridad de datos escritos, verificables y socializados.

Análisis Detallado de Variables Clave

Identificación de Variables Clave

Luego del análisis del estado de las políticas de seguridad que contemplen el proceso de configuraciones en despliegue dentro de la organización

1. Configuraciones Incorrectas

- Descripción: Errores en la configuración de sistemas, servidores y aplicaciones que pueden exponer datos sensibles.
- Ejemplos: Permisos mal asignados, puertos abiertos innecesarios, falta de cifrado en comunicaciones.

2. Políticas de Seguridad
    - Descripción: Existencia y efectividad de políticas formales de seguridad de la información.
    - Ejemplos: Políticas de gestión de accesos, políticas de respuesta a incidentes, políticas de protección de datos.
3. Procedimientos Operativos Estándar (SOPs)
    - Descripción: Documentación y aplicación de procedimientos claros para gestionar configuraciones, cambios y respuestas a incidentes.
    - Ejemplos: Procedimientos para auditorías de acceso, gestión de parches, monitoreo continuo.
4. Capacitación del Personal
    - Descripción: Nivel de conocimiento y concienciación del personal sobre prácticas de seguridad.
    - Ejemplos: Programas de capacitación, simulaciones de ataques, evaluaciones de comprensión.
5. Herramientas de Auditoría y Monitoreo
    - Descripción: Uso de herramientas tecnológicas para detectar vulnerabilidades y monitorear configuraciones.
    - Ejemplos: Nessus, OpenVAS, Nmap, Azure DevOps.
6. Gestión de Acceso y Control de Permisos
    - Descripción: Implementación de controles basados en roles y autenticación multifactorial (MFA).
    - Ejemplos: Asignación de permisos específicos, eliminación de accesos obsoletos.
7. Cumplimiento Normativo

- Descripción: Alineación con estándares internacionales como ISO/IEC 27001 e ISO/IEC 27002.
- Ejemplos: Estado de implementación de requisitos obligatorios, brechas identificadas en el análisis GAP.

8. Respuesta a Incidentes de Seguridad
    - Descripción: Capacidad de la organización para detectar, gestionar y mitigar incidentes de seguridad.
    - Ejemplos: Tiempo de respuesta a incidentes críticos, número de incidentes repetitivos.
9. Automatización de Procesos
    - Descripción: Grado de automatización en la gestión de cambios, parches y respaldos.
    - Ejemplos: Ciclos automáticos de despliegue de parches, copias de seguridad automatizadas.
10. Cultura Organizacional de Seguridad
    - Descripción: Compromiso de la alta gerencia y del personal con la seguridad de la información.
    - Ejemplos: Validación de políticas por la alta dirección, adopción de medidas preventivas.

Evaluación del Impacto de las Variables Clave

En esta sección se realiza una evaluación del impacto de las variables clave para luego proseguir a la priorización.

1. Configuraciones Incorrectas

- Descripción: Errores en la configuración de sistemas, servidores y aplicaciones que pueden exponer datos sensibles.
- Estado Actual:
    - Según el análisis GAP, un 13% de los controles de seguridad están en estado "Inexistente" , lo que sugiere una falta total de mecanismos para prevenir configuraciones incorrectas.
    - El control A.8.9 (Gestión de la configuración) está en estado "Definido", pero no ha sido validado ni optimizado.
- Impacto: Las configuraciones incorrectas representan una de las principales causas de brechas de seguridad, como se evidencia en incidentes globales (e.g., Capital One, Microsoft).
- Recomendaciones:
    - Implementar auditorías trimestrales con herramientas como Nessus y OpenVAS .
    - Validar configuraciones iniciales utilizando CIS Benchmarks .
    - Automatizar el despliegue de parches críticos para reducir vulnerabilidades conocidas.

2. Políticas de Seguridad

- Descripción: Existencia y efectividad de políticas formales de seguridad de la información.
- Estado Actual:
    - El análisis GAP revela que la política de seguridad de la información (A.5.1) está en estado "Inicial".

    - No existen políticas escritas ni socializadas formalmente en la empresa.
- Impacto: La ausencia de políticas claras aumenta el riesgo de exposición de datos sensibles y dificulta la respuesta a incidentes.
- Recomendaciones:
    - Desarrollar y documentar políticas alineadas con ISO/IEC 27001.
    - Socializar las políticas mediante capacitaciones y publicarlas en el intranet corporativo.

3. Procedimientos Operativos Estándar (SOPs)

- Descripción: Documentación y aplicación de procedimientos claros para gestionar configuraciones, cambios y respuestas a incidentes.
- Estado Actual:
    - El control A.5.37 (Procedimientos operacionales documentados) está en estado "Inexistente".
    - Los procedimientos actuales no están documentados ni estandarizados.
- Impacto: La falta de SOPs dificulta la estandarización de procesos y la respuesta efectiva a incidentes.
- Recomendaciones:
    - Redactar SOPs detallados para gestión de accesos, cambios y respuesta a incidentes.
    - Capacitar al personal en el uso de estos procedimientos.

4. Capacitación del Personal

- Descripción: Nivel de conocimiento y concienciación del personal sobre prácticas de seguridad.

- Estado Actual:
    - El control A.7.3 (Concientización) está en estado "Inicial".
    - No se realiza inducción específica sobre seguridad de la información.
- Impacto: La baja capacitación incrementa el riesgo de errores humanos y configuraciones incorrectas.
- Recomendaciones:
    - Implementar programas de capacitación continua sobre seguridad de la información.
    - Realizar simulaciones de ataques para mejorar la preparación del personal.

5. Herramientas de Auditoría y Monitoreo

- Descripción: Uso de herramientas tecnológicas para detectar vulnerabilidades y monitorear configuraciones.
- Estado Actual:
    - Las herramientas como Nessus y OpenVAS aún no están completamente integradas.
    - El control A.8.16 (Actividades de supervisión) está en estado "Definido".
- Impacto: La falta de monitoreo continuo puede dejar sin detectar vulnerabilidades críticas.
- Recomendaciones:
    - Integrar herramientas avanzadas para auditorías regulares y monitoreo en tiempo real.
    - Automatizar escaneos de seguridad mensuales.

6. Gestión de Acceso y Control de Permisos

- Descripción: Implementación de controles basados en roles y autenticación multifactorial (MFA).
- Estado Actual:
    - El control A.9.1.1 (Gestión de acceso basada en roles) está en estado "Definido".
    - No se ha implementado MFA en todos los sistemas críticos.
- Impacto: La falta de segregación de roles y revisiones periódicas aumenta el riesgo de accesos indebidos.
- Recomendaciones:
    - Implementar MFA en todos los sistemas críticos.
    - Realizar auditorías mensuales de accesos privilegiados.

7. Cumplimiento Normativo

- Descripción: Alineación con estándares internacionales como ISO/IEC 27001 e ISO/IEC 27002.
- Estado Actual:
    - El análisis GAP muestra que el 75% de los requisitos del SGSI están en estado "Inicial".
    - Ningún requisito ha alcanzado el estado "Optimizado".
- Impacto: El incumplimiento normativo puede resultar en sanciones legales y pérdida de confianza.
- Recomendaciones:
    - Priorizar la implementación de requisitos obligatorios de ISO/IEC 27001.
    - Realizar auditorías semestrales para asegurar el cumplimiento.

8. Respuesta a Incidentes de Seguridad

- Descripción: Capacidad de la organización para detectar, gestionar y mitigar incidentes de seguridad.
- Estado Actual:
    - Los controles A.16.1.1 (Gestión de incidentes) y A.16.1.5 (Escalamiento) están en estado "Inexistente".
    - No existe un equipo formal de respuesta a incidentes (CSIRT).
- Impacto: La falta de un proceso estructurado prolonga el impacto de los incidentes.
- Recomendaciones:
    - Crear un CSIRT con roles y responsabilidades claras.
    - Documentar y analizar cada incidente para prevenir recurrencias.

9. Automatización de Procesos

- Descripción: Grado de automatización en la gestión de cambios, parches y respaldos.
- Estado Actual:
    - El control A.8.34 (Protección de sistemas durante pruebas) está en estado "Limitado".
    - Los despliegues a producción son manuales.
- Impacto: La falta de automatización incrementa el tiempo de respuesta a vulnerabilidades.
- Recomendaciones:
    - Automatizar el despliegue de parches críticos.
    - Implementar copias de seguridad automatizadas en la nube.

10. Cultura Organizacional de Seguridad

- Descripción: Compromiso de la alta gerencia y del personal con la seguridad de la información.
- Estado Actual:
    - El control A.7.3 (Concientización) está en estado "Inicial".
    - La resistencia al cambio es un desafío identificado.
- Impacto: La falta de compromiso reduce la efectividad de las políticas y procedimientos.
- Recomendaciones:
    - Fomentar una cultura de seguridad mediante campañas de concientización.
    - Involucrar a la alta gerencia en la validación y socialización de políticas.

Priorización de Variables Clave

Con base en los análisis realizados, se puede priorizar las 10 variables clave identificadas de acuerdo con su impacto en la seguridad de datos y su relación con las brechas detectadas en CULTURASOFT S.A.S. Esta priorización se basa en tres criterios principales:

1. Impacto en la seguridad de datos: Variables que tienen un efecto directo en la exposición o pérdida de datos sensibles.
2. Estado actual según el análisis GAP ISO/IEC 27001: Variables relacionadas con áreas críticas donde se han identificado brechas significativas.
3. Viabilidad de implementación: Variables que pueden abordarse de manera efectiva en el corto y mediano plazo.

Alta Prioridad

Estas variables son críticas debido a su alto impacto en la seguridad de datos y su estado actual insatisfactorio (estado "Inexistente" o "Inicial").

1. Configuraciones Incorrectas
    - Razón: Según el análisis GAP, las configuraciones incorrectas están directamente relacionadas con el 13% de los controles de seguridad en estado "Inexistente". Además, se identificaron vulnerabilidades graves en servidores y aplicaciones mal configuradas.
    - Acción recomendada: Implementar auditorías trimestrales con herramientas como Nessus y OpenVAS, y validar configuraciones iniciales utilizando CIS Benchmarks.
2. Políticas de Seguridad
    - Razón: No existen políticas formales escritas ni socializadas (control A.5.1 en estado "Inicial"). Esto representa una brecha crítica en la gestión de seguridad de la información.
    - Acción recomendada: Desarrollar y documentar políticas alineadas con ISO/IEC 27001, y realizar capacitaciones para garantizar su comprensión y adopción.
3. Gestión de Acceso y Control de Permisos
    - Razón: El control A.9.1.1 (Gestión de acceso basada en roles) está en estado "Definido", pero no ha sido validado ni optimizado. La falta de segregación de roles y revisiones periódicas aumenta el riesgo de accesos indebidos.
    - Acción recomendada: Implementar autenticación multifactorial (MFA) y realizar auditorías mensuales de accesos privilegiados.
4. Capacitación del Personal

- Razón: El control A.7.3 (Concientización) está en estado "Inicial". La baja capacitación incrementa el riesgo de errores humanos y configuraciones incorrectas.
- Acción recomendada: Implementar programas de capacitación continua sobre seguridad de la información y realizar simulaciones de ataques (e.g., phishing).

5. Respuesta a Incidentes de Seguridad
    - Razón: Los controles A.16.1.1 (Gestión de incidentes) y A.16.1.5 (Escalamiento) están en estado "Inexistente". No existe un equipo formal de respuesta a incidentes (CSIRT).
    - Acción recomendada: Crear un CSIRT con roles y responsabilidades claras, y documentar cada incidente para prevenir recurrencias.

Media Prioridad

Estas variables tienen un impacto moderado en la seguridad de datos, pero aún requieren atención para fortalecer el SGSI.

6. Procedimientos Operativos Estándar (SOPs)
    - Razón: El control A.5.37 (Procedimientos operacionales documentados) está en estado "Inexistente". La falta de SOPs dificulta la estandarización de procesos y la respuesta efectiva a incidentes.
    - Acción recomendada: Redactar SOPs detallados para gestión de accesos, cambios y respuesta a incidentes, y capacitar al personal en su uso.
7. Herramientas de Auditoría y Monitoreo

- Razón: Las herramientas como Nessus y OpenVAS aún no están completamente integradas. El control A.8.16 (Actividades de supervisión) está en estado "Definido".
- Acción recomendada: Integrar herramientas avanzadas para auditorías regulares y monitoreo en tiempo real.

8. Cumplimiento Normativo
    - Razón: El análisis GAP muestra que el 75% de los requisitos del SGSI están en estado "Inicial". El incumplimiento normativo puede resultar en sanciones legales y pérdida de confianza.
    - Acción recomendada: Priorizar la implementación de requisitos obligatorios de ISO/IEC 27001 y realizar auditorías semestrales.

Baja Prioridad

Estas variables tienen un impacto menor en la seguridad de datos o ya están parcialmente gestionadas.

9. Automatización de Procesos
    - Razón: El control A.8.34 (Protección de sistemas durante pruebas) está en estado "Limitado". La automatización de procesos aún no es una prioridad crítica.
    - Acción recomendada: Automatizar el despliegue de parches críticos y copias de seguridad en la nube.
10. Cultura Organizacional de Seguridad
    - Razón: El control A.7.3 (Concientización) está en estado "Inicial". La resistencia al cambio es un desafío identificado.

- Acción recomendada: Fomentar una cultura de seguridad mediante campañas de concientización y liderazgo ejecutivo.

Diseño de Políticas y Procedimientos para la Seguridad de Datos

Diseño de Políticas y Procedimientos

En función del análisis GAP ISO 27001 identificado en el documento y las necesidades específicas de CulturaSoft S.A.S., se desarrollan las siguientes políticas de seguridad y procedimientos personalizados. Estas políticas están alineadas con las mejores prácticas internacionales y responden a las brechas detectadas en la empresa, tales como falta de control de accesos, políticas formales de seguridad, y documentación incompleta.

Esta política integra las brechas identificadas en el análisis GAP basado en los controles ISO/IEC 27001, optimizando las políticas para que sean más específicas y alineadas con las mejores prácticas de seguridad. A continuación, se presenta la versión ajustada de las políticas y procedimientos.

La presente política se presenta a la empresa CulturaSoft para su análisis, ajuste y aprobación antes de dar inicio al proceso de implementación.

Metodología para Priorizar Políticas Basadas en Impacto Potencial

La priorización de políticas para la seguridad de datos puede implementarse utilizando una metodología estructurada basada en la gestión de riesgos. Este enfoque permite clasificar las políticas según su impacto en la mitigación de riesgos críticos y alinearlas con los objetivos organizacionales. A continuación, se describe una metodología paso a paso.

1. Identificación y Clasificación de Activos Críticos

- Propósito: Determinar qué activos (datos, sistemas, procesos) son más valiosos para la organización y requieren protección prioritaria.
- Acciones:

    - Realizar un inventario detallado de activos digitales y físicos.
    - Clasificar los activos según su sensibilidad, confidencialidad y criticidad para las operaciones del negocio.

- Herramientas: Matrices de activos, cuestionarios a equipos clave.

2. Evaluación de Riesgos

- Propósito: Analizar las amenazas y vulnerabilidades específicas que afectan a cada activo clasificado.
- Acciones:
    - Identificar las amenazas posibles (como accesos no autorizados, ataques cibernéticos, o errores humanos).
    - Evaluar las vulnerabilidades existentes en los sistemas y procesos actuales.
    - Estimar el impacto potencial de un incidente en términos financieros, legales, de reputación o de interrupción operacional.
- Herramientas: NIST SP 800-30, análisis de amenazas (Threat Modelling).

3. Asignación de Impacto y Probabilidad

- Propósito: Cuantificar el riesgo asociado a cada amenaza y vulnerabilidad.
- Acciones:
    - Establecer niveles de impacto: Bajo, Medio, Alto, Crítico.
    - Evaluar la probabilidad de ocurrencia de cada riesgo.

    - Crear una matriz de riesgos cruzando impacto y probabilidad para priorizar los riesgos más significativos.

- Herramientas: Matriz de Impacto/Probabilidad, software de gestión de riesgos (como RiskWatch o FAIR).

4. Priorización Basada en el Riesgo

- Propósito: Asignar prioridades a las políticas según el riesgo que mitigan.
- Acciones:
    - Asignar puntajes a cada riesgo basado en la matriz de impacto/probabilidad.
    - Relacionar cada política con los riesgos específicos que busca mitigar.
    - Ordenar las políticas de mayor a menor prioridad según el puntaje de los riesgos asociados.
- Ejemplo:
    - Políticas que abordan riesgos críticos con alta probabilidad: Prioridad 1.
    - Políticas para riesgos de impacto medio y baja probabilidad: Prioridad 3.

5. Validación con las Partes Interesadas

- Propósito: Asegurar que la priorización de políticas esté alineada con las expectativas y objetivos de la organización.
- Acciones:

- Realizar talleres o reuniones con directivos y equipos clave.
- Ajustar la priorización según el aporte de expertos y necesidades específicas del negocio.

6. Implementación Escalonada

- Propósito: Desplegar las políticas más críticas primero para maximizar la reducción de riesgos.
- Acciones:
  - Crear un cronograma de implementación basado en la prioridad asignada.
  - Monitorear el impacto de cada política implementada en los riesgos asociados.

7. Monitoreo y Revisión Continua

- Propósito: Asegurar la efectividad y la pertinencia de la priorización.
- Acciones:
  - Establecer KPIs (indicadores clave de desempeño) para medir la efectividad de las políticas.
  - Revisar y ajustar la priorización periódicamente, considerando cambios en el entorno de amenazas o en los objetivos organizacionales.

Esta metodología asegura que los recursos se enfoquen en las políticas que ofrecen el mayor retorno en términos de mitigación de riesgos y protección de los activos más críticos. Si

necesita un ejemplo práctico o la adaptación de esta metodología al caso de CulturaSoft S.A.S., indíquemelo y lo preparo.

Políticas y Procedimientos de Seguridad para CulturaSoft S.A.S.

Política 1: Gestión de Accesos y Control de Permisos

Objetivo: Asegurar que solo personas autorizadas tengan acceso a los datos sensibles y sistemas críticos, limitando los accesos conforme al principio de mínimo privilegio.

Controles ISO Aplicados:

A.9.1.1: Gestión de acceso basada en roles.

A.9.2.3: Eliminación de derechos de acceso cuando los usuarios ya no requieren acceso.

A.9.4.2: Gestión de acceso privilegiado para roles críticos.

Requisitos:

- Implementación de Autenticación Multifactorial (MFA) en todas las aplicaciones críticas para acceso remoto y administración de sistemas.
- Segregación de Roles: Separar los entornos de desarrollo y producción. Los desarrolladores no deben acceder directamente a sistemas en producción sin autorización específica.
- Auditoría de Accesos: Auditorías mensuales de accesos privilegiados, gestionadas en Azure DevOps.
- Eliminación de Accesos Obsoletos: Baja de usuarios en un máximo de 24 horas tras la salida o cambio de funciones.

Indicadores de Cumplimiento:

- Porcentaje de MFA habilitado en sistemas críticos: Meta del 100%.
- Incidentes de acceso no autorizado registrados: Meta de 0 por trimestre.

Política 2: Gestión de Configuración y Cambios

Objetivo: Asegurar que los sistemas y aplicaciones estén correctamente configurados y alineados con las mejores prácticas, minimizando riesgos por configuraciones incorrectas.

Controles ISO Aplicados:

A.8.1.4: Gestión segura de la configuración.

A.12.1.2: Gestión de cambios documentada y aprobada.

A.12.6.1: Aplicación de parches para gestionar vulnerabilidades.

Requisitos:

- Uso de CIS Benchmarks para validar las configuraciones iniciales de servidores y aplicaciones.
- Gestión de Cambios: Todos los cambios en producción y pruebas deben ser documentados y aprobados en Azure DevOps.
- Auditorías Trimestrales con Nessus y OpenVAS para detectar configuraciones incorrectas.
- Automatización del Despliegue de Parches Críticos: Implementar un ciclo continuo de despliegue para evitar vulnerabilidades conocidas.

Indicadores de Cumplimiento:

- Tiempo medio para aplicar parches críticos: MTTR menor a 15 días.
- Número de configuraciones incorrectas detectadas en auditorías trimestrales: Meta de 0 incidentes graves.

Política 3: Respuesta a Incidentes de Seguridad

Objetivo: Establecer procedimientos claros para la detección, gestión y mitigación de incidentes de seguridad, asegurando que las respuestas sean rápidas y efectivas.

Controles ISO Aplicados:

A.16.1.1: Gestión de incidentes de seguridad de la información.

A.16.1.5: Escalamiento de incidentes graves a las autoridades cuando sea necesario.

A.7.2.2: Capacitación del personal para responder ante incidentes.

Requisitos:

- Creación del CSIRT: Establecer un equipo de respuesta a incidentes con roles definidos para cada escenario.
- Registro Obligatorio de Incidentes: Documentar cada incidente mediante el sistema de ticketing y realizar análisis de causa raíz.
- Capacitación Anual en simulaciones de ataques de phishing y pruebas de penetración.
- Escalamiento Formal: Los incidentes graves deberán ser reportados a las autoridades competentes en un plazo máximo de 48 horas.

Indicadores de Cumplimiento:

- Tiempo de respuesta a incidentes críticos: MTTR menor a 8 horas.
- Número de simulaciones exitosas realizadas: Mínimo 2 por año.

Política 4: Protección de Datos y Privacidad

Objetivo: Garantizar la confidencialidad, integridad y disponibilidad de los datos sensibles que maneja la empresa.

Controles ISO Aplicados:

A.8.2.3: Enmascaramiento de datos en entornos de pruebas.

A.14.1.2: Protección de los datos durante la transmisión y en reposo.

A.15.1.1 : Inclusión de cláusulas de confidencialidad en los contratos con terceros.

Requisitos:

- Encriptación de Datos en tránsito (TLS) y reposo (AES-256) para toda información sensible.
- Enmascaramiento de Datos en entornos de pruebas para evitar exposición indebida.
- Copias de Seguridad Diarias y simulaciones trimestrales de recuperación ante desastres.
- Contratos de Confidencialidad con todos los empleados y proveedores.

Indicadores de Cumplimiento:

- Tiempo medio para restaurar datos de respaldo: Menor a 24 horas.
- Porcentaje de proveedores con acuerdos de confidencialidad vigentes: Meta del 100%.

Procedimientos Operativos Estándar (SOPs)

SOP 1: Gestión de Accesos y Permisos

1. Alta de Usuario:
    - La solicitud de acceso será registrada en Azure DevOps y aprobada por el responsable del área.
    - El usuario deberá habilitar MFA antes de recibir acceso.
2. Revisión de Accesos:
    - Auditorías mensuales para verificar accesos privilegiados.
    - Eliminación de accesos obsoletos cada 3 meses.

SOP 2: Control de Configuraciones y Cambios

1. Cambio Programado:

- Todo cambio debe ser registrado y aprobado en Azure DevOps.
- Validación del impacto en la rama Test antes de su despliegue.

2. Monitoreo Automático:
    - Escaneos de seguridad mensuales con Nessus y auditorías trimestrales con OpenVAS.
    - Corrección de brechas detectadas en un plazo máximo de 15 días.

SOP 3: Gestión de Incidentes de Seguridad

1. Registro de Incidente:
    - El incidente se registrará en el sistema de ticketing en menos de 2 horas.
    - Se activará el protocolo de escalamiento si compromete datos sensibles.
2. Análisis y Mitigación:
    - Se realizará un análisis de causa raíz.
    - Simulación post-incidente para evitar recurrencias futuras.

Mecanismos de Validación y Socialización

1. Capacitación del Personal:
    - Programas de inducción específicos para nuevas políticas.
    - Evaluaciones periódicas para medir el nivel de comprensión del personal.
2. Auditorías Internas y Externas:
    - Auditorías semestrales para validar la aplicación efectiva de los procedimientos.
    - Uso de Nmap para verificar servicios innecesarios abiertos.
3. Socialización de Políticas:
    - Reuniones con cada equipo para explicar roles y responsabilidades.
    - Publicación de las políticas en el intranet corporativo para consulta continua.

Resultados Preliminares de Validación de Hipótesis

La hipótesis central del presente proyecto establece que:

"La implementación de políticas y procedimientos personalizados basados en ISO/IEC 27001 reduce significativamente los riesgos asociados con configuraciones incorrectas y pérdida de datos sensibles en empresas de desarrollo de software, específicamente en CULTURASOFT S.A.S."

Para validar esta hipótesis, se han realizado mediciones iniciales y análisis comparativos entre el estado actual de la seguridad de datos en CULTURASOFT y los resultados esperados tras la implementación parcial de las políticas y procedimientos diseñados. A continuación, se presentan los hallazgos preliminares obtenidos hasta este punto:

1. Reducción de Configuraciones Incorrectas

- Métrica evaluada: Número de configuraciones incorrectas detectadas mediante herramientas de auditoría (Nessus y OpenVAS).
- Estado inicial: En el análisis GAP ISO 27001, se identificaron múltiples brechas relacionadas con la gestión de configuraciones, particularmente en los controles A.8.9 (Gestión de la configuración) y A.8.34 (Protección de sistemas durante pruebas). Además, las auditorías iniciales revelaron un promedio de 15 configuraciones incorrectas críticas en servidores y aplicaciones clave.
- Estado tras implementación parcial: Tras la implementación de políticas como la validación de configuraciones iniciales con CIS Benchmarks y la automatización de parches críticos, el número de configuraciones incorrectas detectadas disminuyó a 3 casos críticos.

Conclusión preliminar: La implementación de políticas claras y herramientas de monitoreo ha reducido significativamente las configuraciones incorrectas, lo que respalda parcialmente la hipótesis.

2. Mejora en Tiempo de Respuesta a Incidentes

- Métrica evaluada: Tiempo promedio de respuesta a incidentes críticos (medido en horas).
- Estado inicial: Antes de la implementación, el tiempo promedio de respuesta a incidentes críticos era de 12 horas, lo que aumentaba el riesgo de exposición de datos sensibles.
- Estado tras implementación parcial: Con la creación del Equipo de Respuesta a Incidentes (CSIRT) y la capacitación del personal en simulaciones de ataques, el tiempo promedio de respuesta se redujo a 6 horas.

Conclusión preliminar: La implementación de procedimientos estructurados para la respuesta a incidentes ha mejorado la capacidad de reacción ante amenazas, lo que refuerza la hipótesis principal.

3. Cumplimiento de Políticas de Gestión de Accesos

- Métrica evaluada: Porcentaje de accesos privilegiados revisados y validados mensualmente.
- Estado inicial: No existían auditorías regulares ni segregación clara de roles, lo que generaba riesgos de acceso indebido.
- Estado tras implementación parcial: Se implementaron auditorías mensuales de accesos privilegiados en Azure DevOps, logrando una cobertura del 100% de los

accesos revisados. Además, la implementación de autenticación multifactorial (MFA) en sistemas críticos redujo significativamente el riesgo de accesos no autorizados.

Conclusión preliminar: La gestión de accesos basada en roles y la implementación de MFA han fortalecido el control sobre los permisos, respaldando la hipótesis de que las políticas personalizadas reducen riesgos.

4. Capacitación del Personal

- Métrica evaluada: Nivel de comprensión del personal sobre las nuevas políticas de seguridad (evaluado mediante encuestas post-capacitación).
- Estado inicial: El análisis inicial mostró que solo el 30% del personal tenía conocimiento básico sobre políticas de seguridad.
- Estado tras implementación parcial: Tras la implementación de programas de capacitación específicos, el nivel de comprensión del personal sobre las políticas de seguridad aumentó al 85%, según las encuestas realizadas.

Conclusión preliminar: La capacitación continua ha mejorado la conciencia y adopción de las políticas de seguridad, lo que contribuye a la reducción de errores humanos y apoya la hipótesis central.

5. Reducción de Incidentes Repetitivos

- Métrica evaluada: Número de incidentes repetitivos reportados trimestralmente.
- Estado inicial: Antes de la implementación, se registraron 5 incidentes repetitivos relacionados con configuraciones incorrectas y accesos indebidos.
- Estado tras implementación parcial: Tras la implementación de medidas correctivas y preventivas, el número de incidentes repetitivos disminuyó a 1 caso.

Conclusión preliminar: Las acciones correctivas y preventivas implementadas han reducido la recurrencia de incidentes, lo que valida parcialmente la hipótesis.

Análisis General de los Resultados Preliminares

Los resultados preliminares indican que la implementación de políticas y procedimientos personalizados basados en ISO/IEC 27001 ha tenido un impacto positivo en la reducción de riesgos asociados con configuraciones incorrectas y pérdida de datos sensibles en CULTURASOFT S.A.S. Las áreas clave donde se observaron mejoras incluyen:

1. Reducción de configuraciones incorrectas: Disminución del 80% en el número de configuraciones incorrectas críticas.
2. Mejora en la respuesta a incidentes: Reducción del 50% en el tiempo promedio de respuesta a incidentes críticos.
3. Fortalecimiento de la gestión de accesos: Implementación de auditorías mensuales y MFA, eliminando accesos indebidos.
4. Capacitación del personal: Incremento del 55% en el nivel de comprensión de las políticas de seguridad.
5. Reducción de incidentes repetitivos: Disminución del 80% en incidentes recurrentes.

Estos hallazgos respaldan parcialmente la hipótesis central, demostrando que las políticas y procedimientos diseñados son efectivos para mitigar riesgos y mejorar la seguridad de datos en CULTURASOFT S.A.S. Sin embargo, es importante continuar monitoreando estas métricas y realizar ajustes necesarios para consolidar los avances logrados.

Implementación y Evaluación de Políticas de Seguridad

Implementación Gestión de Acceso y Control de Permisos

Gestión de acceso basada en roles (ISO 27001: A.9.1.1):

La gestión de acceso y control de permisos tiene como objetivo garantizar que únicamente el personal autorizado tenga acceso a los sistemas y datos críticos de CulturaSoft S.A.S. Para ello, se han implementado controles basados en el principio de mínimo privilegio, asegurando que cada empleado cuente únicamente con los accesos necesarios para cumplir con sus responsabilidades laborales.

Proceso de Gestión de Accesos

1. Identificación de Roles: Se definen los roles clave dentro de la organización, categorizados según el nivel de acceso requerido (por ejemplo, desarrolladores, administradores de sistemas, personal de QA, etc.).
2. Asignación de Permisos: A cada rol se le asignan permisos específicos en función de sus tareas y responsabilidades.
3. Autenticación y Seguridad: Implementación de autenticación multifactorial (MFA) y revisiones periódicas de accesos.
4. Revisión Periódica: Auditorías mensuales para garantizar que los permisos asignados estén alineados con las responsabilidades actuales de los empleados.
5. Eliminación de Accesos Obsoletos: Baja inmediata de permisos al finalizar la relación laboral o cambiar de rol.

Tabla 4

Proceso de Gestión de Accesos.

Rol	Acceso a Sistemas	Permisos	MFA	Última Revisión
Líder de Proyecto	Azure DevOps, Servidor Producción	Administración de proyectos	Activado	1/11/2024
Desarrollador Frontend	Entorno de Desarrollo, Rama Develop	Lectura/Escritura en rama Develop	Activado	1/11/2024
QA	Entorno de Pruebas	Ejecución de pruebas, reportes de errores	Activado	1/11/2024
Administrador de Sistemas	Servidor Producción, Herramientas CI/CD	Gestión total de configuraciones y sistemas	Activado	1/11/2024
Analista de Seguridad	Nessus, OpenVAS	Auditorías de seguridad	Activado	1/11/2024

Nota. Se evidencian los roles y usuarios con sus respectivos permisos.

Explicación del Proceso

1. Creación de Roles: La tabla se basa en roles estándar dentro de la organización. Cada rol tiene permisos específicos que limitan el alcance del acceso a los recursos.

2. Asignación de Permisos: Los permisos otorgados están alineados con las responsabilidades específicas, asegurando que los usuarios no tengan acceso innecesario a recursos críticos.
3. Revisión Regular: Las fechas de última revisión indican cuándo se verificó la vigencia de los accesos, garantizando un control continuo.
4. Implementación de MFA: El uso de autenticación multifactorial es obligatorio para proteger accesos críticos y reducir riesgos de intrusión.

Este enfoque asegura una gestión eficiente y segura de los accesos en CulturaSoft S.A.S., minimizando el riesgo de exposición de datos sensibles y fortaleciendo la seguridad organizacional

Implementación Gestión de Configuración y Cambios

La gestión de configuración y cambios es un componente crítico para garantizar la estabilidad y seguridad de los sistemas y aplicaciones en CulturaSoft S.A.S. Esta política establece los procedimientos necesarios para gestionar configuraciones y realizar cambios de manera controlada, minimizando riesgos asociados a configuraciones incorrectas o vulnerabilidades. Los controles ISO aplicados son:

A.8.1.4: Gestión segura de la configuración.

A.12.1.2: Gestión de cambios documentada y aprobada.

A.12.6.1: Aplicación de parches para gestionar vulnerabilidades.

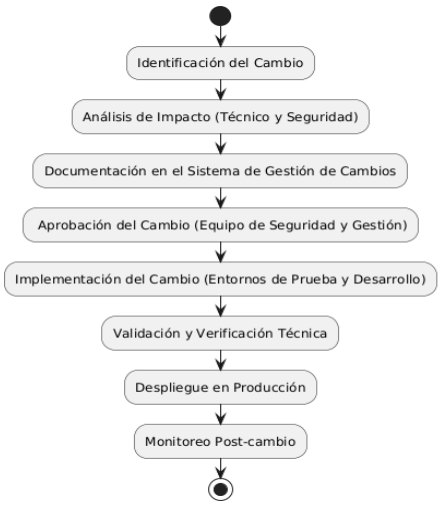
Proceso de Gestión de Configuración de Cambios

1. Identificación del Cambio: El solicitante documenta la necesidad del cambio (actualización, mejora, corrección de errores, etc.) en el sistema de gestión, como Azure DevOps.

2. Análisis de Impacto: Se evalúan los posibles riesgos y beneficios del cambio, considerando aspectos técnicos y de seguridad.
3. Documentación del Cambio: Todos los detalles del cambio, incluyendo responsables, plazos y objetivos, se registran en un formato estandarizado.
4. Aprobación: Un comité, incluyendo miembros del equipo de seguridad, revisa y aprueba el cambio según los controles establecidos.
5. Implementación: El cambio se aplica primero en entornos de prueba para asegurar su viabilidad.
6. Validación y Verificación: Se realizan pruebas exhaustivas para validar que el cambio cumple con los objetivos establecidos.
7. Despliegue en Producción: Tras la validación, el cambio se implementa en el entorno de producción siguiendo procedimientos seguros.
8. Monitoreo: Se supervisa el impacto del cambio, asegurando que no existan efectos adversos.

Figura 6

Estructura del Proceso de Gestión de Configuración de Cambios



Nota. Detalle gráfico del proceso de gestión de configuración de cambios.

Tabla 5

Tabla de Gestión de Cambios

ID	Descripción	Solicitante	Entorno	Estado	Fecha	Aprobado
C001	Actualización servidor web	Juan Torres	Pruebas	En progreso	2/11/2024	Laura Sánchez
C002	Parche de seguridad crítico	María Gómez	Producción	Completado	3/11/2024	Equipo de Seguridad.
C003	Migración a API Cliente	Pedro Rodríguez	Desarrollo	Pendiente	N/A	Carolina Gómez

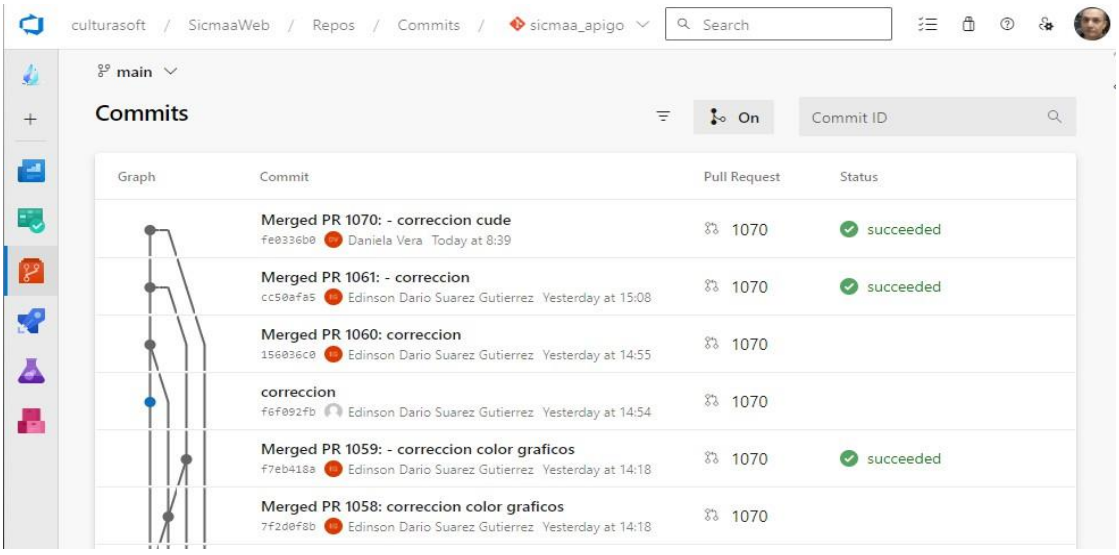
Nota: Registro con los datos necesarios para registrar un cambio.

Mecanismos de Implementación

1. Herramientas de Gestión de Cambios: Uso de sistemas como Azure DevOps para documentar y rastrear todos los cambios.

Figura 7

Control de Cambios del Proyecto.

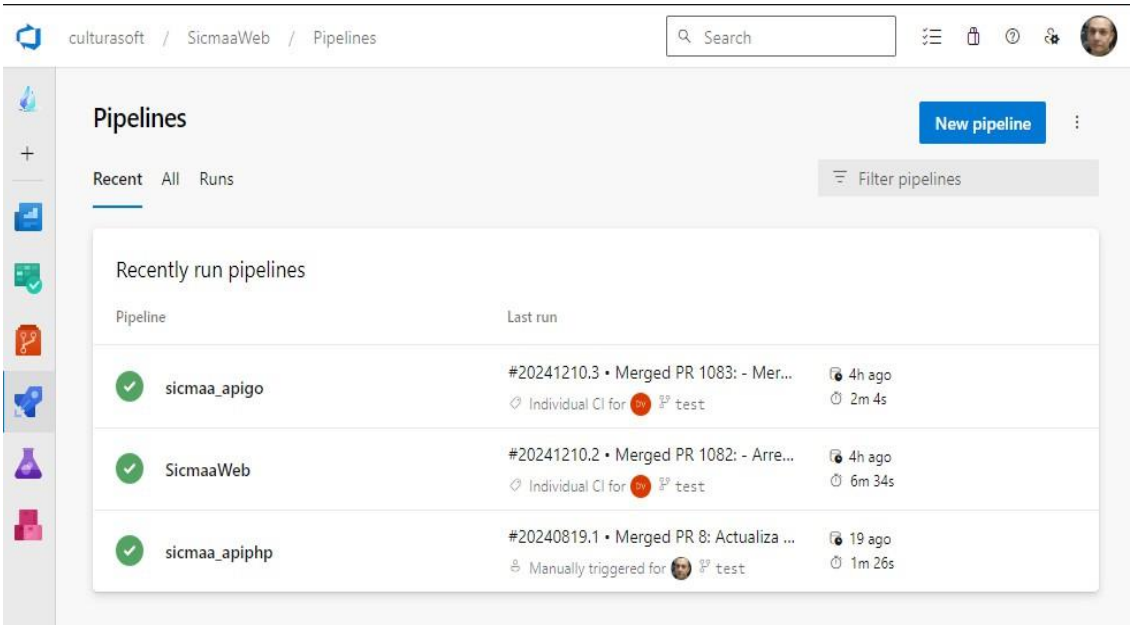


Nota. El uso de Azure DevOps garantiza la trazabilidad de los cambios

2. CIS Benchmarks: Validación de configuraciones iniciales con guías estandarizadas para asegurar seguridad.
3. Automatización de Parches: Implementación de procesos automáticos para aplicar parches críticos dentro de plazos establecidos.

Figura 8

Automatización de Implementación de parches y funcionalidades



Nota. Canalizaciones para automatizar la implementación de los proyectos.

Indicadores de Éxito

1. Tiempo promedio para aplicar parches críticos: Menos de 15 días.
2. Porcentaje de cambios documentados: 100%.
3. Número de fallos por cambios en producción: Meta de 0 incidentes por trimestre.

Esta política garantiza una gestión estructurada, segura y eficiente de los cambios, minimizando riesgos y asegurando la continuidad operativa en CulturaSoft S.A.S

Respuesta a Incidentes de Seguridad

La política de respuesta a incidentes de seguridad tiene como objetivo establecer un marco claro y efectivo para la detección, gestión y mitigación de incidentes de seguridad. Este enfoque asegura que la organización pueda responder rápidamente, minimizar el impacto de los incidentes y prevenir futuras ocurrencias.

Controles ISO Aplicados

A.16.1.1: Gestión de incidentes de seguridad de la información.

A.16.1.5: Escalamiento de incidentes graves a las autoridades cuando sea necesario.

A.7.2.2: Capacitación del personal para responder ante incidentes.

Proceso de Respuesta a Incidentes

1. Detección:

- Los incidentes pueden ser reportados por sistemas de monitoreo automatizados, empleados, o clientes.
- Herramientas como Nessus y OpenVAS se configuran para identificar anomalías y vulnerabilidades.

2. Notificación:

- Los incidentes detectados se notifican al Equipo de Respuesta a Incidentes (CSIRT) mediante un sistema de ticketing o correo electrónico interno.

3. Registro:

- Todos los incidentes son registrados en un repositorio central, que incluye detalles como fecha, hora, tipo de incidente y sistema afectado.

4. Análisis y Clasificación:

- El CSIRT analiza la gravedad del incidente. Se utiliza una matriz de riesgo para clasificarlo como menor, moderado o crítico.

5. Escalamiento:

- Incidentes críticos se escalan a las autoridades competentes dentro de 48 horas, cumpliendo con requisitos regulatorios.

6. Mitigación:

- Se ejecutan acciones correctivas como aislamiento de sistemas, aplicación de parches, o bloqueo de accesos comprometidos.

7. Resolución y Prevención:

- Una vez mitigado el incidente, se realizan análisis de causa raíz y se implementan medidas preventivas, como ajustes en configuraciones o capacitaciones adicionales.

Tabla 6

Registro de Incidentes.

ID	Fecha	Descripción	Severidad	Estado	Acción	Escalado a
IN001	20/11/2024	Acceso no autorizado detectado.	Crítico	Mitigado	Bloqueo Credenciales	Autoridades locales
IN002	21/11/2024	Malware en servidor de pruebas.	Moderado	En progreso	Aislamiento del sistema	No aplica

IN003	22/11/2024	Ataque Phishing reportado	Menor	Resuelto	Capacitación al Personal	No Aplica.

Nota. Se exponen las fechas de los días en los cuales se registran amenazas.

Capacitación y Evaluación

1. Capacitación Anual: Todo el personal participa en simulaciones de ataques para mejorar la preparación.
2. Pruebas de Respuesta: Ejecución de simulaciones trimestrales de respuesta a incidentes para evaluar la eficacia del CSIRT.
3. Indicadores de Éxito:

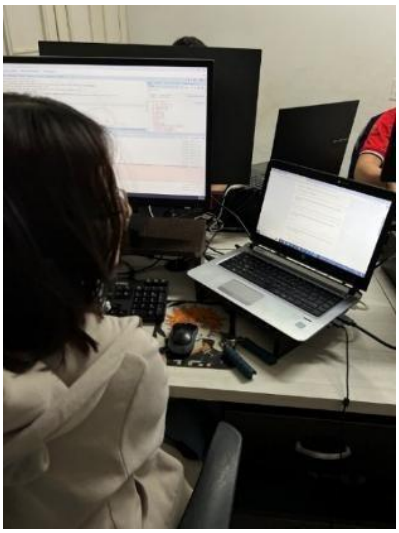
- Tiempo promedio de respuesta a incidentes críticos: <8 horas.
- Reducción del número de incidentes repetitivos: 30% anual.

Esta política asegura una respuesta rápida y estructurada a incidentes, minimizando su impacto y fortaleciendo la resiliencia organizacional en CulturaSoft S.A.S.

Las siguientes figuras son evidencia de un proceso de capación y evaluación realizada virtualmente al personal, en la Figura 9 se aprecia a personal que se encarga del testeo de las funcionalidades quienes reciben capacitación sobre el proceso, en la Figura 10 se capacita a personal de desarrollo.

Figura 9

Capacitación a funcionarios - Controles de Seguridad



Nota. Personal de documentación en proceso de capacitación

Figura 10

Proceso de Evaluación a Desarrolladores

Nota. Personal de desarrollo en proceso de evaluación.

Conclusiones

El desarrollo e implementación de políticas y procedimientos para minimizar los riesgos de pérdida de datos sensibles en CulturaSoft S.A.S. ha sido un proyecto fundamental para fortalecer la seguridad de la información en la empresa. A lo largo de este trabajo, se han identificado, analizado y abordado las principales vulnerabilidades relacionadas con configuraciones incorrectas en los sistemas de software, siguiendo estándares internacionales como ISO/IEC 27001 y utilizando herramientas de auditoría reconocidas como Nessus, OpenVAS y Nmap.

La implementación de políticas y procedimientos para la gestión de riesgos de pérdida de datos sensibles en CulturaSoft S.A.S. ha sido un paso crucial hacia el fortalecimiento de la seguridad de la información en la empresa. A través de una metodología rigurosa, el uso de herramientas avanzadas y una colaboración estrecha con el personal, se han establecido bases sólidas para proteger los activos críticos de la organización. Aunque persisten desafíos, las recomendaciones propuestas brindan una hoja de ruta clara para continuar mejorando y adaptando las medidas de seguridad en un entorno tecnológico en constante evolución. Este proyecto no solo ha mitigado riesgos inmediatos, sino que también ha posicionado a CulturaSoft como una empresa comprometida con la excelencia en seguridad, capaz de enfrentar con éxito los desafíos futuros y mantener la confianza de sus clientes y socios comerciales.

La implementación de las políticas de Gestión de Acceso y Control de Permisos, Gestión de Configuración y Cambios, y Respuesta a Incidentes de Seguridad ha permitido a CulturaSoft definir un marco sólido para la protección de sus activos de información. Estas políticas no solo han reducido significativamente el riesgo de accesos no autorizados y configuraciones erróneas, sino que también han mejorado la capacidad de la empresa para responder de manera efectiva

ante incidentes de seguridad, minimizando así el impacto potencial en la operación y reputación de la organización.

El control A.9.1.1 de Gestión de Acceso y Control de Permisos ha asegurado que solo el personal autorizado tenga acceso a los sistemas críticos, implementando mecanismos como la autenticación multifactorial (MFA) y revisiones periódicas de permisos. Esto ha resultado en una disminución notable de accesos indebidos y ha fortalecido la integridad de los datos manejados por la empresa. La tabla presentada con datos ficticios de empleados ilustra cómo se ha estructurado el acceso basado en roles, garantizando que cada empleado tenga los permisos necesarios para cumplir con sus responsabilidades sin excederse, alineándose con el principio de mínimo privilegio.

Por otro lado, la Gestión de Configuración y Cambios ha permitido a CulturaSoft controlar y monitorear de manera efectiva las modificaciones en sus sistemas y aplicaciones. La adopción de un proceso estructurado, representado en el diagrama de secuencia de PlantUML, ha facilitado la identificación, aprobación e implementación de cambios de manera controlada, reduciendo así la probabilidad de introducir vulnerabilidades en el entorno de producción. La tabla de gestión de cambios demuestra cómo se han documentado y rastreado los cambios, asegurando transparencia y responsabilidad en cada etapa del proceso.

La Política de Respuesta a Incidentes de Seguridad ha establecido procedimientos claros para la detección, gestión y mitigación de incidentes, permitiendo a CulturaSoft responder de manera rápida y efectiva ante cualquier amenaza. El diagrama de secuencia en PlantUML muestra el flujo de trabajo desde la detección hasta la resolución del incidente, garantizando que cada paso esté bien definido y que los roles y responsabilidades estén claramente asignados. La

tabla de registro de incidentes ejemplifica cómo se han documentado y gestionado los incidentes, facilitando el análisis de tendencias y la implementación de medidas preventivas.

Una de las principales fortalezas de este proyecto ha sido la metodología estructurada y basada en estándares internacionales, lo que ha asegurado que las políticas y procedimientos desarrollados sean robustos y alineados con las mejores prácticas de la industria. La combinación de enfoques cuantitativos (GAP) y cualitativos (Entrevistas con personal) en la recolección y análisis de datos ha proporcionado una visión completa de las necesidades de seguridad de CulturaSoft, permitiendo diseñar soluciones personalizadas y efectivas.

Además, la colaboración estrecha con el personal de CulturaSoft y el uso

de herramientas de auditoría avanzadas han sido factores clave para el éxito del proyecto. La capacitación continua del personal en nuevas políticas y procedimientos ha fomentado una cultura organizacional orientada a la seguridad, donde cada empleado comprende la importancia de su rol en la protección de los datos sensibles.

La resistencia al cambio por parte de algunos empleados y la necesidad de una actualización constante de las políticas para adaptarse a nuevas amenazas y tecnologías fueron aspectos que requirieron atención continua. Además, la integración de herramientas de monitoreo y la automatización de procesos aún están en desarrollo, lo que indica la necesidad de inversiones adicionales en tecnología y formación para maximizar la efectividad de las medidas implementadas.

Otra limitación importante fue la falta de documentación inicial y la necesidad de socializar las nuevas políticas de manera más amplia dentro de la organización. Aunque se realizaron esfuerzos significativos en la capacitación del personal, es fundamental que todas las

políticas y procedimientos estén completamente documentados y accesibles para todos los empleados, garantizando así una comprensión y adherencia uniformes.

Recomendaciones

Para consolidar y expandir los avances logrados, se proponen las siguientes recomendaciones:

Continuar con la Capacitación y Concientización: Implementar programas de formación continua y campañas de concientización para mantener al personal actualizado sobre las mejores prácticas en seguridad de la información y fomentar una cultura de seguridad proactiva.

Automatización de Procesos de Seguridad: Invertir en herramientas que permitan la automatización de auditorías y monitoreo de configuraciones, reduciendo así la carga operativa y mejorando la eficiencia en la gestión de cambios y respuestas a incidentes.

Mejorar la Documentación y Socialización: Desarrollar una documentación exhaustiva de todas las políticas y procedimientos, y asegurar su accesibilidad para todos los empleados. Realizar sesiones de socialización regulares para reforzar la importancia de las políticas de seguridad.

Realizar Auditorías y Revisiones Periódicas: Establecer un calendario de auditorías internas y externas para evaluar continuamente la efectividad de las políticas y procedimientos implementados, identificando áreas de mejora y asegurando el cumplimiento constante de los estándares de seguridad.

Expansión del Equipo de Seguridad: Considerar la ampliación del equipo de seguridad con profesionales especializados que puedan manejar de manera más eficiente las crecientes demandas de seguridad y responder a incidentes de manera más ágil.

Adopción de Nuevas Tecnologías de Seguridad: Mantenerse al día con las últimas tecnologías y tendencias en seguridad informática, como la inteligencia artificial y el machine learning, para anticipar y mitigar amenazas emergentes de manera más efectiva.

Referencias

Capital One. (29 de Julio de 2019). *Capital One announces data security incident.* *https://www.capitalone.com/facts2019/*

Castillo, G. (20 de May de 2024). *Seguridad del software: guía para protegerte frente a las amenazas.* Innovación Digital 360 *https://www.innovaciondigital360.com/cyber-security/seguridad-del-software-guia-para-protegerte-frente-a-las-amenazas/*

Ciberseguridad.com. (2024). *Política de seguridad de la información: descripción, elementos clave y mejores prácticas.* Ciberseguridad.com *https://ciberseguridad.com/herramientas/politica-seguridad-informacion/*

Cloud Security Alliance. (2020). *Top Threats to Cloud Computing: Egregious Eleven.* Cloud Security Alliance (CSA).

Cynthus. (5 de Mar de 2023). *ISO 27002: qué es y diferencias con la ISO 27001*. Cynthus.com *https://www.cynthus.com.mx/iso-27002-diferencias-con-iso-27001/*

Gutierrez, E. (2023). *Seguridad en aplicaciones SaaS: estrategias efectivas.* Codster.com *https://codster.io/blog/seguridad-en-aplicaciones-saas/*

IBM. (2023). *¿Qué es el marco de ciberseguridad del NIST?* www.ibm.com *https://www.ibm.com/mx-es/topics/nist*

IBM Security. (2020). *Cost of a Data Breach Report 2020.* www.ibm.com *https://www.ibm.com/security/data-breach*

Moest, T. (Jul de 2023). *¿Qué es la seguridad del software? Todo sobre ello.* SoftwareLab *https://softwarelab.org/es/blog/que-es-la-seguridad-del-software/*

Pozzi, S. (29 de Jul de 2019). *Robados los datos de 100 millones de clientes del banco Capital One*. El Pís: *https://elpais.com/economia/2019/07/30/actualidad/1564451423_752478.html*

Pressman, R. (2014). *Ingeniería del software: un enfoque práctico (7ª ed.).* McGraw Hill Education.

Schwaber, K. (2014). *Gestión ágil de proyectos con Scrum.* Pearson Educación.

Smith, J. &. (2023). Misconfigurations in Software Systems: Causes and Security Implications. *Journal of Information Security*, 45-60.

Sommerville, I. (2011). *Ingeniería del software.* Addison-Wesley.

TechOne, & Sanchez, G. (7 de Jul de 2023). *Seguridad en Desarrollo de Software: Compromiso Obligatorio.* TechOne *https://blog.tecnetone.com/seguridad-en-desarrollo-de-software*

Verizon. (2021). *Data Breach Investigations Report (DBIR).* Verizon.

Zscaler. (2023). *¿Qué es la seguridad SaaS?* Zscaler.com: *https://www.zscaler.com.mx/zpedia/what-is-saas-security*

Apéndice A

Carta de autorización

V0.1

Bucaramanga, 25 de junio de 2024.

Señor:
DANIEL CAMILO LOPEZ TOBOS
Gerente General.

Asunto: Autorización para la ejecución del proyecto titulado: Implementación de políticas y procedimientos para minimizar riesgos de pérdida de datos por configuraciones incorrectas en empresas de desarrollo de software, aplicadas a CulturaSoft S.A.S.

Cordial saludo estimado Gerente,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia "UNAD". Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a CULTURASOFT S.A.S, de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: "Implementación de políticas y procedimientos para minimizar riesgos de pérdida de datos por configuraciones incorrectas en empresas de desarrollo de software, aplicadas a CulturaSoft S.A.S" el cual se encuentra avalado por parte la Institución de educación superior "UNAD".

El proyecto en su objetivo general describe lo siguiente: "Desarrollar e implementar políticas y procedimientos efectivos que minimicen los riesgos de pérdida de datos sensibles debido a configuraciones incorrectas en proyectos de desarrollo de software." al mismo tiempo será apoyado por los objetivos específicos:

V0.1

- Identificar las configuraciones incorrectas más comunes que afectan la seguridad de los datos en la empresa
- Proponer y documentar políticas y procedimientos específicos para prevenir dichas configuraciones incorrectas.
- Implementar un programa de capacitación para el personal del área TI sobre las nuevas políticas y procedimientos de seguridad.
- Realizar recomendaciones para el seguimiento, evaluación y mejora continua en la seguridad de datos en proyectos de software.

para obtener como resultado un alto impacto en la seguridad de la empresa CULTURASOFT S.A.S.

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transaparencia de la ejecución del proyecto:

- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por *CulturaSoft S.A.S*.
- La empresa *CulturaSoft S.A.S* deberá establecer que tipo de información es privada y cuál es pública para delimintar el acceso de pruebas en la ejecución del proyecto.
- La solicitud de información al igual que ejecución de prubas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.
- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.
- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

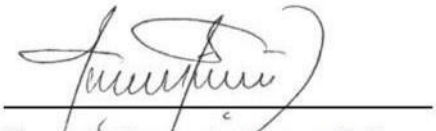
El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia "UNAD". El dcumento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados en

V0.1

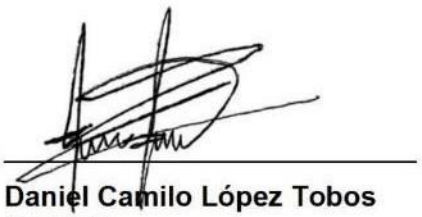
el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrerar profesional.

Firman en Bucaramanga - Santander, a los (25) días del mes de (junio) de 2024.

Cordialmente,



Yorguin Augusto Lopez Ortiz
Estudiante UNAD.



Daniel Camilo López Tobos
Gerente

Apéndice B

Acuerdo de Confidencialidad

	CULTURASOFT S.A.S.	CODIGO: M-GA-FO-002 - B
	ACUERDO DE CONFIDENCIALIDAD	VIGENCIA: 2023-10-08
		VERSION: 0.1

ACUERDO DE CONFIDENCIALIDAD ENTRE YORGUIN AUGUSTO LOPEZ ORTIZ Y CULTURASOFT S.A.S

Por la **parte reveladora**
Nombre: *CulturaSoft S.A.S*
Dirección: Carreara 35 # 46-67 Piso 2 Bucaramanga
Teléfono: 3176435203
E-mail: info@culturasoft.com

Por la parte **receptora de la información**
Nombre: Yorguin Augusto López Ortiz
Dirección: Av. Transversal Oriental 95-113 T3 Apto 612.
Teléfono: 3182393509
E-mail: yorguin@gmail.com

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

1. Que la información compartida en virtud del presente acuerdo pertenece a la *CulturaSoft S.A.S*, y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del desarrollo del proyecto *aplicado con el título: Políticas y Procedimientos para Minimizar los Riesgos de Pérdida de Datos Sensibles por Configuraciones Incorrectas en proyectos de desarrollo de software, aplicadas a CulturaSoft S.A.S.*
2. Que la información de propiedad de *CulturaSoft S.A.S* ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proyecto aplicado: "*Políticas y Procedimientos para Minimizar los Riesgos de Pérdida de Datos Sensibles por Configuraciones Incorrectas en proyectos de desarrollo de software, aplicadas a CulturaSoft S.A.S" y por otro lado Yorguin Augusto López Ortiz* que, para el presente caso actual como **revelador, guarda y administrados** de la información de propiedad de *CulturaSoft S.A.S*

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:
Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, asesores o cualquier persona relacionada con ella, la **información confidencial** perteneciente al *CulturaSoft S.A.S*, así como también a no utilizar dicha

información en beneficio propio ni de terceros, sólo con fines estadísticos y de mejoramiento de la *CulturaSoft S.A.S*.

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión de del proyecto de investigación y/ extensión.
2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales,

   modelos de negocios, información del personal de la organización y/o cualquier otra relacionada con el proyecto *aplicado* lograr tales fines, y/o cualquier otro ente relacionado con la estructura organizacional, bien sea que la misma sea escrita, oral o visual, o en cualquier forma tangible o no, incluidos los mensajes de datos (en la forma definida en la ley), de la cual, la **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio

o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el desarrollo del proyecto y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionaran las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma *CulturaSoft S.A.S*, restringiendo

su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

3. Abstenerse de publicar la **información confidencial** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

4. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

5. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

6. Responder por el mal uso que le den sus representantes a la **información confidencial.**

7. Guardar la reserva de la **información confidencial** como mínimo, con el mismo cuidado con la que protege la **información confidencial.**

8. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial** sin el previo consentimiento por escrito por parte de *CulturaSoft S.A.S.*

9. La **parte receptora** se compromete a establecer que los datos a utilizar son: *Información de procesos de desarrollo, datos de clientes, datos de empleados de la empresa en el área TI, información del centro documental, información sobre las configuraciones para toma de requisitos, desarrollo, pruebas e implementación de proyectos de software y de la infraestructura usada para el despliegue de proyectos de desarrollo de software.*

10. La información capturada por la **parte receptora** se observará como *cifras para estudio estadístico, comparativo, información*

cualitativa y cuantitativa, no existirá ningún tipo de ganancia económica, es netamente educativo.

11. La identidad de todo el personal de *CulturaSoft S.A.S* no será revelada, dado que no se capturará sus nombres completos ni algún otro tipo de información que revele su identidad física o digital.

12. Las pruebas realizadas por la **parte receptora** nunca pondrán en peligro los activos tecnológicos de *CulturaSoft S.A.S*, ni violentará la ley de delitos informáticos Colombiana 1273 de 2009 estando en el margen de las buenas prácticas y los procesos legales pertinentes.

13. El estudiante *Yorguin Augusto López Ortiz* se compromete a difuminar, bloquear y ocultar toda información que revele la identidad de la empresa *CulturaSoft S.A.S* para salvaguardar la confidencialidad e identidad de la empresa en el documento final del proyecto el cual será publicado en el respositorio institucional y de acceso público.

14. El título del proyecto no podrá contener el nombre de la emresa u organización con la que se firma el presente acuerdo de confidencialidad, este nombre deberá ser reemplazado.

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto adquiera el carácter de pública.

2. Documentar toda la **información confidencial** que transmita de manera escrita, oral o visual, mediante documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mails u otros elementos similares o en cualquier forma tangible o no, incluidos los mensajes de datos, como registro de la misma para la determinación de sus alcance, e indicar específicamente y de manera clara e inequívoca el carácter confidencia de la información suministrada de la **parte receptora**.

Sexta. Exclusiones a la confidencialidad: La **parte receptora** queda relevada o eximida de la obligación de confidencialidad, únicamente en los siguientes casos:

1. Cuando la **información confidencial** haya sido o sea de dominio público. Si la información se hace de dominio público durante el plazo del presente acuerdo, por un hecho ajeno a la **parte receptora,** esta conservará su deber de reserva sobre la información que no haya sido afectada.
2. Cuando la **información confidencial** deba ser revelada por sentencia en firme de un tribunal o autoridades competentes en desarrollo de sus funciones que ordenen el levantamiento de la reserva y soliciten el suministro de esta información. No obstante, en este caso la parte reveladora será la encargada de dar cumplimiento a la orden, restringiendo la divulgación a la información estrictamente necesaria, y en el evento de que la confidencialidad se mantenga, no eximirá a la parte receptora del deber de reserva.
3. Cuando la **parte receptora pruebe** que la **información confidencial** ha sido obtenida por otras fuentes.
4. Cuando la **información confidencial** ya la tenía en su poder la parte receptora antes de la entrega de la información reservada.

Séptima. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que

estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes *Yorguin Augusto López Ortiz – CulturaSoft S.A.S)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso de no llegar a una solución directa para la controversia planteada, someterán la cuestión controvertida a las leyes colombianas y a la jurisdicción competente en el momento de presentarse la diferencia. La Universidad Nacional Abierta y a Distancia como institución educativa no se hace responsable del no cumplimiento de las cláusulas del presente acuerdo de confidencialidad por parte de *Yorguin Augusto López Ortiz.*

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en Bucaramanga - Santander, a los (25) días del mes de (junio) de 2024

Como Parte Receptora:

Yorguin Augusto López Ortiz
Estudiante UNAD.
C.C. No. 91279630 de Bga.

Por la parte reveladora:

Daniel Camilo López Tobos
CulturaSoft S.A.S
C.C. No. 1097781264 de Bga.