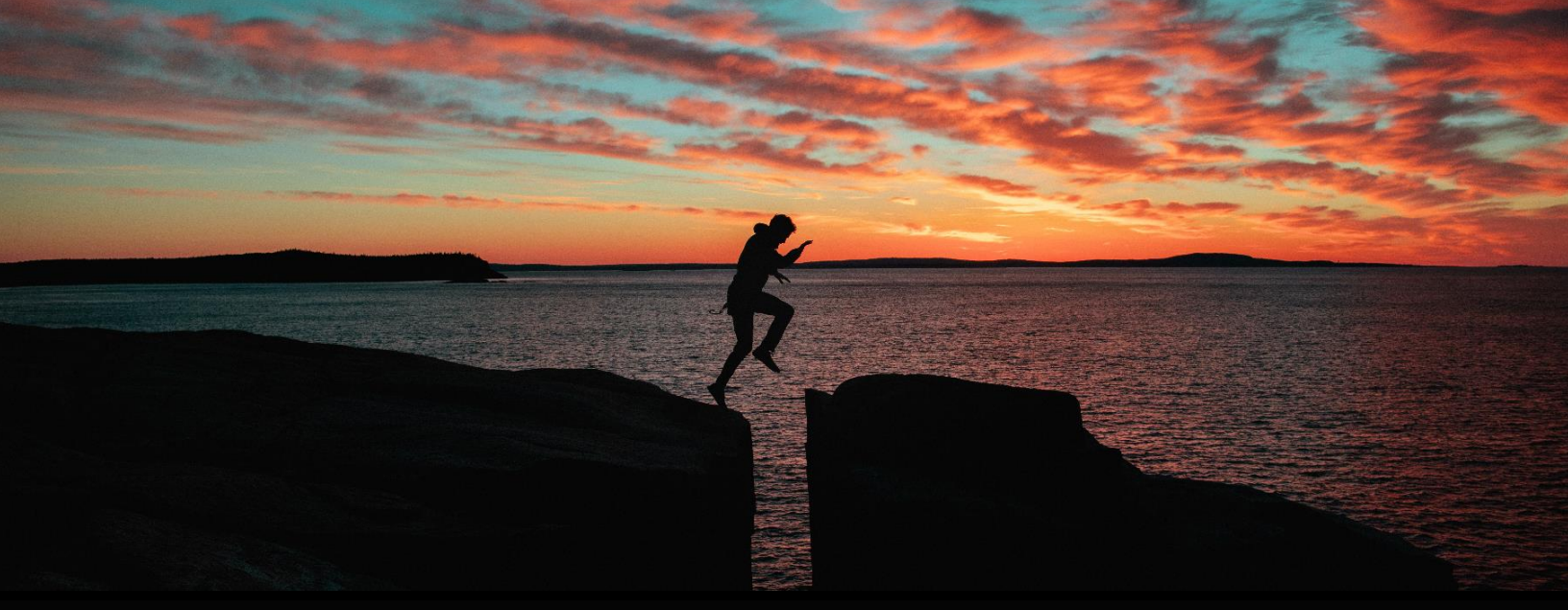


MÁSTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES (MISTIC)

Plan de Implementación del Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2013

Estudiante: Jorge Andrés Correa Morales

Director: Antonio José Segovia Henares

Empresa: Consultora JC S.A.S.

Mayo 2019

Photo by Kristopher Roller on Unsplash

Resumen

Este trabajo recoge la experiencia obtenida durante el transcurso del Máster; los diferentes aspectos técnicos y metodológicos estudiados apoyaron el diseño y desarrollo del plan de implementación del Sistema de Gestión de Seguridad de la Información (SGSI), objeto del presente documento. En concreto, el plan de implementación se desarrolló para una empresa ficticia del sector de la consultoría llamada *Consultora JC S.A.S.* En este documento se describen las principales características de la empresa, y se realiza un diagnóstico inicial de su estado de seguridad de la información tomando como referencia la norma NTC-ISO-IEC 27001:2013. Así mismo, en el marco del plan de implementación del Sistema de Gestión de Seguridad de la Información, se desarrolló la política general de seguridad y los procedimientos principales para su operación. De igual forma, se definió la metodología para el análisis y gestión de riesgos de Seguridad de la Información con base en las normas NTC-ISO 31000:2009 y NTC-ISO 27005:2008 y los respectivos indicadores para medir el desempeño del Sistema. Como mecanismo fundamentar dentro de la estrategia de seguridad de la información, se ejecutó un análisis de riesgos que permitió establecer trece proyectos encaminados a la implementación de controles de seguridad para garantizar la protección de la información, estableciendo los elementos necesarios para la operación del sistema en un esquema de optimización de recursos y mejora continua.

Summary

This document consolidates the experience obtained studying the mastery; Different technical and methodological aspects studied helped to design and development the implementation plan of the Information Security Management System (ISMS), which is the subject of this document. Specifically, the implementation plan was developed for a fictitious consultancy company called *Consultora JC S.A.S.* This document describes the main characteristics of the company, and the results of the initial diagnosis about its information security status, regarding the NTC-ISO-IEC 27001: 2013 standard. Likewise, within the ISMS implementation plan work, the general security policy and the main procedures for its operation were developed. Also, the information security risks management methodology was defined based on the standards NTC-ISO 31000: 2009 and NTC-ISO 27005: 2008. The indicators to measure the performance of the System were defined too. As an essential mechanism within the information security strategy, a risk analysis was carried out, and its results allowed to establish thirteen projects related to the implementation of security controls to guarantee the information protection, establishing the necessary elements for the operation of the system in an environment of resource optimization and continuous improvement.

TABLA DE CONTENIDO

1 INTRODUCCIÓN

El documento se ha desarrollado como memoria del Trabajo Final del Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones, en el cual se desarrolló el Plan de implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma NTC-ISO-IEC 27001:2013 de la empresa **Consultora JC S.A.S.**[1]

Como documentos de referencia normativa se han tomado las versiones vigentes en Colombia de las siguientes normas y guías técnicas publicadas por el Icontec[2]:

- NTC-ISO-IEC 27001:2013
- GTC-ISO-IEC 27002:2013
- NTC-ISO 31000:2009
- NTC-ISO-IEC 27005:2008

2 DEFINICIONES

Aceptación del riesgo[3]: Decisión informada para tomar un riesgo en particular.

Actitud hacia el riesgo[4]: Enfoque de la organización para evaluar y eventualmente buscar, retener, tomar o alejarse del riesgo.

Activo[5]: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Amenaza[6]: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

Ataque[7]: Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera.

Auditoría de seguridad: Estudio y examen independiente del historial y actividades de un sistema de información, con la finalidad de comprobar la idoneidad de los controles del sistema, asegurar su conformidad con la estructura de seguridad y procedimientos operativos

[1] El trabajo se ha desarrollado con base en la información de una empresa real y sus datos sensibles se han modificado para proteger su confidencialidad

[2] Instituto Colombiano de Normas Técnicas y Certificación

[3] (ISO-IEC 27000, 2014)

[4] (NTC-ISO 31000, 2009)

[5] (Ministerio de Hacienda y Administraciones Públicas, 2012)

[6] (Ministerio de Hacienda y Administraciones Públicas, 2012)

[7] (Ministerio de Hacienda y Administraciones Públicas, 2012)

establecidos, a fin de detectar brechas en la seguridad y recomendar cambios en los procedimientos, controles y estructuras de seguridad.

Confidencialidad[8]: Propiedad de que la información no esté disponible o no sea divulgada a personas, entidades o procesos no autorizados.

Contexto externo[9]: Ambiente externo en el cual la organización busca alcanzar sus objetivos.

Contexto interno[10]: Ambiente interno en el cual la organización busca alcanzar sus objetivos.

Control de seguridad[11]: Controles administrativos, operativos y técnicos (por ejemplo, salvaguardas y contramedidas) prescritos para un sistema de información a fin de proteger la confidencialidad, integridad y disponibilidad del sistema y su información.

Declaración de aplicabilidad[12]: Documento formal en el que, para un conjunto de salvaguardas, se indica sin se aplican en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.

Disponibilidad[13]: Propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada.

Gestión de riesgos[14]: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Impacto[15]: Consecuencia que sobre un activo tiene la materialización de una amenaza.

Incidente de seguridad de la información[16]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad[17]: Propiedad de exactitud y completitud.

Parte involucrada (interesada)[18]: Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada por una decisión o actividad.

Probabilidad[19]: Oportunidad de que algo suceda.

---

[8] (ISO-IEC 27000, 2014)

[9] (NTC-ISO 31000, 2009)

[10] (NTC-ISO 31000, 2009)

[11] (National Institute of Standards and Technology (NIST), 2013)

[12] (Ministerio de Hacienda y Administraciones Públicas, 2012)

[13] (ISO-IEC 27000, 2014)

[14] (NTC-ISO 31000, 2009)

[15] (Ministerio de Hacienda y Administraciones Públicas, 2012)

[16] (ISO-IEC 27000, 2014)

[17] (ISO-IEC 27000, 2014)

[18] (NTC-ISO 31000, 2009)

[19] (NTC-ISO 31000, 2009)

Propietario del riesgo[20]**:** Persona o entidad con la responsabilidad y autoridad para gestionar un riesgo.

Proyecto de seguridad[21]**:** Agrupación de tareas orientadas a tratar el riesgo del sistema. La agrupación se realiza por conveniencia, bien porque se trata de tareas que en singular carecerían de eficacia, bien porque se trata de tareas con un objetivo común, bien porque se trata de tareas que competen a una única unidad de acción.

Riesgo[22]**:** Efecto de la incertidumbre sobre los objetivos.

Riesgo residual[23]**:** Riesgo remanente después del tratamiento del riesgo.

Tratamiento del riesgo[24]**:** Proceso para modificar el riesgo. El tratamiento del riesgo puede implicar:

- Evitar el riesgo.
- Tomar o incrementar el riesgo.
- Retirar la fuente del riesgo.
- Cambiar la probabilidad.
- Cambiar las consecuencias.
- Compartir el riesgo con una o varias de las partes.
- Retener o aceptar el riesgo a través de la decisión informada.

3 ESTÁNDARES DE LA SERIE ISO 27000

3.1 NTC[25]-ISO-IEC 27001:2013

La norma NTC-ISO-IEC 27001:2013 (actualizada el 11 de diciembre de 2013) corresponde a la "adopción idéntica por traducción" del estándar internacional ISO/IEC 27001:2013, en la cual se establecen los requisitos para los Sistemas de Gestión de Seguridad de la Información (SGSI). Esta norma tiene como origen la BS 7799-1 de 1995 en la que se definían las mejores prácticas para ayudar a las empresas a administrar la seguridad de la información en la Gran Bretaña (el documento lo generó la entidad normalizadora británica BSI); posteriormente, en la segunda parte (BS 7799-2), se establecieron los requisitos para establecer un Sistema de Gestión de Seguridad de la Información certificable. En el año 2000 la Organización Internacional para la Estandarización (ISO) creo la primera versión de la ISO 17799 tomando como base la norma BS 7799-1. En el año 2002 se publicó una nueva versión de la BS7799 con la cual las empresas podían certificar su Sistema de Gestión y en el año 2005 aparece la

[20] (ISO-IEC 27000, 2014)

[21] (Ministerio de Hacienda y Administraciones Públicas, 2012)

[22] (NTC-ISO 31000, 2009)

[23] (NTC-ISO 31000, 2009)

[24] (NTC-ISO 31000, 2009)

[25] Sigla para nombrar una Norma Técnica Colombiana

primera versión de la ISO 27001 y la que sería la última versión de la ISO 17799 ya que en 2007 se convertiría en la primera versión de la ISO 27002.

En 2013 el estándar ISO/IEC 27001, y por tanto la traducción oficial para Colombia se actualizaron a la versión vigente y es utilizado como referencia para la certificación reconocida internacionalmente de un Sistema de Gestión de Seguridad de la Información, el cual busca "*preservar la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brindar confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente*." (NTC-ISO-IEC 27001, 2013)

La norma NTC-ISO-IEC 27001:2013 define 7 grupos de requisitos que deben ser cumplidos por una organización para que su SGSI esté en conformidad con la norma, estos grupos son:

- Capítulo 4: Contexto de la organización.
- Capítulo 5: Liderazgo.
- Capítulo 6: Planificación.
- Capítulo 7: Soporte.
- Capítulo 8: Operación.
- Capítulo 9: Evaluación del desempeño.
- Capítulo 10: Mejora.

Estos capítulos corresponden con la estructura de alto nivel del "Anexo SL"; este Anexo define un marco para la construcción de un sistema de gestión genérico y la estructura para las normas de diferentes sistemas de gestión (ej. calidad, medioambiental, servicios, continuidad, etc.), bien sean nuevos o revisiones de normas ya existentes (ISOTOOLS, 2019). Esta estructura común facilita la integración de los diferentes sistemas de gestión dentro de una organización, facilitando las sinergias entre ellos y facilitando su gestión y mejora continua.

3.2 GTC[26]-ISO-IEC 27002:2013

La GTC-ISO-IEC 27002:2013 (actualizada el 22 de julio de 2015) corresponde a la "adopción idéntica por traducción" del estándar internacional ISO/IEC 27002:2013, en el cual se establece el código de práctica para controles de seguridad de la información. Esta guía ha sido diseñada para ser utilizada como preferencia por parte de las empresas para la selección de controles de seguridad durante el proceso de implementación del SGSI (de acuerdo con la NTC-ISO-IEC 27001) o como documento de referencia para las organizaciones que desean implementar buenas prácticas de seguridad de la información (GTC-ISO-IEC 27002, 2013).

La guía está compuesta por 14 numerales de control de seguridad de la información, en los cuales se agrupan 114 controles, y que a su vez pueden estar divididos en categorías en algunos casos en los que así lo amerita la naturaleza del control (GTC-ISO-IEC 27002, 2013). Los numerales de control definidos en la guía son los siguientes:

- Políticas de seguridad de la información.

[26] Sigla para nombrar una Guía Técnica Colombiana

- Organización de la seguridad de la información.
- Seguridad de los recursos humanos.
- Gestión de activos.
- Control de acceso.
- Criptografía.
- Seguridad física y del entorno.
- Seguridad de las operaciones.
- Seguridad de las comunicaciones.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Relaciones con los proveedores.
- Gestión de incidentes de seguridad de la información.
- Aspectos de seguridad de la información de la gestión de continuidad del negocio.
- Cumplimiento.

Los numerales mencionados corresponden con los controles propuestos en el Anexo A de la norma NTC-ISO-IEC 27001:2013, de manera que proporcionan una guía de implementación de cada uno de ellos. Es importante resaltar que en el numeral 6.1.3.c de los requisitos de la norma se pide lo siguiente "*comparar los controles determinados en 6.1.3 b) con los del Anexo A, y verificar que no se han omitidos controles necesarios*" (NTC-ISO-IEC 27001, 2013), por lo cual es fundamental contar con una referencia de implementación de estos controles para la implementación exitosa del SGSI en la empresa.

4 EMPRESA SELECCIONADA

Consultora JC S.A.S. es una empresa con una trayectoria de cerca de 10 años en Colombia, teniendo en la casa matriz en Europa una experiencia superior a los 20 años en el sector de los servicios tecnológicos, especializados en seguridad informática, implementación de infraestructura tecnológica de seguridad, asesoramiento a empresas públicas y privadas y servicios de seguridad administrada de forma remota 24 horas al día los 7 días de la semana.

Desde el año 2010 **Consultora JC S.A.S.** ha mantenido sus operaciones en Suramérica centralizadas en Bogotá, Colombia; aunque atendiendo y desarrollando diversos proyectos en las principales ciudades del territorio nacional y en algunos países vecinos como Panamá, Perú, Ecuador, Uruguay y Paraguay.

4.1 ORGANIGRAMA

En la siguiente imagen se muestra el organigrama actual de **Consultora JC S.A.S.**

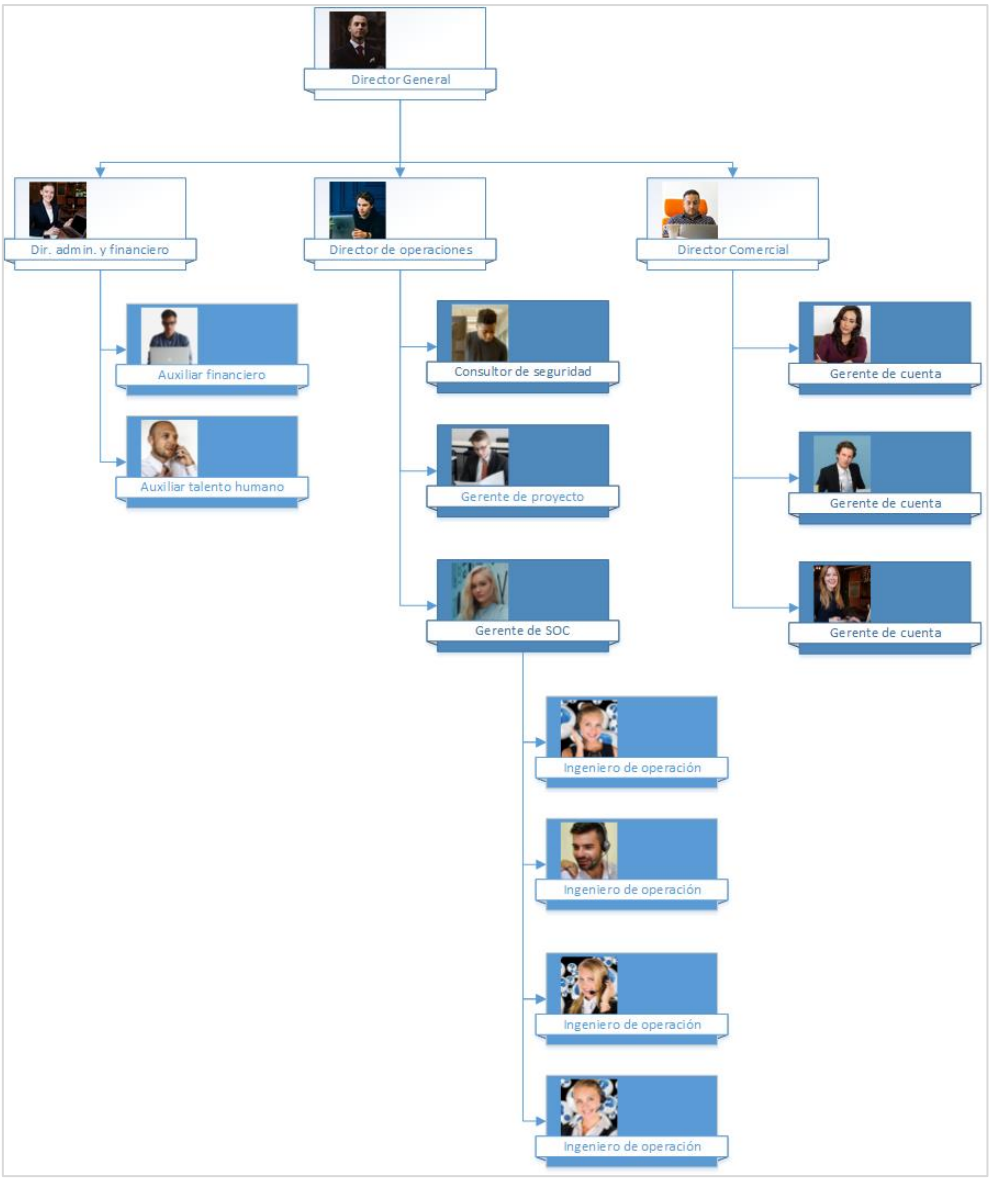


Imagen 4-1 Organigrama de la empresa

4.2 MAPA DE PROCESOS

En el marco de la implementación del Sistema de Gestión de Calidad se ha establecido el mapa de procesos de **Consultora JC S.A.S.** como se describe en la siguiente imagen:

Imagen 4-2 Mapa de procesos de Consultora JC S.A.S.

4.3 CONTEXTO INTERNO DE LA EMPRESA

4.3.1 CAPACIDAD DIRECTIVA

A pesar de ser una sucursal de una compañía europea, **Consultora JC S.A.S.** goza de una autonomía completa con respecto a las decisiones directivas y estratégicas en la región. Los directivos de cada una de las áreas de la compañía tienen una amplia experiencia en su campo de acción y han participado activamente en la definición de la planeación estratégica de la empresa, la cual está proyectada al año 2022 y han liderado la implementación de un Sistema de Gestión de Calidad que, en cabeza del Director General, define los procesos y procedimientos necesarios para la operación de la empresa.

4.3.2 CAPACIDAD COMPETITIVA

Fruto de la planeación estratégica desarrollada en el año 2017 se cuenta con un análisis de la competencia en cada línea de servicio, lo cual ha permitido al equipo comercial establecer una oferta competitiva frente a las demás compañías del sector. La estrategia de diferenciación de **Consultora JC S.A.S.** ha sido enfocada en el precio, puesto que se ha identificado un mercado con un nivel alto de competitividad, la oferta de consultores independientes y un bajo nivel de apalancamiento gubernamental ya que no existen regulaciones para todos los sectores económicos que fomenten la inversión en Seguridad Informática. Esto deja al mercado en una situación desfavorable con respecto a otras líneas de mercado de tecnología que responden a necesidades más inmediatas y terminan relegando a la Seguridad Informática a un segundo plano.

4.3.3 CAPACIDAD FINANCIERA

Financieramente la compañía se mantiene en su punto de equilibrio y en algunos años ha generado ganancias para sus accionistas. Adicionalmente, cuente con el respaldo de la casa matriz con préstamos económicos e inversión cuando se requiere para la estructuración de un proyecto importante en la región. Con respecto a los proveedores **Consultora JC S.A.S.** cuenta con acuerdos económicos que le permiten pagar las facturas a términos de 30 a 60 días en la mayoría de los casos, lo cual le beneficia para el flujo de caja. Así mismo, la relación con los bancos es excelente, lo que habilita a la compañía para acceder a créditos para financiar proyectos y adquisición de infraestructura para su desarrollo.

4.3.4 CAPACIDAD TECNOLÓGICA

El tipo de proyectos que desarrolla la compañía no requieren de una gran cantidad de activos tecnológicos, aunque sí algunos muy especializados y de alto costo. Siempre que sea posible, la empresa se apoya en soluciones de código abierto (Open Source) tanto a nivel de sistemas operativos como de software específico para la ejecución de los servicios. Los acuerdos con los proveedores permiten tener algunas de las implementaciones de software (e incluso hardware) en un modelo de arriendo que facilita la renovación tecnológica y el mantenimiento de los equipos.

4.3.5 CAPACIDAD DEL TALENTO HUMANO

Una de las fortalezas de **Consultora JC S.A.S.** es el nivel técnico y de especialización de su personal operativo, tanto sus consultores, como sus ingenieros de operación y sus gerentes de proyecto están altamente especializados en sus áreas, esto demostrado a través de múltiples certificaciones profesionales que los acreditan a nivel internacional con expertos en sus campos. Las principales especializaciones y certificaciones con las que cuenta el personal operativo se describen a continuación:

- CISSP
- CISM
- PMP
- CEH
- OSCP
- ECIH
- CRISC

Y estudios de especialización como:

- Especialistas en seguridad informática.
- Especialistas en seguridad de la información.
- Especialistas en gerencia de proyectos.
- Especialistas en administración de empresas.

La inversión en la capacitación del personal permite soportar el modelo de prestación de servicios a precios competitivos, pero de alta calidad, siendo este uno de los puntos fuertes de la empresa.

4.4 CONTEXTO EXTERNO DE LA EMPRESA

4.4.1 ÁMBITO ECONÓMICO

De acuerdo con las estimaciones del gobierno nacional, el año 2019 tendrá un nivel de crecimiento general de la economía superior al 3%, lo cual representa un panorama positivo no solo para la compañía, sino para todo el sector de los servicios y la tecnología. El aumento de los presupuestos de las entidades gubernamentales representa un vector de posible mercado para la empresa.

Otro factor económico relevante para la empresa es la tasa de cambio con el dólar estadounidense, especialmente porque muchos de los proveedores de los cuales dependen sus ventas y operaciones facturan en dólares y algunos clientes en países extranjeros también tienen el dólar estadounidense como moneda oficial. Durante el año 2018 se mantuvo una tendencia de incremento del dólar cuyo efecto fue encarecer los insumos que se compran en dólares, con respecto a los servicios que se cobran a los clientes en peses, y sobre los cuales se pueden establecer plazos de pago que generan que la tasa de cambio represente un riesgo para la rentabilidad de los proyectos.

4.4.2 ÁMBITO TECNOLÓGICO

La empresa cuenta con 5 proveedores tecnológicos principales en lo que respecta a la infraestructura propia con la que opera y aquella que hace parte de su proceso de comercialización. Todos estos proveedores son reconocidos internacionalmente, y hacen parte de los fabricantes de mayor prestigio en cada uno los campos de aplicación de sus herramientas. No se cuenta actualmente con acuerdos comerciales con ninguno de los proveedores que permitan acceder a créditos o plazos en los pagos de los equipos adquiridos, por lo cual es necesario que la propia empresa financie su adquisición o que se realice s través de los propios proyectos para los cuales se adquiere.

4.4.3 ÁMBITO SOCIOCULTURAL

Por una parte, la empresa cuenta con una mezcla de personal experimentado en diferentes ámbitos de la operación de tecnología y los servicios, y personal joven que aporta conocimientos en nuevas tecnologías y capacidades de investigación y desarrollo en tecnologías pioneras en la industria. Por la naturaleza de los servicios que presta la empresa, estos están dirigidos a empresas del sector público y privado de tamaño medio y grande. Las pequeñas empresas y las microempresas del país no representan un nicho de mercado importante debido a que no se cuenta con leyes o regulaciones que fomenten la adquisición de productos o servicios relacionados con seguridad informática.

Las relaciones comerciales de la empresa con el sector público han sido históricamente excelentes, desarrollando proyectos en varias organizaciones del gobierno, tanto de índoles local como nacional y ejecutando proyectos de diversos tamaños y alcances.

4.4.4 PRODUCTOS Y/O SERVICIOS

La empresa comercializa productos de desarrollo propio (producto de procesos de investigación y desarrollo internos) y productos de fabricantes reconocidos en el mercado de la seguridad informática, los cuales son respaldados principalmente por las evaluaciones que realiza Gartner para comparar las diferentes características de las soluciones y su proyección. En el mercado colombiano, Gartner es una de las principales fuentes de "benchmarking" para soluciones de seguridad informática y comunicaciones, por lo cual es importante para la empresa mantener una referencia de los resultados de las evaluaciones y estudios realizados por esta firma. En los productos desarrollados internamente, es fundamental que se cuente con prácticas de desarrollo seguro y se integre el proceso de gestión de riesgos de seguridad de la información al ciclo de vida de los proyectos de investigación y desarrollo.

Los servicios que presta la compañía se centran en dos frentes: el primero relacionado con la implementación, configuración y soporte de los equipos tecnológicos que vende, teniendo una gran cantidad de empresas compitiendo en el mismo sector. Esta alta competencia, y el hecho de que varias compañías comercializan las mismas marcas de productos, ha llevado al mercado a tener precios muy competitivos en lo que respecta a los productos, con márgenes de ganancia muy bajos. El comprador tiene múltiples alternativas para adquirir el mismo producto, por lo cual no hay una posibilidad de diferenciarse de la competencia en el producto. Usualmente, donde las compañías pueden tener un margen más alto, y en donde se puede agregar mucho más valor al cliente, es en la prestación de servicios asociados a los productos y es allí donde la empresa ha enfocado sus esfuerzos.

El segundo frente de servicios que presta la compañía está orientado a la consultoría técnica de seguridad informática. Se prestan servicio de análisis de vulnerabilidades, hacking ético, entrenamiento especializado, análisis diferencial, bastionado de plataformas, afinamiento de dispositivos de seguridad, diseño de redes de comunicaciones, revisión de código fuente de las aplicaciones, entre otros.

En el campo de los servicios, si bien existen múltiples empresas a nivel local y nacional con un portafolio similar, la organización ha enfocado sus esfuerzos en prestar servicios a un costo inferior y con estándares altos de calidad y buscando la satisfacción de sus clientes.

En general el panorama para la comercialización de servicios especializados en seguridad informática para los próximos años en la región es bastante optimista de acuerdo con los principales analistas de tendencias en el sector. Desde el gobierno nacional se impulsan iniciativas y estrategias que seguirán teniendo un efecto positivo en el mercado de la seguridad informática.

4.4.5 ÁMBITO LEGAL

Históricamente la cultura de la seguridad informática y la protección de la información no han sido muy fuertes en las empresas del país, e incluso de la región. El sector financiero, es el que más ha tenido que enfrentar riesgos relacionados con la protección de la información de sus clientes. Evidentemente, por la naturaleza de sus operaciones ha sido el sector más afectado y así mismo el que más ha trabajado en contar con regulaciones para apoyar los temas relacionados con la protección de la información. Se cuenta en Colombia con múltiples regulaciones específicas del sector financiero como:

- Circular 052 de 2007 – Lineamientos de seguridad y calidad en los servicios
- Circular 042 de 2012 – Actualización de la circular 052
- Circular 029 de 2014 – Circular Básica Jurídica
- Circular 007 de 2018 – Circular de ciberseguridad

Sin embargo, desde el año 2010 el gobierno colombiano ha reconocido a la ciberseguridad como uno de los principales pilares del desarrollo del país, puesto que ha identificado múltiples amenazas al respecto y ha identificado los diferentes sectores del país que cuenta con infraestructuras críticas para el desarrollo y normal funcionamiento de las instituciones y ha establecido amplias estrategias para fomentar la inversión y el desarrollo de proyectos en este sentido. Puntualmente se han establecido las siguientes leyes y regulaciones al respecto:

- Ley 1266 de 2008 – Habeas data.
- Ley 1581 de 2012 – Protección de datos personales
- Ley 1273 de 2015 – Delitos informáticos

Estas regulaciones motivan al mercado a implementar estrategias de seguridad e invertir en soluciones tecnológicas y no tecnológicas para abordar la protección de sus activos de información críticos. En el sector público existen obligaciones de implementar medidas de protección, de acuerdo con un plan de implementación liderado por el Ministerio de las Tecnologías de la Información, mientras tanto en el sector privado existen regulaciones para el sector financiero y diferentes iniciativas en otros sectores para la inversión en tecnología de seguridad informática.

4.5 ANÁLISIS DOFA

	Fortalezas	Debilidades
Interno	Equipo de trabajo altamente capacitado. Consciencia de la necesidad de la implementación de un SGSI. Apoyo de la alta dirección a la implementación del SGSI. Soporte de la casa matriz.	Falta de documentación de procesos de operación. Falta de una estrategia de continuidad de negocio. No cuenta con una estrategia Corporativa para la gestión de la seguridad de la Información.

		No existe un análisis del impacto financiero de la prevención y materialización de los riesgos de seguridad.
	Oportunidades	**Amenazas**
Externo	Servicios de consultoría en seguridad de la información en sistemas de control de infraestructura crítica (SCADA). Servicios de consultoría en seguridad de la información en el sector eléctrico. Regulaciones gubernamentales que apoyan la inversión en seguridad informática.	Alta capacidad y flexibilidad en el mercado de la competencia. Mayor experiencia y tiempo en el mercado de la competencia. Adquisición de productos en dólares. Altos impuestos para la importación de equipos.

4.6 ALCANCE DEL SGSI

En conjunto con la Dirección General y el comité directivo de **Consultora JC S.A.S.** se estableció el alcance del SGSI los procesos de "operaciones de seguridad informática", en el cual se prestan los servicios de SOC (Centro de operaciones de Seguridad) y "gestión de proyectos", esto debido a que son los procesos principales del negocio, la planeación estratégica está enfocada en su crecimiento y la importancia que tiene el SGSI a nivel comercial para este servicio.

4.7 PARTES INTERESADAS

En conjunto con la Dirección General y el comité directivo de **Consultora JC S.A.S.** se establecieron las siguientes partes interesadas y sus expectativas:

- Accionistas y directivos de la casa matriz.
    - Que el SGSI esté alineado con los objetivos estratégicos.
    - Que el SGSI apoye el cumplimiento de las normas vigentes en relación con protección de información y datos personales.
    - Que de administren los riesgos de seguridad de la información que puedan impactar negativamente la reputación de la empresa.
- Otras sucursales a nivel mundial.
    - Que la información compartida entre las sucursales sea protegida tanto en reposo como en tránsito.
    - Que se les informe sobre la implementación de controles y acciones de mejora del SGSI.
    - Que las prácticas de seguridad establecidas sean homogéneas.
- Entes de control y gobierno nacional.
    - Que se cumplan las leyes y normas nacionales relacionadas con protección de información y datos personales.
- Proveedores.

    - Que se apliquen las medidas de seguridad definidas para la protección de la información compartida.
- Empleados del proceso “operaciones de seguridad informática”.
    - Que se protejan sus datos personales de acuerdo con las leyes y acuerdos vigentes.
    - Que se les capacite sobre las buenas prácticas y controles de seguridad de la información.
- Clientes.
    - Que se cumplan las medidas de seguridad definidas para la información proporcionada.
    - Que se cumplan las normas nacionales vigentes relacionadas con protección de información y datos personales.
    - Que se cumplan las medidas de seguridad de la información que se hayan establecido contractualmente en el marco del proyecto en ejecución.

4.8 INFRAESTRUCTURA TECNOLÓGICA

La infraestructura tecnológica que apoya la ejecución de los procesos de “operaciones de seguridad informática” y “gestión de proyectos” se describe a continuación:

- Sistema iTop en el cual se documenta la gestión de requerimientos e incidentes por parte del cliente. Está instalado en un servidor virtual que se encuentra soportado por un equipo físico y un hypervisor VMware. Su sistema operativo es Linux.
- Sistema OSSIM para la correlación de eventos de seguridad. Está instalado en un servidor virtual que se encuentra en el mismo VMware del sistema iTop. Su sistema operativo es Linux.
- Sistema Nagios para la monitorización de disponibilidad de la infraestructura tecnológica. Está instalado en un servidor virtual que se encuentra en el mismo VMware del sistema iTop. Su sistema operativo es Linux.
- Servidor Linux para el almacenamiento y protección de la información de los clientes. Está instalado en un servidor virtual que se encuentra en el mismo VMware.
- Video Wall de monitorización compuesto por 8 pantallas de 50 pulgadas de alta resolución y uso industrial.
- 8 equipos de cómputo de usuario final (portátil y PC) para el trabajo cotidiano de todo el equipo perteneciente a los procesos establecidos.

La operación de los procesos, especialmente el de “operaciones de seguridad informática” tiene una alta dependencia de la infraestructura de red, por lo cual lo siguientes elementos son de vital importancia para la continuidad de la operación:

- 2 dispositivos Firewall UTM que administran la seguridad entre los segmentos de la red, la cual está dividida en:
    - Corporativa (LAN).

- Corporativa red inalámbrica.
- SOC.
- DMZ.
- Zona protegida de servidores.
- Visitantes red inalámbrica.

Estos equipos se encuentran en alta disponibilidad y soportan la protección de la DMZ (mediante reglas de IPS y WAF) y de los usuarios a través del control de navegación y control de acceso a las redes. Adicionalmente, están configuradas las redes VPN con los diferentes clientes a los que se les presta servicio.

- 4 dispositivos Switch para la gestión de las comunicaciones dentro de las instalaciones de la oficina principal.
- 3 UPS para el respaldo de la alimentación eléctrica.
- 2 canales de Internet para la conectividad vía VPN con los clientes y el acceso a Internet de la oficina.
- 1 planta telefónica para la atención de clientes.
- 1 teléfono móvil para la atención de clientes.

En la siguiente imagen se presenta un esquema general de red con la ubicación lógica de los dispositivos de comunicaciones y servidores de la compañía.

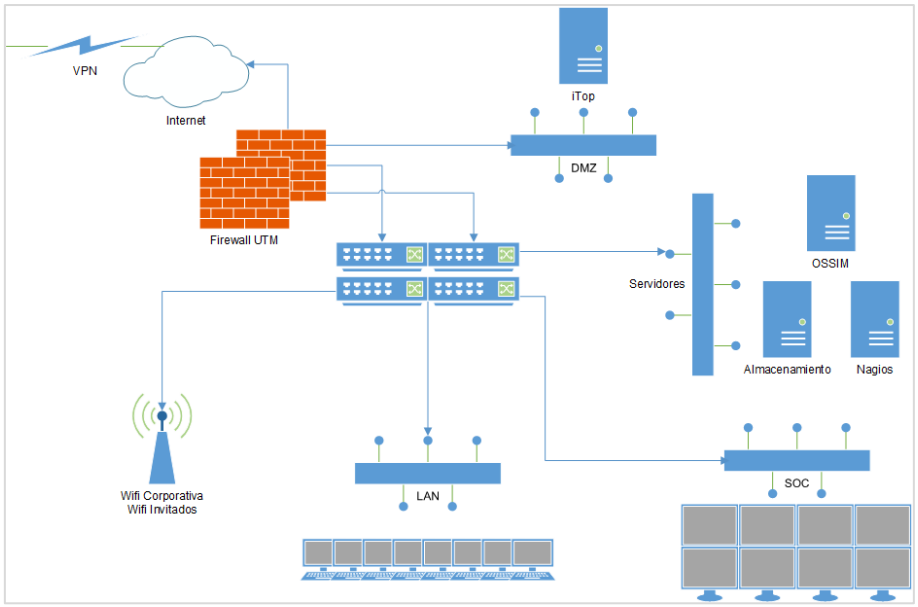


Imagen 4-3 Topología de red

5 PLAN DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN

5.1 ALCANCE

El alcance del plan director comprende los procesos de negocio de la empresa como se enuncian a continuación:

- Gestión de proyectos.
- Gestión de operaciones de seguridad informática.

Estos procesos en el marco de la ejecución de los servicios en las oficinas ubicadas en la ciudad de Bogotá, Colombia.

5.2 OBJETIVOS

Generar confianza en los clientes, accionistas, proveedores y empleados con respecto al manejo de su información.

Identificar los riesgos de seguridad de la información en los activos que hacen parte de los procesos dentro del alcance del SGSI y mantenerlos en el nivel aceptable para la empresa.

Preservar la Confidencialidad, Integridad y Disponibilidad de la información en los procesos dentro del alcance del SGSI.

Cumplir con los requisitos legales y contractuales en lo que respecta a la seguridad de la información.

Certificar el SGSI en conformidad con la norma NTC-ISO-IEC 27001:2013 con alcance de los procesos de “Operaciones de seguridad informática” y “Gestión de proyectos”.

6 ANÁLISIS DIFERENCIAL (NTC-ISO-IEC 27001:2013)

6.1 METODOLOGÍA

Se realizó el análisis diferencial con respecto a los requisitos de la norma NTC-ISO/IEC 27001: 2013 y con respecto a los controles incluidos en el Anexo A de la misma norma y desarrollados en la guía GTC-ISO/IEC 27002:2013. Para la evaluación se utilizaron dos escalas diferentes; los requisitos se evaluaron con la siguiente escala:

- **No implementado:** El requisito no ha sido implementado aún.
- **En proceso de implementación:** Se cuenta con algún tipo de evidencia que demuestra que el requisito se está implementando en el momento del análisis, pero aún no es satisfactoria su implementación.
- **Implementado:** El requisito se satisface completamente al momento de realizar el análisis.

Para la valoración de los 114 controles del Anexo A se utilizó la siguiente escala tomada del Framework CobIT v5:

- **0 - Proceso incompleto:** El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.

- **1 - Proceso ejecutado:** El proceso implementado alcanza su propósito.
- **2 - Proceso gestionado:** El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.
- **3 - Proceso establecido:** El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso.
- **4 - Proceso predecible:** El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.
- **5 - Proceso optimizado**: El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con las metas empresariales presentes y futuros.

6.2 RESULTADOS

En general, los resultados obtenidos para el estado de cumplimiento de los requisitos de la norma se resumen en la siguiente gráfica:

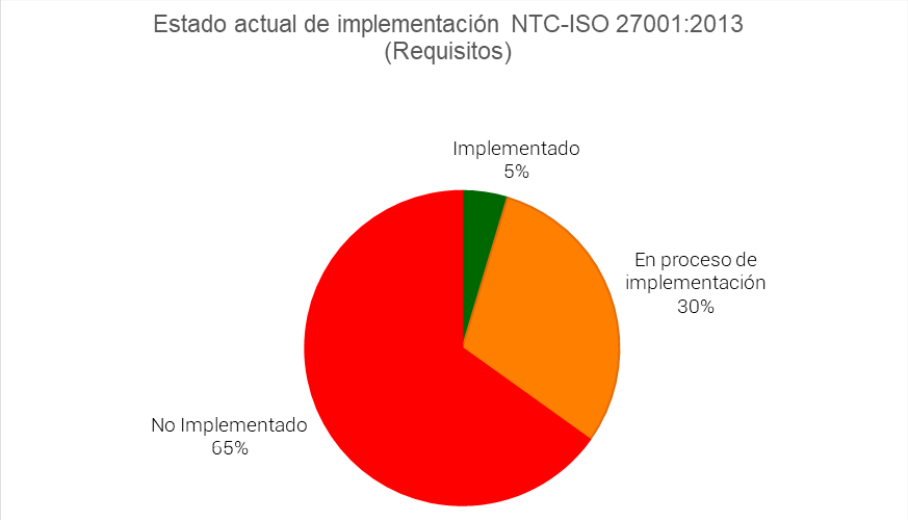


Imagen 6-1 Estado de avance en la implementación de los requisitos

Como se puede observar, el 65% de los requisitos no se encuentran implementados, por lo cual el plan director será una hoja de ruta fundamental para lograr la implementación del Sistema de Gestión de Seguridad de la Información. Sin embargo, es importante destacar que el 30% de los requisitos se encuentran en proceso de implementación, por lo cual es posible que se logren avances significativos durante las primeras etapas del proyecto.

En lo que respecta al estado de madurez de los 114 controles del Anexo A de la norma NTC-ISO-IEC 27001:2013, en la siguiente gráfica se puede observar la cantidad de controles por nivel con respecto a la escala de CobIT v5:

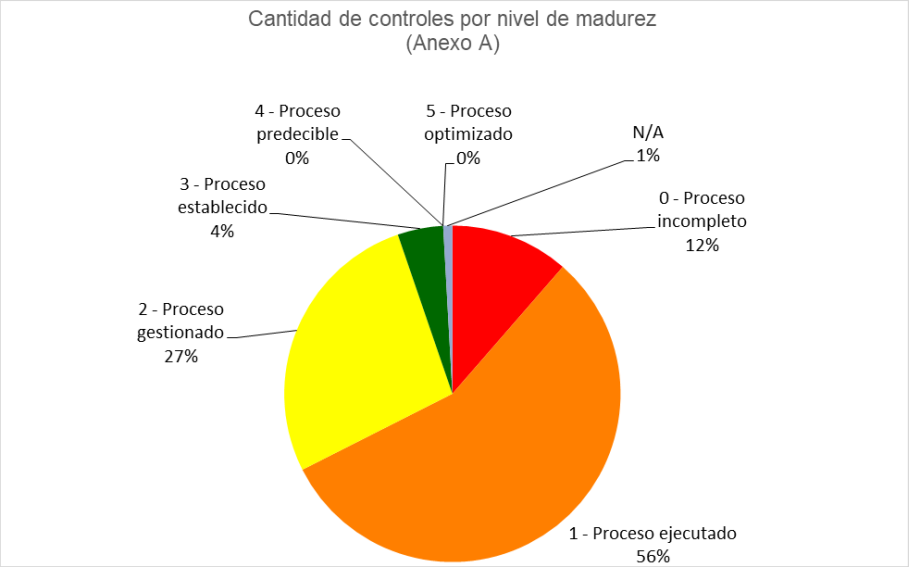


Imagen 6-2 Estado de implementación de los controles del Anexo A

Si bien el estado de madurez de los controles presenta un panorama general de la empresa y la gestión que se ha realizado orientada a la protección de los activos de información, será el resultado del análisis de riesgo el que oriente las prioridades que se deberán establecer para la implementación o mejora de los controles de seguridad. El análisis diferencial con respecto a los controles del Anexo A puede actualizarse periódicamente como instrumento de seguimiento para cuantificar el avance en la implementación de los controles de seguridad de la información. De igual forma, el formato de análisis diferencial puede ser utilizado para establecer y dar seguimiento a metas específicas de evolución en la madurez de los diferentes controles como se puede observar en la siguiente imagen.

Imagen 6-3 Nivel de madurez proyectado para un periodo de 1 año

Del resultado anterior es importante destacar los resultados obtenidos en el área de la seguridad en los recursos humanos puesto que fue el que mostró un mejor avance con respecto al estado actual de madurez de los controles de seguridad.

7 SISTEMA DE GESTIÓN DOCUMENTAL

7.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se presenta la declaración de política de seguridad de la información de acuerdo con lo establecido en la norma NTC-ISO-IEC 27001:2013, la cual será divulgada y mantenida al alcance de los interesados a través de los medios de comunicación dispuestos por la empresa:

***Consultora JC S.A.S.**, pone de manifiesto su compromiso con la protección de la seguridad de la información, los objetivos de seguridad establecidos y el cumplimiento de la legislación vigente en lo que respecta a la protección de la información y los datos personales. Así mismo, consciente de la importancia de la seguridad de la información de sus empleados, procesos de negocio, clientes, accionistas y proveedores, ha establecido un Sistema de Gestión de Seguridad de la Información basado en la norma NTC-ISO-IEC 27001:2013 cuyo alcance abarca las operaciones en la ciudad de Bogotá, Colombia y específicamente las actividades descritas en los procesos:*

- ***Gestión de operaciones de seguridad informática.***
- ***Gestión de proyectos.***

Con el fin de desarrollar el compromiso citado, la Dirección establece los siguientes objetivos de seguridad de la información:

- *Preservar la Confidencialidad, Integridad y Disponibilidad de la información en los procesos dentro del alcance del SGSI.*
- *Identificar y gestionar el riesgo de seguridad de la información en los activos que hacen parte del alcance del SGSI, y mantenerlos en el nivel aceptable para la empresa.*
- *Gestionar los incidentes de seguridad identificados, procurando la mejora del sistema para reducir la probabilidad de repetirse.*
- *Capacitar al personal que hace parte de los procesos en el alcance del SGSI con respecto a las mejores prácticas de seguridad y su responsabilidad dentro del Sistema.*
- *Establecer y revisar periódicamente indicadores que permitan definir las acciones necesarias para mejorar la operación del SGSI.*

En línea con estos objetivos, la Dirección General se compromete a proveer los recursos necesarios para alcanzarlos y a liderar la operación del Sistema de Gestión propendiendo por el compromiso de toda la organización con la obtención de los resultados esperados.

7.2 PROCEDIMIENTO DE AUDITORÍAS INTERNAS

7.2.1 OBJETIVO

Establecer un procedimiento a través del cual se planifiquen y ejecuten periódicamente las auditorías internas al Sistemas de Gestión de Seguridad de la Información, con el fin de evaluar la conformidad con los requisitos de la norma NTC-ISO-IEC 27001:2013, los requisitos legales, de la organización y sus partes interesadas.

7.2.2 ALCANCE

Este procedimiento aplica para los procesos dentro del alcance del Sistema de Gestión de Seguridad de la Información y se aplicará de acuerdo con el programa de auditorías definido.

7.2.3 RESPONSABLE

El responsable de la ejecución de este procedimiento será quién sea designado como auditor interno del SGSI y que a su vez deberá cumplir con los siguientes requisitos mínimos:

- Contar con una experiencia comprobada mínima de 1 año en la ejecución de actividades de auditoría o haber liderado la implementación y atención de mínimo una auditoría de certificación en la norma NTC-ISO-IEC 27001:2013.
- Certificación como auditor interno o auditor líder en la norma NTC-ISO-IEC 27001:2013.
- Independencia de los procesos auditados, de forma que se pueda asegurar la imparcialidad con respecto al proceso.
- Tener conocimientos básicos que le permitan entender la actividad principal de los proyectos, o en caso de no tenerlos, contar con la asesoría técnica durante el proceso de auditoría.

El plan de auditorías internas debe ser publicado al interior de la empresa con 3 días de anticipación y debe incluir:

- Proceso por auditar.
- Nombre del auditor líder y del equipo auditor (si aplica).
- Listado de controles que serán incluidos en la auditoría (*).
- Criterios de la auditoría.
- Fecha, hora y lugar de la auditoría.
- Auditado(s) responsable(s).

*Los controles de seguridad que se incluyen en la auditoría deben seleccionarse teniendo en cuenta la declaración de aplicabilidad vigente, y ser equivalente a un tercio del total de los controles, cuidándose de repetir aquellos que fueron auditados el año anterior, salvo alguna excepción por considerarse prioritario revisarlo nuevamente.

7.2.4 DESCRIPCIÓN DE ACTIVIDADES

N.º	¿QUÉ?	¿QUIÉN?	¿CÓMO?	¿CUÁNDO?
1	Planificar y programar las auditorías internas	Oficial de seguridad/Auditor Interno	Definir el auditor interno y planificar en conjuntos las actividades del programa de auditorías de acuerdo con los requerimientos establecidos. El programa debe ser aprobado por la dirección general.	Una vez al año
2	Publicar y comunicar la programación de las auditorías internas	Oficial de seguridad	El programa de auditorías internas se pone en conocimiento de las personas implicadas, bien sea como auditores o como miembros del proceso auditado.	Una vez aprobado por la dirección general
	Seleccionar la muestra de controles a auditar	Auditor interno/Equipo auditor	Teniendo en cuenta los resultados y el plan de la auditoría del año anterior, se selecciona el grupo de controles que serán auditados, los cuales se incluyen en el plan de auditoría.	Dos semanas antes del inicio de la auditoría
3	Preparar y enviar el plan de auditoría	Auditor interno/Equipo auditor	Preparar el plan de auditoría para coordinar los horarios de las actividades de acuerdo con el formato establecido. El plan de auditoría debe incluir los aspectos descritos y deberá ser enviado a los auditados y, si es necesario y está justificado, ajustar el plan.	Dos semanas antes del inicio de la auditoría
4	Realizar la reunión de apertura	Auditor interno/Equipo auditor/Dirección General/Oficial de Seguridad	Se realiza la reunión de apertura de la auditoría en la cual se presenta el plan y se socializa el cronograma de entrevistas con los involucrados.	En la fecha programada de inicio
5	Revisar la documentación	Auditor interno/Equipo auditor	El equipo auditor debe revisar los documentos del SGSI y los registros solicitados para verificar el desempeño del sistema, de acuerdo con el alcance de la auditoría.	Después de la actividad anterior
6	Realizar las entrevistas y visitas de verificación	Auditor interno/Equipo auditor/Entrevistados	El equipo auditor se entrevista con los responsables de los procesos en el alcance de la auditoría y los responsables de los controles de seguridad y	De acuerdo con el cronograma de entrevistas

N.º	¿QUÉ?	¿QUIÉN?	¿CÓMO?	¿CUÁNDO?
			demás actividades seleccionadas.	
7	Documentar los hallazgos	Auditor interno/Equipo auditor	Se genera un informe con los hallazgos de la revisión de los documentos y las entrevistas realizadas, destacando aquellos hallazgos que puedan ser catalogados como no conformidades.	Al culminar las entrevistas y visitas de verificación
8	Realizar la reunión de cierre	Auditor interno/Equipo auditor/Dirección General/Oficial de Seguridad	En la reunión de cierre se presenta el informe con los resultados de la auditoría y se revisan aquellos puntos en los que se puede presentar alguna situación de discordia.	De acuerdo con la programación de la auditoría
9	Desarrollar el plan de acción y mejora	Dirección General/Oficial de Seguridad	Con los resultados obtenidos en la auditoría, es fundamental establecer el plan de acción que permita atender aquellas falencias y no conformidades que fueron identificadas.	Al finalizar el ejercicio de auditoría, máximo 2 semanas después de la reunión de cierre

Tabla 7-1 Procedimiento de auditorías internas

7.3 GESTIÓN DE INDICADORES

Con el fin de evaluar el desempeño de la seguridad de la información y la eficacia del SGSI, se han planteado los siguientes indicadores:

7.3.1 NIVEL DE CONCIENTIZACIÓN

Medición base	Número de personas que aprobaron la prueba (PA)	Número de personas que presentaron prueba (PP)
Objetivo	Verificar el grado de apropiación del conocimiento de las políticas de seguridad	
Controles/Procesos relacionados	7.3 Toma de conciencia. A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	
Unidad de medida	# de Personas	
Objeto de medición	Examen	Lista de asistencia al examen

Método	Contar la cantidad de personas con resultados superiores al 70% en la prueba	Contar la cantidad de personas que presentaron la prueba
Frecuencia	Bimestral	Bimestral
Función de medición	$x = \frac{PA}{PP} x100$	
Valor objetivo	85%	
Valor umbral	70%	
Modelo analítico	$x < 70\%$	**Inaceptable**
	$x \geq 70\%$	**Aceptable**
Criterio de decisión	**Inaceptable -** Analizar las posibles causas del resultado y tomar acciones correctivas. **Aceptable -** Tomar medidas de refuerzo del conocimiento de forma individual con quienes no aprobaron la prueba para lograr el valor objetivo.	

7.3.2 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Medición base	# de incidentes detectados (ID)	# de incidentes reportados (IR)	# de incidentes gestionados (IG)
Objetivo	Medir el número de incidentes de seguridad información detectados y reportados que fueron gestionados		
Controles/Procesos relacionados	A.16 Gestión de incidentes de seguridad de la información		
Unidad de medida	# de incidentes de seguridad de la información		
Objeto de medición	Tickets de incidentes de seguridad de la información abiertos por el Oficial de Seguridad	Tickets de incidentes de seguridad de la información abiertos por otros empleados	Tickets de incidentes de seguridad de la información solucionados
Método	Contar la cantidad de incidentes de seguridad identificados por el Oficial de Seguridad	Contar la cantidad de Tickets recibidos notificando incidentes de seguridad	Contar la cantidad de tickets de incidentes de seguridad solucionados
Frecuencia	Mensual	Mensual	Mensual
Función de medición	$x = \left(1 - \frac{IG}{ID + IR}\right) x100$		

Valor objetivo	0%	
Valor umbral	10%	
Modelo analítico	$x \geq 10\%$	**Inaceptable**
	$x < 10\%$	**Aceptable**
Criterio de decisión	**Inaceptable –** Identificar las causas de la falta de resolución de los incidentes y revisar el procedimiento de gestión de incidentes de seguridad de la información y realizar los ajustes necesarios. **Aceptable –** Mantener el seguimiento de los incidentes de seguridad de la información.	

7.3.3 GRADO DE IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD

Medición base	# de controles de seguridad implementados (CI)	# de controles de seguridad planeados a implementar (CP)
Objetivo	Medir el grado de cumplimiento de los planes de tratamiento de riesgo y demás proyectos de implementación de controles de seguridad de la información	
Controles/Procesos relacionados	6.1.3 Tratamiento de riesgos de la seguridad de la información	
Unidad de medida	# de controles	
Objeto de medición	Avance en la implementación de controles de seguridad de la información	Planeación de la implementación de controles de seguridad de la información
Método	Contar el número de controles de seguridad implementados de acuerdo con el plan	Contar el número de controles de seguridad planeados para ser implementados
Frecuencia	Trimestral	Trimestral
Función de medición	$x = \frac{CI}{CP} x100$	
Valor objetivo	90%	
Valor umbral	70%	
Modelo analítico	$x < 70\%$	**Inaceptable**
	$x \geq 70\%$	**Aceptable**

Criterio de decisión	**Inaceptable –** Revisar el plan de tratamiento de riesgos y el cronograma de ejecución con el fin de establecer las posibles causas de los retrasos, para implementar los ajustes necesarios en cuanto a tiempos y recursos. **Aceptable –** Continuar con el proceso de implementación según lo establecido en el cronograma de ejecución y verificar la posibilidad generar un plan de choque para aquellos controles con más dificultades.

7.3.4 NIVEL DE MEJORA CONTINUA DEL SGSI

Medición base	# de no conformidades identificadas en un periodo (NC)	# no conformidades de causas recurrentes en un periodo (NCR)
Objetivo	Identificar el grado de efectividad de las acciones de mejora tomadas en el SGSI midiendo la recurrencia de no conformidades asociadas a las mismas causas dentro de las auditorías realizadas	
Controles/Procesos relacionados	10.1 No conformidades y acciones correctivas 10.2 Mejora continua	
Unidad de medida	# de no conformidades	
Objeto de medición	Resultados de auditorías internas	Histórico de resultados de auditorías internas
Método	Contar la cantidad de no conformidades halladas en la auditoría interna	Contar la cantidad de no conformidades halladas en la auditoría interna cuyas causas son recurrentes con respecto a auditorías anteriores
Frecuencia	Semestral	Semestral
Función de medición	$x = \frac{NCR}{NC} x100$	
Valor objetivo	90%	
Valor umbral	80%	
Modelo analítico	$x < 80\%$	**Inaceptable**
	$x \geq 80\%$	**Aceptable**
Criterio de decisión	**Inaceptable –**Indagar e identificar las causas por las cuales no se controlaron las causas relacionadas con las no conformidades y proponer medidas de control que ataquen las causas de las no conformidades de causas recurrentes. **Aceptable –** Hacer seguimiento a las no conformidades recurrentes y no tratadas para darles debida gestión. Identificar si o han sido solucionadas o se vuelves a presentar por falta de atención a las causas.	

7.4 PROCEDIMIENTO REVISIÓN POR DIRECCIÓN

7.4.1 OBJETIVO

Establecer un procedimiento que permita a la Alta Dirección de ***Consultora JC S.A.S.*** revisar el desempeño y los resultados del SGSI y asegurar su conveniencia, adecuación, mejoramiento continuo, e identificación de la necesidad de efectuar cambios para el cumplimiento de las políticas y objetivos de la compañía.

7.4.2 ALCANCE

El procedimiento aplica para toda la información documentada y resultados de los procedimientos del SGSI.

7.4.3 RESPONSABLE

El responsable del procedimiento es el Oficial de Seguridad de la Información con la participación del Director General.

7.4.4 DESCRIPCIÓN DE ACTIVIDADES

N.º	¿QUÉ?	¿QUIÉN?	¿CÓMO?	¿CUÁNDO?
1	Iniciar la reunión	Oficial de seguridad de la información	Iniciar la reunión de revisión por la dirección con la verificación de los compromisos de la reunión anterior.	De acuerdo con la programación de las revisiones
2	Definir el plan de acción para los compromisos no cerrados	Oficial de seguridad de la información/Director General	En caso de que se algún compromiso previo no sea cumplido, es necesario identificar la causa y establecer un plan de acción para cumplirlo.	Después de la actividad anterior
3	Presentar los cambios en las partes externas e internas	Oficial de seguridad de la información	Si durante el periodo se presentaron cambios en el contexto interno o externo relevantes para el SGSI se deben socializar con la Dirección General.	Después de la actividad anterior
4	Definir los ajustes y el plan de acción necesarios	Oficial de seguridad de la información/Director General	En caso de que los cambios en las partes externas afecten de forma significativa el SGSI, es necesario identificar, priorizar y planear la	Después de la actividad anterior

N.º	¿QUÉ?	¿QUIÉN?	¿CÓMO?	¿CUÁNDO?
			ejecución de los cambios necesario.	
5	Revisar los resultados de no conformidades y acciones correctivas	Oficial de seguridad de la información/Director General	Si existen, se presentan y revisan las no conformidades presentadas, así como el resultado de las acciones correctivas tomadas en el periodo.	Cuando se hayan registrado no conformidades y/o acciones correctivas
6	Revisar los resultados de los indicadores	Oficial de seguridad de la información/Director General	Se presentan y revisan los resultados de la medición de los indicadores de acuerdo con los periodos definidos.	Durante la reunión, después de la actividad anterior
7	Revisar los resultados de la auditoría interna	Oficial de seguridad de la información/Director General	Se revisan los resultados de la auditoría interna como insumo para la toma de decisiones de mejora del SGSI.	Durante la reunión, después de la actividad anterior
8	Discutir el avance en el cumplimiento de los objetivos de seguridad	Oficial de seguridad de la información/Director General	Con analiza cada uno de los objetivos de seguridad y los diferentes proyectos que apoyan su cumplimiento con el fin de identificar si siguen siendo pertinentes o requieren algún ajuste.	Durante la reunión, después de la actividad anterior
9	Revisar la retroalimentación de las partes interesadas	Oficial de seguridad de la información/Director General	Se revisan las observaciones o requisitos nuevos de las diferentes partes interesadas para identificar la necesidad de ajustar algún aspecto del SGSI.	Durante la reunión, después de la actividad anterior
10	Revisar los resultados de la valoración de riesgos y el avance del plan de tratamiento de riesgos	Oficial de seguridad de la información/Director General	Se presentan los resultados del último análisis de riesgos y del avance de los planes de tratamiento establecidos con el fin de identificar la necesidad de recursos o ajustes.	Durante la reunión, después de la actividad anterior
11	Discutir las oportunidades de mejora del SGSI	Oficial de seguridad de la información/Director General	Se consolidan todos los puntos anteriores en los cuales se identificó alguna oportunidad de mejora.	Durante la reunión, después de la actividad anterior

N.º	¿QUÉ?	¿QUIÉN?	¿CÓMO?	¿CUÁNDO?
12	Definir y planear las acciones de mejora identificadas	Oficial de seguridad de la información/Director General	Con las oportunidades de mejora establecidas, se genera un plan de acción o se incorporan elementos a los planes de tratamiento que permitan su implementación.	Durante la reunión, después de la actividad anterior
13	Documentar los resultados de la revisión en el Acta de Revisión por la Dirección	Oficial de seguridad de la información	En el acta se consignan todos los aspectos tratados, las conclusiones y las decisiones tomadas para facilitar el seguimiento en la siguiente reunión.	Durante la reunión, después de la actividad anterior

Tabla 7-2 Procedimiento de revisión por la dirección

7.5 GESTIÓN DE ROLES Y RESPONSABILIDADES

7.5.1 DIRECTOR GENERAL

El Director General debe:

- Garantizar la provisión de los recursos para el funcionamiento del SGSI.
- Liderar la toma de decisiones estratégicas relacionadas con la gestión de seguridad de la información
- Revisar y aprobar la Política de Seguridad de la información de la empresa.
- Designar a la persona que ocupe la función de Oficial de Seguridad de la Información.
- Establecer, en conjunto con el Oficial de Seguridad, los controles y auditorias necesarias para hacer seguimiento del desempeño del SGSI.
- Evaluar, por lo menos una vez al año, la gestión de la Seguridad de la Información e implementar las acciones necesarias para el cumplimiento de los objetivos del SGSI.
- Participar en el comité de Seguridad de la Información que se estableció para realizar el seguimiento periódico del SGSI en conjunto con los líderes de las áreas involucradas.

7.5.2 OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

El Oficial de Seguridad de la Información debe:

- Asegurar que el contenido y definiciones del SGSI se encuentran en concordancia con las disposiciones vigentes en lo que respecta a la protección de la información y los datos personales.
- Liderar las actividades de difusión y sensibilización de las políticas y procedimientos de Seguridad de la Información.

- Controlar la documentación que hace parte del SGSI de acuerdo con las directrices del Sistema de Gestión de Calidad de la empresa.
- Mantener los registros relacionados con la gestión de incidentes de seguridad de la información, los resultados de los análisis de riesgo, las actividades de capacitación y sensibilización, los resultados de la revisión por la dirección y las acciones correctivas y de mejora.
- Realizar el seguimiento de los indicadores del SGSI para reportar a la Dirección General.
- Coordinar la investigación de las causas de las No Conformidades identificadas y la ejecución de acciones correctivas o de mejora pertinentes.
- Participar en la revisión del SGSI con la Dirección y elaborar el informe de resultados.
- Liderar la ejecución de las actividades de análisis de riesgo en los procesos dentro del alcance del SGSI.
- Establecer en conjunto con los responsables de los procesos, los controles de seguridad para construir los planes de tratamiento de riesgo.
- Velar por el cumplimiento de las políticas de seguridad de la información en la organización.
- Mantener el Plan de Seguridad actualizado de acuerdo con los cambios que se presenten en las necesidades de la organización y los procesos.

7.5.3 DIRECTOR DE OPERACIONES DE SEGURIDAD INFORMÁTICA

El Director de Operaciones de Seguridad Informática debe:

- Apoyar a la Dirección General en el establecimiento de la política de seguridad de la información.
- Participar en el comité de seguridad de la información como representante de los procesos incluidos en el alcance del SGSI.
- Identificar y clasificar los activos de información que apoyan la operación de su proceso de forma completa y detallada.
- Ejecutar el análisis de riesgo a los activos de información de su proceso y plantear, en conjunto con el Oficial de Seguridad de la Información, los planes de tratamiento de riesgo.
- Velar por el cumplimiento de las políticas de seguridad de la información en las actividades propias del proceso que lidera.
- Facilitar las actividades de sensibilización y capacitación dispuestas por parte del Oficial de Seguridad de la Información cuando incluyan al personal que hace parte de su proceso.

7.5.4 ENCARGADO DE LA GESTIÓN DE TECNOLOGÍA INTERNA

El encargado de la gestión de tecnología interna debe:

- Administrar y dar mantenimiento a todo el entorno operativo (Servidores, Sistemas Operativos, Redes y Comunicaciones, Bases de Datos, etc.), teniendo en cuenta los procedimientos y controles de seguridad establecidos para cada actividad.
- Establecer los mecanismos que permitan garantizar el acceso a los sistemas de información únicamente a las personas autorizadas.
- Disponer de un lugar seguro para la custodia de las copias de respaldo realizadas.
- Proveer los mecanismos para la realización de las copias de respaldo y velar por su ejecución de acuerdo con la programación establecida.
- Establecer los mecanismos de registro de incidentes de seguridad y su posterior atención y seguimiento por parte del Oficial de Seguridad de la información.
- Manejar de manera responsable y de acuerdo con las políticas de seguridad la información a la cual tiene acceso por sus privilegios de administración de los sistemas o servidores.
- Trabajar en conjunto con el Oficial de Seguridad de la Información para la implementación de controles de técnicos de seguridad.
- Custodiar los usuarios y contraseñas con privilegio de administrador de los sistemas internos que administre.
- Notificar al Oficial de Seguridad de la Información cuando en la infraestructura tecnológica identifique posibles incidentes de seguridad.

7.5.5 EMPLEADOS INVOLUCRADOS EN LOS PROCESOS

Los empleados involucrados en los procesos dentro del alcance del SGSI deben:

- Mantener la seguridad de sus puestos de trabajo de acuerdo con las políticas de seguridad de la información.
- Velar especialmente por la protección de las áreas seguras (ej. el Centro de Operaciones de Seguridad), protegiéndolas del acceso físico no autorizado y reportado al Oficial de Seguridad en caso de identificar alguna situación sospechosa.
- Aplicar las políticas de seguridad de la información y velar porque los demás empleados, proveedores y clientes actúen en concordancia con las mismas.
- Asegurar la fortaleza y confidencialidad de sus contraseñas de acceso a los sistemas de información y, en el caso de que se produzca cualquier situación que genere sospecha de que se ha perdido su confidencialidad, reportar el incidente de seguridad y cambiarla inmediatamente.
- Firmar los acuerdos de confidencialidad a los que haya lugar en el desarrollo de sus actividades con la empresa y sus clientes.
- Mantener reserva en cuanto a la información de acuerdo con su nivel de clasificación.
- Comunicar cualquier situación sospechosa de ir en contra de las políticas de seguridad de la información de la organización a través de los medios establecidos para tal fin por parte del Oficial de Seguridad de la Información.

- Cuando sea requerido, participar en el proceso de clasificación de los activos de información, así como en la valoración de los riesgos de seguridad de la información proporcionando información veraz y completa al respecto.

7.6 METODOLOGÍA DE ANÁLISIS DE RIESGOS

La metodología de riesgos de ***Consultora JC S.A.S.*** está compuesta por las siguientes etapas:

Imagen 7-1 Ciclo de gestion de riesgos

- Identificación
  - Identificación de activos.
  - Identificación de riesgos.
- Análisis
  - Valoración de impacto y probabilidad.
  - Nivel de riesgo.
- Evaluación
  - Revisión de controles.
  - Comparación con el nivel aceptable de riesgo.
- Tratamiento

7.6.1 IDENTIFICACIÓN

7.6.1.1 Identificación de activos

Consultora JC S.A.S. debe mantener un inventario actualizado de sus activos de información, agrupándolos de acuerdo con los siguientes tipos de activo[27]:

- Superiores
  - Información
  - Servicios
- Inferiores
  - Datos
  - Claves criptográficas
  - Personal
  - Instalaciones
  - Comunicaciones
  - Hardware
  - Software
  - Equipamiento auxiliar

En esta etapa se identifica al propietario como responsable de los activos de información con el fin de establecer quién estará a cargo de la identificación y análisis de riesgos, debido a que cuenta con el conocimiento sobre el proceso, servicio y la importancia que tienen los activos de información para obtener los resultados esperados con respecto a dichos procesos o servicios.

El propietario de los activos de información es aquel que pueda tomar decisiones relacionadas con la selección de la opción de tratamiento del riesgo, la implementación de los controles de seguridad o la formalizar su aceptación. El responsable del activo es aquel al que se le ha delegado su custodia o que, por sus funciones dentro del proceso o la organización, es quien interactúa directamente con el activo y debe velar por su seguridad.

Como resultado de la identificación de los activos de información se obtendrá una tabla como la del siguiente ejemplo.

ID	TIPO	ACTIVO	PROPIETARIO
AS_1	Información	Base de datos de tickets (iTop)	Director Operaciones
AS_2	Información	Reportes a clientes	Director Operaciones
AS_3	Información	Configuración de correlación y monitorización	Gerente de SOC
AS_4	Información	Cronogramas de proyectos	Gerente de proyecto
AS_5	Información	Base de datos de empleados	Director Administrativo

Tabla 7-3 Inventario de activos

Los activos superiores deben ser valorados de acuerdo con su criticidad para el proceso y la organización tomando como criterio la gravedad que tendría para el proceso y para la empresa la materialización de un riesgo que afecte su confidencialidad, integridad, disponibilidad, de acuerdo con las siguientes descripciones:

[27] Adaptado de MAGERIT v 3.0 de acuerdo con las necesidades de la empresa

VALORACIÓN	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Crítica	La divulgación, fuga o acceso no autorizado a uno o varios activos de información afecta de manera muy grave a la organización o a alguno de sus clientes. Se pueden producir sanciones legales o demandas. Puede ser la divulgación no autorizada de información estratégica o relacionada con la seguridad de sus clientes.	La alteración accidental o intencionada de uno o varios activos de información afecta de manera muy grave a la organización o a alguno de sus clientes. Se pueden producir detenciones de algún proceso misional debido a la necesidad de regenerar o reconstruir información.	La pérdida o imposibilidad de acceder a uno o varios activos de información afecta de manera muy grave a la organización o alguno de sus clientes. Se pueden generar detenciones de algún proceso misional debido a la indisponibilidad de la información. Puede ser la pérdida de algún servicio que detenga la ejecución normal de los procesos.
Alta	La divulgación, fuga o acceso no autorizado a uno o varios activos de información afecta de manera grave a alguno de sus procesos o se ve afectado uno de sus clientes. Se pueden producir investigaciones por parte de entes de control o quejas/reclamos por parte de un cliente. Puede ser la divulgación no autorizada de información confidencial de su operación o de los acuerdos con sus clientes.	La alteración accidental o intencionada de uno o varios activos de información afecta de manera grave a alguno de sus procesos o está involucrada información de uno o varios clientes. Se puede requerir la recuperación de información.	La pérdida o imposibilidad de acceder a uno o varios activos de información afecta de manera grave a alguno de sus procesos o clientes. Se pueden generar una interrupción temporal de algún proceso debido a la indisponibilidad de la información. Puede ser la intermitencia o degradación de algún servicio que afecte la ejecución normal de los procesos.
Media	La divulgación, fuga o acceso no autorizado a uno o varios activos de información afecta a alguno de sus procesos sin impacto a los clientes. Puede ser la divulgación de activos de información clasificados como confidenciales dentro de la empresa o alguno de sus aliados sin mayor repercusión.	La alteración accidental o intencionada de uno o varios activos de información afecta a alguno de sus procesos sin impacto a los clientes. La información puede recuperarse fácilmente, pero es complejo identificar la pérdida de integridad rápidamente. Puede ser información interna comprometida.	La pérdida o imposibilidad de acceder a uno o varios activos de información afecta a alguno de sus procesos son impacto a los clientes. La información puede recuperarse fácilmente, pero toma un tiempo importante. La falla puede recuperarse y casi no se presenta pérdida de servicios, pero requiere de la intervención humana.

VALORACIÓN	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Baja	La divulgación, fuga o acceso no autorizado a uno o varios activos de información no afecta de forma considerable a la compañía o a sus clientes. Puede ser la divulgación de activos de información clasificados como internos de la empresa.	La alteración accidental o intencionada de uno o varios activos de información no afecta de forma considerable a la compañía o sus clientes. La información puede recuperarse fácilmente y es posible identificar la pérdida de integridad rápidamente.	La pérdida o imposibilidad de acceder a uno o varios activos de información no afecta de forma considerable a la organización o sus clientes. La información puede recuperarse fácilmente. La falla puede recuperarse rápidamente y casi no se presenta pérdida de servicios.

Tabla 7-4 Criterios para la valoración de los activos de información

Una vez valorado el activo en las dimensiones de Confidencialidad, Integridad, y Disponibilidad se debe generar el resultado final de la valoración del activo de información de acuerdo con la siguiente fórmula:

$$Valor = C + I + D$$

El valor resultante se ubica en la siguiente tabla y este resultado se establece como el valor total del activo.

VALOR (C+I+D)	NIVEL FINAL
12	C: crítica
11	
10	
9	A: alta
8	
7	
6	M: media
5	
4	
3	B: baja
2	
1	

Tabla 7-5 Valoración total del activo

Los activos inferiores heredan la valoración del activo de nivel superior relacionado. En el caso en que un activo inferior esté relacionado con más de un activo de nivel superior, hereda la valoración más alta de todas las de los activos superiores.

Aquellos activos cuyo resultado se encuentre en los niveles Crítico y Alto de acuerdo con la valoración anterior, serán aquellos a incluir en el análisis de riesgo posterior. Esto con el fin de

simplificar el análisis enfocándose en los activos más importantes para la operación de los procesos y la organización.

7.6.1.2 Identificación de riesgos

Durante la etapa de identificación de riesgos se identifican aquellas situaciones que potencialmente pueden desviar los resultados esperados del proceso objeto del análisis debido a la afectación de los activos de información. Estas desviaciones pueden ser negativas o positivas, es decir, pueden aumentar, acelerar, degradar, retrasar o evitar el logro de los objetivos.

Para la identificación de riesgos se pueden tener en cuenta eventos que se hayan presentado en el pasado, o aquellos que se pueden presentar a futuro (de acuerdo con la experiencia y conocimiento de los involucrados en el proceso y el contexto de la organización). También se debe tener en cuenta las debilidades (vulnerabilidades) o la carencia de controles que pueden propiciar la materialización del riesgo, estas debilidades pueden aumentar la probabilidad de ocurrencia de los escenarios de riesgo analizados.

7.6.2 ANÁLISIS

7.6.2.1 Valoración de impacto y probabilidad

Durante la primera parte del análisis se debe valorar el impacto y la probabilidad de ocurrencia del riesgo analizado seleccionado los valores de las tablas definidas a continuación.

VALOR	DESCRIPCIÓN
Bajo	El daño derivado de la materialización del riesgo no tiene consecuencias relevantes para ***Consultora JC S.A.S.*** En este nivel se encuentran situaciones como: - Casos en los cuales se presenta la modificación, destrucción, o fuga de al menos un activo de información de criticidad baja. - La interrupción momentánea del proceso.
Medio	El daño derivado de la materialización del riesgo tiene algunas consecuencias para ***Consultora JC S.A.S.*** En este nivel se encuentran situaciones como: - La afectación en los resultados esperados de un proceso misional. - Casos en los cuales se presenta la modificación, destrucción, o fuga de al menos un activo de información de criticidad media. - El incumplimiento de los requisitos de un contrato con un cliente o proveedor que generen sanciones para la organización.
Alto	El daño derivado de la materialización del riesgo tiene consecuencias relevantes para ***Consultora JC S.A.S.*** En este nivel se encuentran situaciones como: - La interrupción de un proceso misional. - Casos en los cuales se presenta la modificación, destrucción, o fuga de al menos un activo de información de criticidad alta. - El incumplimiento de alguna ley o regulación aplicable a la organización. - El incumplimiento de los requisitos de un contrato un cliente o proveedor que causen la interrupción prolongada o cancelación de un contrato.

VALOR	DESCRIPCIÓN
	- La interrupción prolongada se servicios de suministro a los procesos de negocio (Internet, fluido eléctrico, correo electrónico, red interna, etc.)

Tabla 7-6 Escala de valoración del impacto

Para la valoración de la probabilidad de ocurrencia de un riesgo se puede tomar como referencia información histórica que permita identificar eventos o situaciones que han ocurrido en el pasado y suponer de manera razonable la probabilidad de ocurrencia en el futuro.

VALOR	DESCRIPCIÓN
Poco probable	El riesgo se ha materializado alguna vez en la historia de la empresa. Se considera poco probable que el riesgo se materialice durante el próximo año.
Posible	El riesgo se ha materializado al menos una vez durante el año anterior. Se considera razonablemente probable que el riesgo se materialice durante el próximo año.
Probable	El riesgo se ha materializado dos veces o más durante el año anterior. Se considera prácticamente inminente que el riesgo se materialice durante los próximos meses.

Tabla 7-7 Escala de valoración de la probabilidad

Una vez valorada la probabilidad y el impacto de cada uno de los escenarios de riesgo, se procede a calcular en valor definitivo del riesgo inherente como se explica en la siguiente sección.

7.6.2.2 Nivel de riesgo

Con base en la valoración de los criterios descritos en el numeral anterior (probabilidad e impacto) se calcula el nivel de riesgo final para cada escenario de riesgo propuesto. Este nivel corresponde al riesgo inherente, es decir aquel en el cual aún no se ha evaluado el efecto de los controles presentes en la valoración de las dos dimensiones que lo componen. El resultado de la valoración se obtiene del producto cartesiano descrito a continuación:

Impacto				
	Alto	Riesgo apreciable	Riesgo importante	Riesgo importante
	Medio	Riesgo bajo	Riesgo apreciable	Riesgo importante
	Bajo	Riesgo bajo	Riesgo bajo	Riesgo apreciable
		Bajo	Medio	Alto

Probabilidad

Tabla 7-8 Plano cartesiano de valoración del nivel de riesgo

Una vez el nivel de riesgo ha sido identificado para cada uno de los escenarios de riesgo, y teniendo en cuenta que el nivel aceptable para la organización es el nivel de *Riesgo Apreciable*, se identifica el propietario del riesgo para cada uno de los escenarios valorados como *Riesgo Importante*. El propietario del riego es la persona o entidad con la responsabilidad y autoridad para gestionar un riesgo y será el responsable de seleccionar la opción de tratamiento de acuerdo con lo que se describe en el capítulo 7.6.4 Tratamiento.

7.6.3 EVALUACIÓN

7.6.3.1 Revisión de controles

Una vez identificados los escenarios de riesgo y valorado el riesgo inherente, se documentan los controles de seguridad que se encuentran actualmente establecidos, y se evalúa su nivel de madurez de acuerdo con la escala del Framework CobIT v5 (ISACA, 2012):

- **0 - Proceso incompleto:** El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.
- **1 - Proceso ejecutado:** El proceso implementado alcanza su propósito.
- **2 - Proceso gestionado:** El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.
- **3 - Proceso establecido:** El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso.
- **4 - Proceso predecible:** El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.
- **5 - Proceso optimizado**: El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con las metas empresariales presentes y futuros.

El efecto de los controles sobre el riesgo inherente (cuyo resultad es el riesgo residual), se calcula de acuerdo con la siguiente tabla:

Riesgo inherente	Promedio de valoración de controles	Riesgo residual
Riesgo bajo	5 - Proceso optimizado	Riesgo bajo

Riesgo inherente	Promedio de valoración de controles	Riesgo residual
Riesgo bajo	4 - Proceso predecible	Riesgo bajo
Riesgo bajo	3 - Proceso establecido	Riesgo bajo
Riesgo bajo	2 - Proceso gestionado	Riesgo bajo
Riesgo bajo	1 - Proceso ejecutado	Riesgo bajo
Riesgo apreciable	5 - Proceso optimizado	Riesgo bajo
Riesgo apreciable	4 - Proceso predecible	Riesgo bajo
Riesgo apreciable	3 - Proceso establecido	Riesgo bajo
Riesgo apreciable	2 - Proceso gestionado	Riesgo bajo
Riesgo apreciable	1 - Proceso ejecutado	Riesgo apreciable
Riesgo importante	5 - Proceso optimizado	Riesgo bajo
Riesgo importante	4 - Proceso predecible	Riesgo bajo
Riesgo importante	3 - Proceso establecido	Riesgo apreciable
Riesgo importante	2 - Proceso gestionado	Riesgo apreciable
Riesgo importante	1 - Proceso ejecutado	Riesgo importante

Tabla 7-9 Cálculo del efecto de los controles sobre el riesgo inherente

7.6.3.2 Comparación con el nivel aceptable de riesgo.

Finalmente se compara el nivel de riesgo residual par cada uno de los escenarios de riesgo evaluados y con base en el nivel de riesgo aceptable se seleccionan aquellos que se encuentran por debajo de este nivel y se definen planes de tratamiento para disminuirlo a niveles aceptables para la organización.

7.6.4 TRATAMIENTO

La organización decidió dar tratamiento a los riesgos cuya valoración es “A: Importante”, para lo cual tiene la opción de eliminarlo, mitigarlo, transferirlo o aceptarlo.

- **Eliminar el riesgo:** De acuerdo con Magerit 3.0 consiste en “*la eliminación de la fuente de riesgo*” y puede tomar básicamente dos formas: “*Eliminar cierto tipo de activos, empleando otros en su lugar*” o “*Reordenar la arquitectura del sistema de forma que*

alteremos el valor acumulado en ciertos activos expuestos a grandes amenazas" (Ministerio de Hacienda y Administraciones Públicas, 2012).

- **Mitigar el riesgo:** De acuerdo con Magerit 3.0 se tienen dos alternativas para mitigar el riesgo: "*reducir la degradación causada por una amenaza*" o "*reducir la probabilidad de que una amenaza de materializa*" (Ministerio de Hacienda y Administraciones Públicas, 2012). En cualquiera de los dos casos la mitigación suele requerir de la implementación de controles tomados de la guía GTC-ISO-IEC 27002:2013.
- **Transferir el riesgo:** De acuerdo con Magerit 3.0 se puede transferir o compartir el riesgo "*por medio de la externalización de componentes del sistema, de forma que se reparten responsabilidades: unas técnicas para el que opera el componente técnico; y otras legales según el acuerdo que se establezca de prestación del servicio*" o "*por medio de la contratación de seguros, de forma que a cambio de una prima, el tomador reduce el impacto de las posibles amenazas y el asegurador corre con las consecuencias*" (Ministerio de Hacienda y Administraciones Públicas, 2012).
- **Aceptar el riesgo:** La aceptación del riesgo implica la toma consciente de la decisión de no eliminar, mitigar o transferir el riesgo por lo cual es necesario que la empresa reserve fondos para responder en caso de que el riesgo se materialice. Esta aceptación debe quedar documentada formalmente puesto que se trata de casos en los cuales usualmente el costo de la implementación de controles es más elevado que el generado por una eventual materialización.

La selección de controles se realiza en conjunto con el propietario del riesgo, líder del proceso objeto del análisis y se establece una fecha proyectada para su implementación.

7.6.5 PLAN DE TRATAMIENTO DE RIESGOS

El plan de tratamiento está compuesto por los proyectos priorizados para la implementación de controles de seguridad en la organización. Los controles seleccionados son aquellos que se requieren para tratar los riesgos en los cuales se ha tomado la decisión de disminuir su probabilidad de ocurrencia o el impacto en caso de materializarse.

Para el desarrollo de estos planes se tomará como base la descripción de controles de seguridad que se encuentra en la guía GTC-ISO-IEC 27002:2013, teniendo en cuenta que pueden ser controles, por su naturaleza, Administrativos, Técnicos o Físicos dependiendo del tipo de riesgo y la necesidad de protección que se presente.

7.7 DECLARACIÓN DE APLICABILIDAD

En la siguiente tabla se presenta la Declaración de Aplicabilidad preliminar, antes de la ejecución del análisis de riesgo. Por esta razón, es posible que sea actualizada con base en los resultados del análisis.

CONTROLES	APLICA	JUSTIFICACIÓN
5.1.1 Políticas para la seguridad de la información.	SI	Se ha identificado la necesidad de contar con políticas de seguridad de la información para establecer las normas de seguridad dentro de la compañía
5.1.2 Revisión de las políticas para la seguridad de la información.	SI	Se ha identificado la necesidad de contar con políticas de seguridad de la información para establecer las normas de seguridad dentro de la compañía
6.1.1 Roles y responsabilidades para la seguridad de la información.	SI	Existen algunas responsabilidades, pero es necesario formalizarlos en la organización
6.1.2 Separación de deberes.	SI	Debido a la sensibilidad de las actividades que se realizan dentro de los procesos en el alcance del SGSI
6.1.3 Contacto con las autoridades.	SI	Debido a la sensibilidad de las actividades que se realizan dentro de los procesos en el alcance del SGSI
6.1.4 Contacto con grupos de interés especial.	SI	Debido a la sensibilidad de las actividades que se realizan dentro de los procesos en el alcance del SGSI
6.1.5 Seguridad de la información en la gestión de proyectos.	SI	Debido a la sensibilidad de la información que se maneja en los proyectos
6.2.1 Política para dispositivos móviles.	SI	Se ha identificado la necesidad de contar con políticas de seguridad de la información para establecer las normas de seguridad dentro de la compañía
6.2.2 Teletrabajo.	SI	Se ha identificado la necesidad de contar con políticas de seguridad de la información para establecer las normas de seguridad dentro de la compañía
7.1.1 Selección.	SI	Debido a la sensibilidad de la información que se maneja en los proyectos
7.1.2 Términos y condiciones del empleo.	SI	Debido a la sensibilidad de la información que se maneja en los proyectos
7.2.1 Responsabilidades de la dirección.	SI	Con el fin de establecer claramente el rol de la Dirección General
7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	SI	con el fin de divulgar y capacitar al personal en los aspectos más relevantes del SGSI
7.2.3 Proceso disciplinario.	SI	Debido a la sensibilidad de la información que se maneja en los proyectos
7.3.1 Terminación o cambio de responsabilidades de empleo.	SI	Debido a la sensibilidad de la información que se maneja en los proyectos

CONTROLES	APLICA	JUSTIFICACIÓN
8.1.1 Inventario de activos.	SI	Con el fin de controlar la información debido a su sensibilidad y alto valor
8.1.2 Propiedad de los activos.	SI	Con el fin de controlar la información debido a su sensibilidad y alto valor
8.1.3 Uso aceptable de los activos.	SI	Con el fin de controlar la información debido a su sensibilidad y alto valor
8.1.4 Devolución de activos.	SI	Con el fin de controlar la información debido a su sensibilidad y alto valor
8.2.1 Clasificación de la información.	SI	Con el fin de controlar la información debido a su sensibilidad y alto valor
8.2.2 Etiquetado de la información.	SI	Con el fin de controlar la información debido a su sensibilidad y alto valor
8.2.3 Manejo de activos.	SI	Se ha identificado la necesidad de contar con políticas de seguridad de la información para establecer las normas de seguridad dentro de la compañía
8.3.1 Gestión de medios removibles.	SI	Debido a la sensibilidad de la información que se maneja en los proyectos
8.3.2 Disposición de medios.	SI	Debido a la sensibilidad de la información que se maneja en los proyectos
8.3.3 Transferencia de medios físicos.	SI	Debido a la sensibilidad de la información que se maneja en los proyectos
9.1.1 Política de control de acceso.	SI	Se ha identificado la necesidad de contar con políticas de seguridad de la información para establecer las normas de seguridad dentro de la compañía
9.1.2 Control de acceso a las redes y servicios asociados.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
9.2.1 Registro y cancelación del registro de usuarios.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
9.2.2 Suministro de acceso de usuarios.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
9.2.3 Gestión de derechos de acceso privilegiado.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
9.2.4 Gestión de información de autenticación secreta de usuarios.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
9.2.5 Revisión de los derechos de acceso de los usuarios.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
9.2.6 Retiro o ajuste de los derechos de acceso.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
9.3.1 Uso de información de autenticación secreta.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red

CONTROLES	APLICA	JUSTIFICACIÓN
9.4.1 Restricción de acceso a la información.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
9.4.2 Procedimiento de ingreso seguro.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
9.4.3 Sistema de gestión de contraseñas.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
9.4.4 Uso de programas utilitarios privilegiados.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
9.4.5 Control de acceso a códigos fuente de programas.	NO	No se almacena código fuente
10.1.1 Política sobre el uso de controles criptográficos.	SI	Debido a que se implementan controles criptográficos para la protección de la información
10.1.2 Gestión de claves.	SI	Debido a que se implementan controles criptográficos para la protección de la información
11.1.1 Perímetro de seguridad física.	SI	Debido a que las operaciones de los procesos se realizan en áreas que deben ser aseguradas físicamente
11.1.2 Controles de acceso físicos.	SI	Debido a que las operaciones de los procesos se realizan en áreas que deben ser aseguradas físicamente
11.1.3 Seguridad de oficinas, recintos e instalaciones.	SI	Debido a que las operaciones de los procesos se realizan en áreas que deben ser aseguradas físicamente
11.1.4 Protección contra amenazas externas y ambientales.	SI	Debido a la presencia de equipos tecnológicos importantes para los procesos dentro de las instalaciones de la empresa
11.1.5 Trabajo en áreas seguras.	SI	Debido a que las operaciones de los procesos se realizan en áreas que deben ser aseguradas físicamente
11.1.6 Áreas de despacho y carga.	SI	Se han identificado áreas donde se reciben y despachan equipos tecnológicos
11.2.1 Ubicación y protección de los equipos.	SI	Debido a la presencia de equipos tecnológicos importantes para los procesos dentro de las instalaciones de la empresa
11.2.2 Servicios de suministro.	SI	Debido a la presencia de equipos tecnológicos importantes para los procesos dentro de las instalaciones de la empresa
11.2.3 Seguridad del cableado.	SI	Debido a la presencia de equipos tecnológicos importantes para los procesos dentro de las instalaciones de la empresa
11.2.4 Mantenimiento de equipos.	SI	Debido a la presencia de equipos tecnológicos importantes para los procesos dentro de las instalaciones de la empresa

CONTROLES	APLICA	JUSTIFICACIÓN
11.2.5 Retiro de equipos.	SI	Debido a la presencia de equipos tecnológicos importantes para los procesos dentro de las instalaciones de la empresa
11.2.6 Seguridad de equipos y activos fuera de las instalaciones.	SI	Teniendo en cuenta que algunos equipos se utilizan por fuera de las instalaciones físicas
11.2.7 Disposición segura o reutilización de equipos.	SI	Debido a que los equipos almacenan información sensible
11.2.8 Equipos de usuario desatendido.	SI	Debido a que los equipos almacenan información sensible
11.2.9 Política de escritorio limpio y pantalla limpia.	SI	Debido a que los equipos almacenan información sensible
12.1.1 Documentación de procedimientos de operación.	SI	Debido a la alta rotación del personal que trabaja en los procesos
12.1.2 Gestión de cambios.	SI	Debido a la sensibilidad de la información que se maneja en los proyectos
12.1.3 Gestión de capacidades.	SI	Debido a que se genera información en altos volúmenes y se depende de otras capacidades de comunicaciones y suministros
12.1.4 Separación de entornos de desarrollo, prueba y producción.	NO	No se desarrolla software en los procesos ni se cuenta con ambientes de prueba o desarrollo.
12.2.1 Controles contra el código malicioso.	SI	Debido a que los equipos almacenan información sensible
12.3.1 Copias de seguridad de la información.	SI	Debido a que los equipos almacenan información sensible
12.4.1 Registro y gestión de eventos de actividad.	SI	Debido a la sensibilidad de las actividades que se realizan dentro de los procesos en el alcance del SGSI
12.4.2 Protección de los registros de información.	SI	Debido a la sensibilidad de las actividades que se realizan dentro de los procesos en el alcance del SGSI
12.4.3 Registros de actividad del administrador y operador del sistema.	SI	Debido a la sensibilidad de las actividades que se realizan dentro de los procesos en el alcance del SGSI
12.4.4 Sincronización de relojes.	SI	Con el fin de correlacionar los eventos generados
12.5.1 Instalación del software en sistemas operativos.	SI	Debido a que los equipos almacenan información sensible
12.6.1 Gestión de las vulnerabilidades técnicas.	SI	Debido a que los equipos almacenan información sensible
12.6.2 Restricciones en la instalación de software.	SI	Debido a que los equipos almacenan información sensible

CONTROLES	APLICA	JUSTIFICACIÓN
12.7.1 Controles de auditoría de los sistemas de información.	SI	Debido a que los equipos almacenan información sensible
13.1.1 Controles de red.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
13.1.2 Seguridad de los servicios de red.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
13.1.3 Segregación de redes.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
13.2.1 Políticas y procedimientos de intercambio de información.	SI	Se ha identificado la necesidad de contar con políticas de seguridad de la información para establecer las normas de seguridad dentro de la compañía
13.2.2 Acuerdos de intercambio.	SI	Con el fin de proteger la información que se intercambia con terceros
13.2.3 Mensajería electrónica.	SI	Con el fin de proteger la información que se intercambia con terceros
13.2.4 Acuerdos de confidencialidad y secreto.	SI	Con el fin de proteger la información que se intercambia con terceros
14.1.1 Análisis y especificación de los requisitos de seguridad.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
14.1.3 Protección de las transacciones por redes telemáticas.	NO	No se realizan este tipo de transacciones
14.2.1 Política de desarrollo seguro de software.	NO	No se desarrolla software en los procesos incluidos en el alcance del SGSI
14.2.2 Procedimientos de control de cambios en los sistemas.	NO	No se desarrolla software en los procesos incluidos en el alcance del SGSI
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	SI	Debido a la sensibilidad de la información que se maneja en los equipos y la red
14.2.4 Restricciones a los cambios en los paquetes de software.	NO	No se desarrolla software en los procesos incluidos en el alcance del SGSI
14.2.5 Uso de principios de ingeniería en protección de sistemas.	NO	No se desarrolla software en los procesos incluidos en el alcance del SGSI
14.2.6 Seguridad en entornos de desarrollo.	NO	No se desarrolla software en los procesos incluidos en el alcance del SGSI
14.2.7 Externalización del desarrollo de software.	NO	No se desarrolla software en los procesos incluidos en el alcance del SGSI

CONTROLES	APLICA	JUSTIFICACIÓN
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	NO	No se desarrolla software en los procesos incluidos en el alcance del SGSI
14.2.9 Pruebas de aceptación.	NO	No se desarrolla software en los procesos incluidos en el alcance del SGSI
14.3.1 Protección de los datos utilizados en pruebas.	NO	No se desarrolla software en los procesos incluidos en el alcance del SGSI
15.1.1 Política de seguridad de la información para las relaciones con proveedores.	SI	Con el fin de proteger la información que se intercambia con terceros
15.1.2 Tratamiento de la seguridad dentro de acuerdos con proveedores.	SI	Con el fin de proteger la información que se intercambia con terceros
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	SI	Con el fin de proteger la información que se intercambia con terceros
15.2.1 Seguimiento y revisión de los servicios de los proveedores.	SI	Con el fin de proteger la información que se intercambia con terceros
15.2.2 Gestión de cambios en los servicios de los proveedores.	SI	Con el fin de proteger la información que se intercambia con terceros
16.1.1 Responsabilidades y procedimientos.	SI	Con el fin de gestionar las situaciones adversas con respecto a la seguridad de la información
16.1.2 Reporte de eventos de seguridad de la información.	SI	Con el fin de gestionar las situaciones adversas con respecto a la seguridad de la información
16.1.3 Reporte de debilidades de seguridad de la información.	SI	Con el fin de gestionar las situaciones adversas con respecto a la seguridad de la información
16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	SI	Con el fin de gestionar las situaciones adversas con respecto a la seguridad de la información
16.1.5 Respuesta a incidentes de seguridad de la información.	SI	Con el fin de gestionar las situaciones adversas con respecto a la seguridad de la información
16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información.	SI	Con el fin de gestionar las situaciones adversas con respecto a la seguridad de la información
16.1.7 Recolección de evidencias.	SI	Con el fin de gestionar las situaciones adversas con respecto a la seguridad de la información
17.1.1 Planificación de la continuidad de la	SI	Con el fin de garantizar la seguridad en los eventos de contingencia

CONTROLES	APLICA	JUSTIFICACIÓN
seguridad de la información.		
17.1.2 Implantación de la continuidad de la seguridad de la información.	SI	Con el fin de garantizar la seguridad en los eventos de contingencia
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	SI	Con el fin de garantizar la seguridad en los eventos de contingencia
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	SI	Con el fin de garantizar la seguridad en los eventos de contingencia
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales.	SI	Con el fin de cumplir con los requerimientos legales y contractuales
18.1.2 Derechos de propiedad intelectual.	SI	Con el fin de cumplir con los requerimientos legales y contractuales
18.1.3 Protección de los registros de la organización.	SI	Con el fin de cumplir con los requerimientos legales y contractuales
18.1.4 Protección de datos y privacidad de la información personal.	SI	Con el fin de cumplir con los requerimientos legales y contractuales
18.1.5 Reglamentación de controles criptográficos.	NO	No existe una reglamentación al respecto
18.2.1 Revisión independiente de la seguridad de la información.	SI	Debido a la necesidad de identificar las fallas y oportunidades de mejora del sistema
18.2.2 Cumplimiento con las políticas y normas de seguridad.	SI	Debido a la necesidad de identificar las fallas y oportunidades de mejora del sistema
18.2.3 Revisión del cumplimiento técnico.	SI	Debido a la necesidad de identificar las fallas y oportunidades de mejora del sistema

Tabla 7-10 Declaración de aplicabilidad

7.8 ANÁLISIS DE RIESGOS

El análisis de riesgo se realizó siguiendo la metodología definida en el numeral 7.6 del presente documento.

7.8.1 INVENTARIO DE ACTIVOS

En la siguiente tabla se presenta el inventario de activos de información que fueron identificados como parte del alcance del Sistema de Gestión de Seguridad de la Información.

Id	Tipo	Activo	Propietario
AS_1	Información	Base de datos de tickets (iTop)	Director Operaciones
AS_2	Información	Reportes a clientes	Director Operaciones
AS_3	Información	Configuración de correlación y monitorización	Gerente de SOC
AS_4	Información	Cronogramas de proyectos	Gerente de proyecto
AS_5	Información	Base de datos de empleados	Director Administrativo
AS_6	Información	Base de datos de clientes	Director Comercial
AS_7	Servicios	Gestión de infraestructura	Gerente de SOC
AS_8	Servicios	Monitorización	Gerente de SOC
AS_9	Servicios	Gerencia de proyectos	Director Operaciones
AI_1	Datos	Logs de monitorización	Gerente de SOC
AI_2	Instalaciones	Datacenter principal	Director Administrativo
AI_3	Instalaciones	Oficina principal	Director Administrativo
AI_4	Comunicaciones	Canal de Internet	Director Administrativo
AI_5	Comunicaciones	Red interna	Director Administrativo
AI_6	Hardware	Servidor Físico	Director Operaciones
AI_7	Equipamiento auxiliar	VideoWall	Gerente de SOC
AI_8	Hardware	Equipos de usuario final	Director Administrativo
AI_9	Hardware	Firewall UTM	Director Operaciones
AI_10	Hardware	Switch de comunicaciones	Director Operaciones
AI_11	Equipamiento auxiliar	UPS	Director Administrativo
AI_12	Equipamiento auxiliar	Planta telefónica	Director Administrativo
AI_13	Equipamiento auxiliar	Teléfono móvil	Director Administrativo
AI_14	Software	iTop	Director Operaciones
AI_15	Software	OSSIM	Gerente de SOC
AI_16	Software	Nagios	Gerente de SOC
AI_17	Personal	Ingeniero de operación	Gerente de SOC
AI_18	Personal	Gerente de SOC	Director Operaciones
AI_19	Personal	Gerente de proyecto	Director Operaciones

Tabla 7-11 Inventario de activos de información

Posterior a la identificación de los activos de información se realizó la valoración de los superiores, de forma que los inferiores heredaron este valor. El resultado de la valoración de los activos superiores se presenta en la siguiente tabla.

Id	Tipo	Activo	Propietario	C	I	D	Valor Final
AS_1	Información	Base de datos de tickets (iTop)	Director Operaciones	A: alta	C: crítica	A: alta	C: crítica
AS_2	Información	Reportes a clientes	Director Operaciones	C: crítica	C: crítica	M: media	C: crítica
AS_3	Información	Configuración de correlación y monitorización	Gerente de SOC	M: media	C: crítica	M: media	A: alta

AS_4	Información	Cronogramas de proyectos	Gerente de proyecto	M: media	M: media	B: baja	M: media
AS_5	Información	Base de datos de empleados	Director Administrativo	A: alta	A: alta	A: alta	A: alta
AS_6	Información	Base de datos de clientes	Director Comercial	C: crítica	A: alta	C: crítica	C: crítica
AS_7	Servicios	Gestión de infraestructura	Gerente de SOC	A: alta	C: crítica	A: alta	C: crítica
AS_8	Servicios	Monitorización	Gerente de SOC	B: baja	B: baja	C: crítica	M: media
AS_9	Servicios	Gerencia de proyectos	Director Operaciones	B: baja	A: alta	B: baja	M: media

Tabla 7-12 Valoración de los activos superiores

Con los activos inferiores se realizó un análisis de dependencia en el cual se pudo establecer la relacione entre activos superiores e inferiores para establecer la herencia de la valoración. Esto partiendo de la base de que un activo inferior que es necesario para el correcto funcionamiento de un activo superior tiene el mismo valor para la empresa que el activo superior al cual soporta.

Id	Activo	Dependencia								
AI_1	Logs de monitorización								AS_8	
AI_2	Datacenter principal							AS_7	AS_8	AS_9
AI_3	Oficina principal							AS_7	AS_8	AS_9
AI_4	Canal de Internet							AS_7	AS_8	
AI_5	Red interna							AS_7	AS_8	AS_9
AI_6	Servidor Físico							AS_7	AS_8	AS_9
AI_7	VideoWall								AS_8	
AI_8	Equipos de usuario final		AS_2		AS_4	AS_5	AS_6	AS_7		AS_9
AI_9	Firewall UTM								AS_8	
AI_10	Switch de comunicaciones								AS_8	
AI_11	UPS							AS_7	AS_8	
AI_12	Planta telefónica							AS_7		AS_9
AI_13	Teléfono móvil							AS_7	AS_8	AS_9
AI_14	iTop	AS_1	AS_2					AS_7		
AI_15	OSSIM			AS_3					AS_8	
AI_16	Nagios								AS_8	
AI_17	Ingeniero de operación							AS_7	AS_8	
AI_18	Gerente de SOC							AS_7	AS_8	
AI_19	Gerente de proyecto				AS_4					AS_9

Tabla 7-13 Dependencia de activos superiores con inferiores

De acuerdo con los resultados anteriores, la valoración para los activos inferiores se presenta en la siguiente tabla. Es importante tener en cuenta que en los casos en los que un activo inferior soporta más de un activo superior, se toma la valoración más alta entre los activos

apoyados. Esto debido a que se debe conservar el valor del activo superior más crítico para evitar ignorar riesgos que puedan tener un impacto críticos en la organización.

Id	Tipo	Activo	Propietario	C	I	D	Valor Final
AI_1	Datos	Logs de monitorización	Gerente de SOC	B: baja	B: baja	C: crítica	M: media
AI_2	Instalaciones	Datacenter principal	Director Administrativo	C: crítica	C: crítica	C: crítica	C: crítica
AI_3	Instalaciones	Oficina principal	Director Administrativo	C: crítica	C: crítica	C: crítica	C: crítica
AI_4	Comunicaciones	Canal de Internet	Director Administrativo	C: crítica	C: crítica	C: crítica	C: crítica
AI_5	Comunicaciones	Red interna	Director Administrativo	C: crítica	C: crítica	C: crítica	C: crítica
AI_6	Hardware	Servidor Físico	Director Operaciones	C: crítica	C: crítica	C: crítica	C: crítica
AI_7	Equipamiento auxiliar	VideoWall	Gerente de SOC	C: crítica	C: crítica	C: crítica	C: crítica
AI_8	Hardware	Equipos de usuario final	Director Administrativo	A: alta	C: crítica	A: alta	C: crítica
AI_9	Hardware	Firewall UTM	Director Operaciones	B: baja	B: baja	C: crítica	M: media
AI_10	Hardware	Switch de comunicaciones	Director Operaciones	B: baja	B: baja	C: crítica	M: media
AI_11	Equipamiento auxiliar	UPS	Director Administrativo	C: crítica	C: crítica	C: crítica	C: crítica
AI_12	Equipamiento auxiliar	Planta telefónica	Director Administrativo	A: alta	C: crítica	A: alta	C: crítica
AI_13	Equipamiento auxiliar	Teléfono móvil	Director Administrativo	C: crítica	C: crítica	C: crítica	C: crítica
AI_14	Software	iTop	Director Operaciones	A: alta	C: crítica	A: alta	C: crítica
AI_15	Software	OSSIM	Gerente de SOC	C: crítica	C: crítica	C: crítica	C: crítica
AI_16	Software	Nagios	Gerente de SOC	B: baja	B: baja	C: crítica	M: media
AI_17	Personal	Ingeniero de operación	Gerente de SOC	C: crítica	C: crítica	C: crítica	C: crítica
AI_18	Personal	Gerente de SOC	Director Operaciones	C: crítica	C: crítica	C: crítica	C: crítica
AI_19	Personal	Gerente de proyecto	Director Operaciones	B: baja	A: alta	B: baja	M: media

Tabla 7-14 Valoración de los activos inferiores

7.8.2 ANÁLISIS DE RIESGO INHERENTE

Posterior al cálculo del riesgo de acuerdo con la metodología propuesta, se identificaron 83 escenarios diferentes sobre los activos superiores e inferiores y cuyo resultado se encuentra por encima del umbral de riesgo aceptable (el cual se estableció por la Alta Dirección en M: apreciable). En la siguiente gráfica se observa la distribución porcentual del total de escenarios identificados.

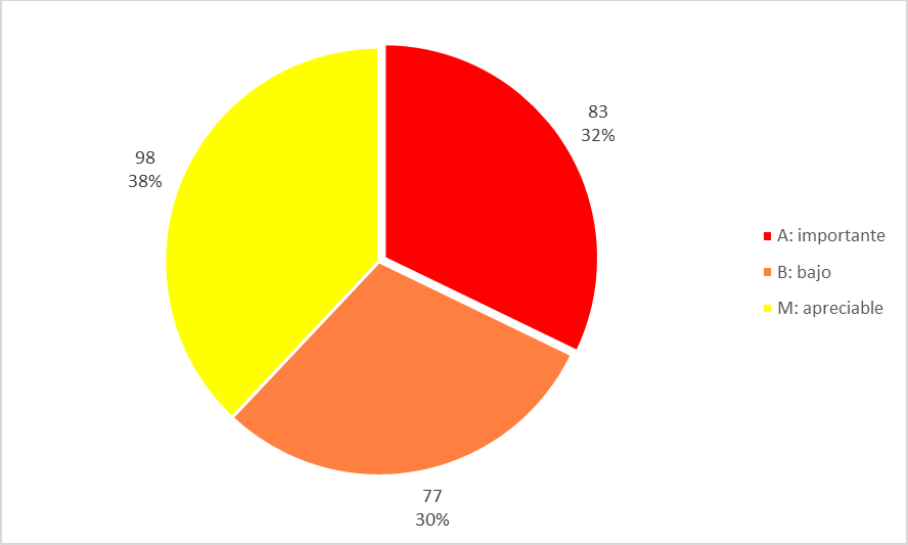


Imagen 7-2 Distribución de escenarios de riesgo por valoración

De los 83 escenarios que se encuentran por encima del nivel de riesgo aceptable, algunos de ellos son recurrentes a través de múltiples activos de información. La cantidad de riesgos más recurrentes se muestran en la siguiente gráfica, en la cual se observa que la fuga de información es la principal amenaza, seguida por los errores de los administradores y de los usuarios respectivamente.

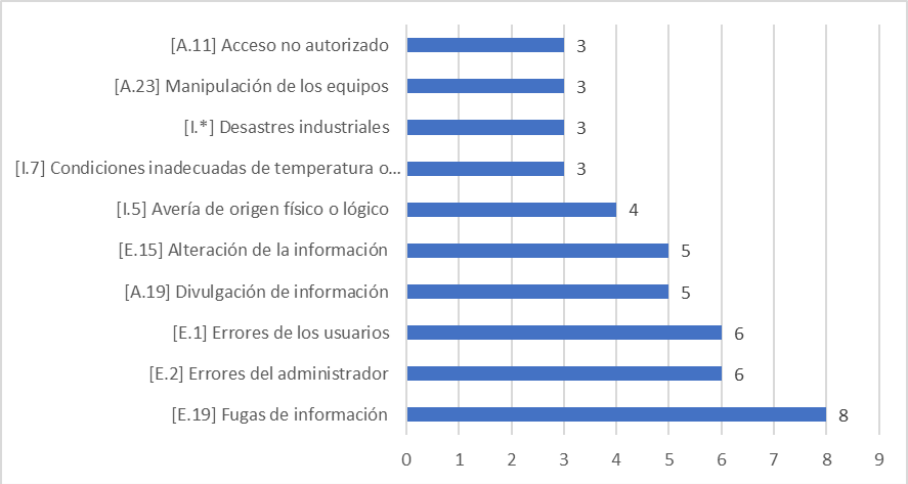


Imagen 7-3 Cantidad de escenarios recurrentes

Es te análisis permitirá definir controles transversales para atender problemáticas comunes a lo largo de la organización (por ejemplo, la fuga de la información) permitiendo, de alguna forma, crear sinergias para la protección de la información, optimizando la inversión. En esta misma línea, es identificar tipos de activo con mayor cantidad de riesgos identificados permite a la organización establecer planes de trabajo transversales, de manera que se aborden estrategias de protección más eficientes. En la siguiente gráfica se puede observar la cantidad de riesgos (que se encuentran por encima del umbral de riesgo aceptable) por tipo de activo.

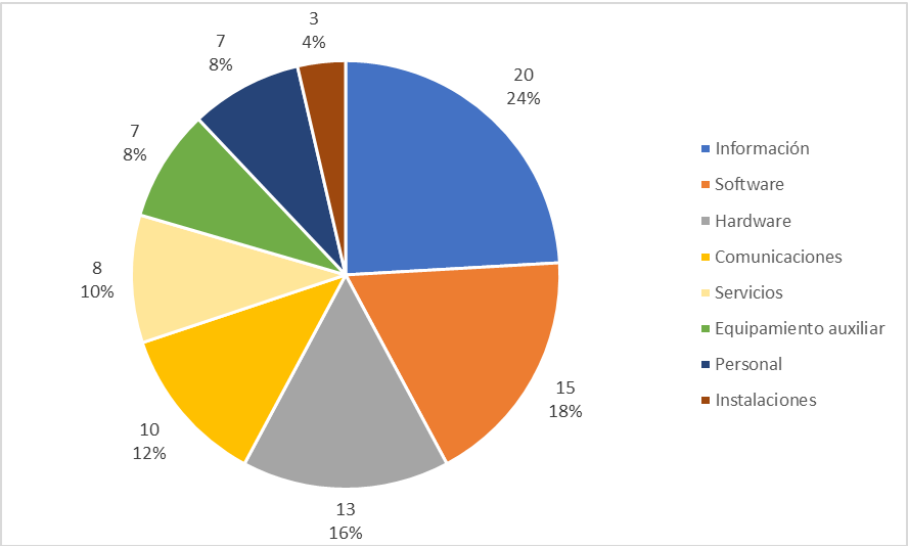


Imagen 7-4 Distribución de riesgos A: importante por tipo de activo

En el Anexo 3 - *Matriz de Riesgos.xlsx*, se encuentra el detalle de la valoración de cada uno de los escenarios de riesgo y los resultados de las valoraciones de probabilidad, impacto y riesgo inherente.

8 PROPUESTAS DE PROYECTOS

Como parte de la gestión de riesgos de seguridad de la información, se tomarán acciones orientadas al despliegue de medidas de control que permita mitigar, bien sea la probabilidad de ocurrencia o el impacto, de aquellas situaciones que potencialmente pueden generar riesgos intolerables para la organización. Algunas de las iniciativas se han agrupado en un solo proyecto debido a su afinidad y otras corresponden a proyectos independientes. En el Anexo 4 - *Cronograma de trabajo (Propuestas de proyectos).mpp* se encuentra el cronograma completo de trabajo para las propuestas de proyectos a desarrollar, el cual se muestra en la siguiente imagen:

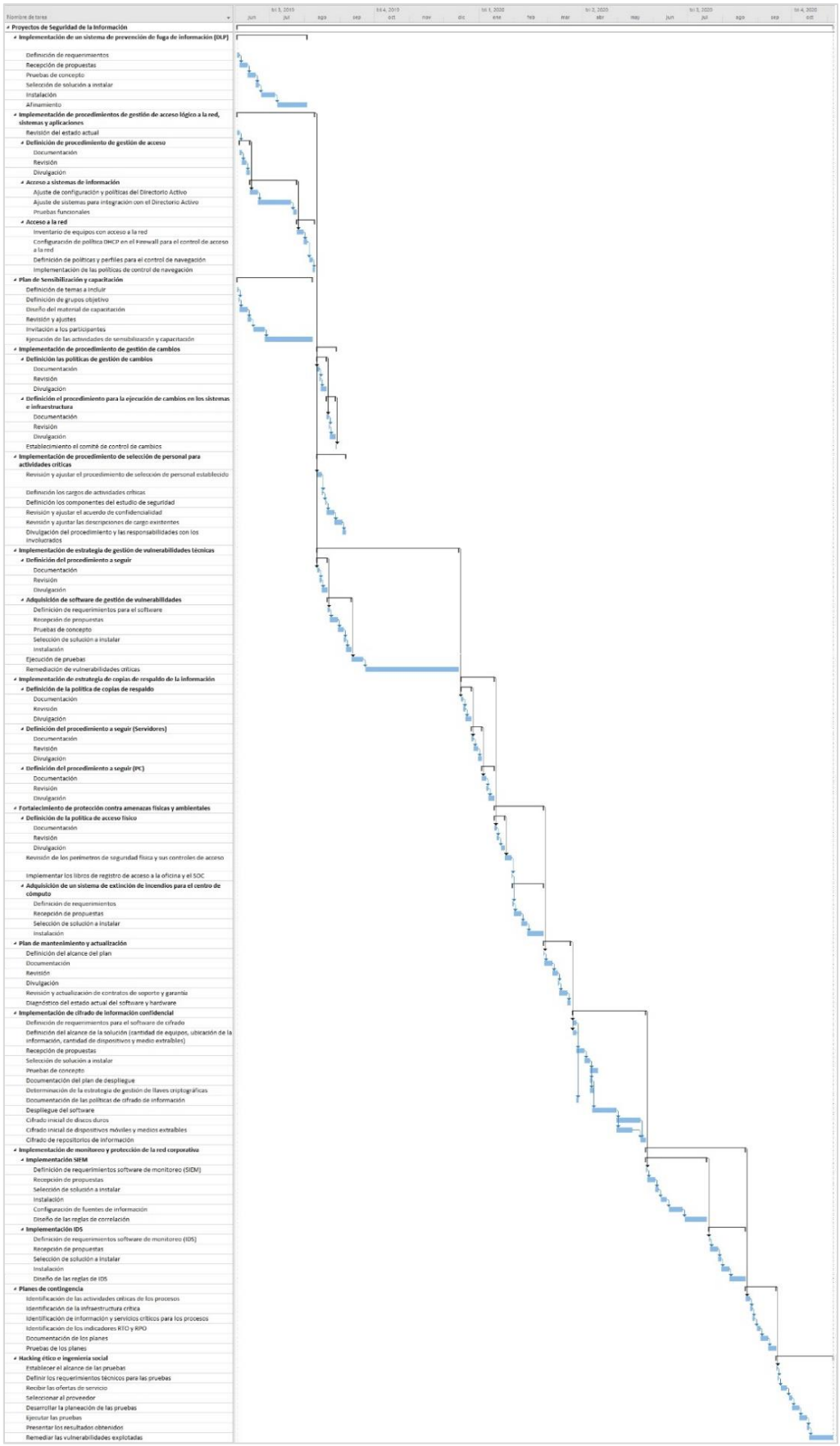


Imagen 8-1 Cronograma de trabajo - Proyectos de seguridad

A continuación, se detalla cada uno de los proyectos con su cronograma de trabajo particular:

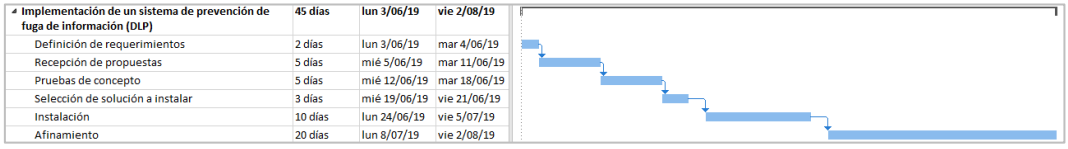
8.1 IMPLEMENTACIÓN DE UN SISTEMA DE PREVENCIÓN DE FUGA DE INFORMACIÓN (DLP)

8.1.1 OBJETIVO

Implementar un sistema para la protección de la información confidencial de la organización de su divulgación, bien sea accidental o no, a través del monitoreo y establecimiento de reglas de bloqueo para los siguientes vectores de comunicación que se utilizan en los procesos dentro del alcance del SGSI:

- Información que se copia a dispositivos de almacenamiento extraíble.
- Información que se envía por correo electrónico.
- Información que se comparte a través de aplicaciones en la nube.
- Documentos que se imprimen.
- Información que se copia a través del portapapeles.
- Captura de pantalla.

8.1.2 CRONOGRAMA



Implementación de un sistema de prevención de fuga de información (DLP)	45 días	lun 3/06/19	vie 2/08/19
Definición de requerimientos	2 días	lun 3/06/19	mar 4/06/19
Recepción de propuestas	5 días	mié 5/06/19	mar 11/06/19
Pruebas de concepto	5 días	mié 12/06/19	mar 18/06/19
Selección de solución a instalar	3 días	mié 19/06/19	vie 21/06/19
Instalación	10 días	lun 24/06/19	vie 5/07/19
Afinamiento	20 días	lun 8/07/19	vie 2/08/19

Imagen 8-2 Cronograma de ejecución estimado

8.1.3 COSTOS

Costos de personal			
Personal involucrado	**Horas**	**Costo por hora (USD)**	**Costo total**
Ingeniero de operaciones	180	$ 20	$ 3.600
Consultor de seguridad	72	$ 35	$ 2.520
Director de operaciones	36	$ 60	$ 2.160
Costos de infraestructura/software/licencias			
Ítem	**Unidades**	**Costo unitario (USD)**	**Costo total**
Licencias DLP	30	$ 20	$ 600
Servidor	1	$ 2.000	$ 2.000
Costo total estimado			$ 10.880

8.2 IMPLEMENTACIÓN DE PROCEDIMIENTOS DE GESTIÓN DE ACCESO LÓGICO A LA RED, SISTEMAS Y APLICACIONES

8.2.1 OBJETIVO

Desarrollar e implementar los procedimientos relacionados con la gestión de acceso lógico por parte de los usuarios a la red de la organización, sus sistemas operativos y las aplicaciones que se utilizan en el marco de la ejecución del proceso. Durante la ejecución del proyecto también se plantea realizar los ajustes necesarios a las políticas del Directorio Activo de la organización, así como los cambios en las aplicaciones para facilitar su integración con el Directorio y en el Firewall para implementar las políticas de control de acceso a la red.

8.2.2 CRONOGRAMA

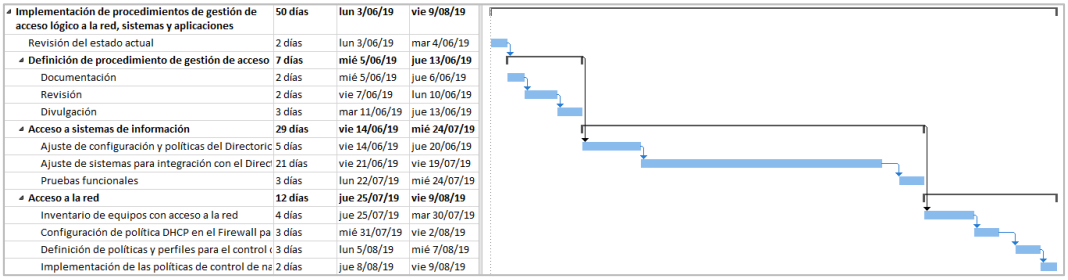


Imagen 8-3 Cronograma de ejecución estimado

8.2.3 COSTOS

Costos de personal			
Personal involucrado	**Horas**	**Costo por hora (USD)**	**Costo total**
Consultor de seguridad	40	$ 35	$ 1.400
Gerente de SOC	20	$ 45	$ 900
Director de operaciones	16	$ 60	$ 960
Desarrollador externo	192	$ 30	$ 5.760
Costos de infraestructura/software/licencias			
Ítem	**Unidades**	**Costo unitario (USD)**	**Costo total**
Licencias AD	1	$ 500	$ 500
Licencias UTM	1	$ 800	$ 800
Costo total estimado			$ 10.320

8.3 IMPLEMENTACIÓN DE PROCEDIMIENTO DE GESTIÓN DE CAMBIOS

8.3.1 OBJETIVO

Diseñar e implementar un procedimiento que permita administrar los cambios que se realizar en la infraestructura tecnológica y lo sistemas de la organización que soportan la ejecución de los procesos incluidos en el alcance del SGSI. Dentro del procedimiento de gestión de cambios es fundamental poder identificar aquellos tipos de cambio que pueden llegar a afectar la confidencialidad, integridad o disponibilidad de la información, de forma que se tomen las acciones necesarias para mitigar un potencial impacto en caso de fallas o errores durante la implementación de los cambios.

8.3.2 CRONOGRAMA

Implementación de procedimiento de gestión de cambios	**13 días**	**lun 12/08/19**	**mié 28/08/19**
Definición las políticas de gestión de cambios	**6 días**	**lun 12/08/19**	**lun 19/08/19**
Documentación	2 días	lun 12/08/19	mar 13/08/19
Revisión	1 día	mié 14/08/19	mié 14/08/19
Divulgación	3 días	jue 15/08/19	lun 19/08/19
Definición el procedimiento para la ejecución de c	**6 días**	**mar 20/08/19**	**mar 27/08/19**
Documentación	2 días	mar 20/08/19	mié 21/08/19
Revisión	1 día	jue 22/08/19	jue 22/08/19
Divulgación	3 días	vie 23/08/19	mar 27/08/19
Establecimiento el comité de control de cambios	1 día	mié 28/08/19	mié 28/08/19

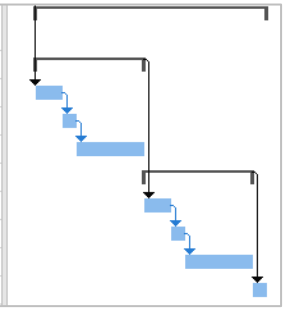


Imagen 8-4 Cronograma de ejecución estimado

8.3.3 COSTOS

Costos de personal			
Personal involucrado	**Horas**	**Costo por hora (USD)**	**Costo total**
Consultor de seguridad	32	$ 35	$ 1.120
Gerente de SOC	12	$ 45	$ 540
Director de operaciones	4	$ 60	$ 240
Director general	4	$ 110	$ 440
Costos de infraestructura/software/licencias			
Ítem	**Unidades**	**Costo unitario (USD)**	**Costo total**
	0	$ 0	$ 0
	0	$ 0	$ 0
Costo total estimado			$ 2.340

8.4 IMPLEMENTACIÓN DE ESTRATEGIA DE GESTIÓN DE VULNERABILIDADES TÉCNICAS

8.4.1 OBJETIVO

Establecer un procedimiento adecuado para la gestión de vulnerabilidades técnicas, de manera que se identifiquen oportunamente, se comuniquen a los responsables de su mitigación y a los propietarios de los activos de información que podrían verse afectados en caso de que alguna de estas vulnerabilidades fuera aprovechada por un atacante para afectar la confidencialidad, integridad o disponibilidad de la información. Dentro de la implementación de esta estrategia se considera la adquisición de una herramienta especializada en la identificación y análisis de vulnerabilidades informáticas.

8.4.2 CRONOGRAMA

Implementación de estrategia de gestión de vulnerabilidades técnicas	**90 días**	**lun 12/08/19**	**vie 13/12/19**
Definición del procedimiento a seguir	**7 días**	**lun 12/08/19**	**mar 20/08/19**
Documentación	2 días	lun 12/08/19	mar 13/08/19
Revisión	2 días	mié 14/08/19	jue 15/08/19
Divulgación	3 días	vie 16/08/19	mar 20/08/19
Adquisición de software de gestión de vulnerabilic	**15 días**	**mié 21/08/19**	**mar 10/09/19**
Definición de requerimientos para el software	2 días	mié 21/08/19	jue 22/08/19
Recepción de propuestas	5 días	vie 23/08/19	jue 29/08/19
Pruebas de concepto	3 días	vie 30/08/19	mar 3/09/19
Selección de solución a instalar	2 días	mié 4/09/19	jue 5/09/19
Instalación	3 días	vie 6/09/19	mar 10/09/19
Ejecución de pruebas	8 días	mié 11/09/19	vie 20/09/19
Remediación de vulnerabilidades críticas	60 días	lun 23/09/19	vie 13/12/19

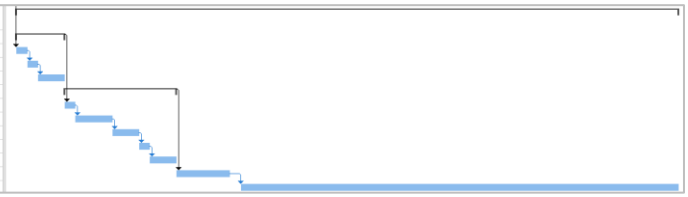


Imagen 8-5 Cronograma de ejecución estimado

8.4.3 COSTOS

Costos de personal			
Personal involucrado	**Horas**	**Costo por hora (USD)**	**Costo total**
Consultor de seguridad	128	$ 35	$ 4.480
Director de operaciones	72	$ 60	$ 4.320
Ingeniero de remediación (externo)	160	$ 25	$ 4.000
Costos de infraestructura/software/licencias			
Ítem	**Unidades**	**Costo unitario (USD)**	**Costo total**
Escáner de vulnerabilidades	1	$ 2.500	$ 2.500
Cambio de infraestructura obsoleta	1	$ 3.000	$ 3.000
Costo total estimado			$ 18.300

8.5 PLAN DE SENSIBILIZACIÓN Y CAPACITACIÓN

8.5.1 OBJETIVO

Crear un plan de sensibilización y capacitación a través del cual se socialicen las políticas de seguridad de la organización y se sensibilice a los empleados con respecto a la importancia de la protección de la información. En el plan se consideran aspectos generales como: buenas prácticas a seguir en el manejo de la información, amenazas más relevantes identificadas en el análisis de riesgo, controles de seguridad que deben ser adoptados y la gestión de incidentes de seguridad. También se contempla la inclusión de capacitación formal en temas especializados para el personal que está involucrado directamente en la operación del SGSI.

8.5.2 CRONOGRAMA

Plan de Sensibilización y capacitación	48 días	lun 3/06/19	mié 7/08/19
Definición de temas a incluir	1 día	lun 3/06/19	lun 3/06/19
Definición de grupos objetivo	1 día	mar 4/06/19	mar 4/06/19
Diseño del material de capacitación	5 días	mié 5/06/19	mar 11/06/19
Revisión y ajustes	3 días	mié 12/06/19	vie 14/06/19
Invitación a los participantes	8 días	lun 17/06/19	mié 26/06/19
Ejecución de las actividades de sensibilización y ca	30 días	jue 27/06/19	mié 7/08/19

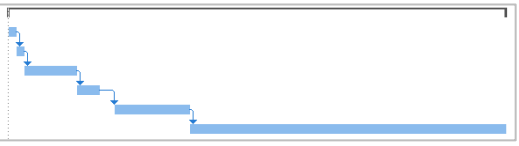


Imagen 8-6 Cronograma de ejecución estimado

8.5.3 COSTOS

Costos de personal			
Personal involucrado	**Horas**	**Costo por hora (USD)**	**Costo total**
Consultor de seguridad	96	$ 35	$ 3.360
Director de operaciones	24	$ 60	$ 1.440
Director general	4	$ 110	$ 440
Costos de infraestructura/software/licencias			
Ítem	**Unidades**	**Costo unitario (USD)**	**Costo total**
Curso auditor ISO27001	1	$ 1.200	$ 1.200
Curso gestión de incidentes	1	$ 700	$ 700
Costo total estimado			$ 7.140

8.6 IMPLEMENTACIÓN DE ESTRATEGIA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

8.6.1 OBJETIVO

Definir la estrategia general y los procedimientos a seguir para el respaldo de la información. Estos procedimientos dictan la forma en la cual se realizan operativamente las copias de respaldo, pero se definen también aspectos generales como los tiempos de retención de las copias, el tipo de copia a realizar (completa, diferencia e incremental), la ubicación de la copia, los mecanismos de protección de su confidencialidad, integridad y disponibilidad, las responsabilidades con respecto a la verificación de la ejecución de las copias, la custodia y las pruebas de restauración. Los procedimientos se dividen en aquellos orientados a la copia de información en servidores y en otros orientados al respaldo de la información en equipos de usuario final.

8.6.2 CRONOGRAMA

Implementación de estrategia de copias de respaldo de la información	**21 días**	**lun 16/12/19**	**lun 13/01/20**
Definición de la política de copias de respaldo	**7 días**	**lun 16/12/19**	**mar 24/12/19**
Documentación	2 días	lun 16/12/19	mar 17/12/19
Revisión	2 días	mié 18/12/19	jue 19/12/19
Divulgación	3 días	vie 20/12/19	mar 24/12/19
Definición del procedimiento a seguir (Servidores)	**7 días**	**mié 25/12/19**	**jue 2/01/20**
Documentación	2 días	mié 25/12/19	jue 26/12/19
Revisión	2 días	vie 27/12/19	lun 30/12/19
Divulgación	3 días	mar 31/12/19	jue 2/01/20
Definición del procedimiento a seguir (PC)	**7 días**	**vie 3/01/20**	**lun 13/01/20**
Documentación	2 días	vie 3/01/20	lun 6/01/20
Revisión	2 días	mar 7/01/20	mié 8/01/20
Divulgación	3 días	jue 9/01/20	lun 13/01/20

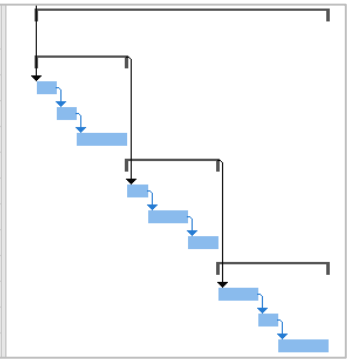


Imagen 8-7 Cronograma de ejecución estimado

8.6.3 COSTOS

Costos de personal			
Personal involucrado	**Horas**	**Costo por hora (USD)**	**Costo total**
Consultor de seguridad	48	$ 35	$ 1.680
Gerente de SOC	36	$ 45	$ 1.620
Director de operaciones	12	$ 60	$ 720
Director general	4	$ 110	$ 440
Costos de infraestructura/software/licencias			
Ítem	**Unidades**	**Costo unitario (USD)**	**Costo total**
	0	$ 0	$ 0
	0	$ 0	$ 0
Costo total estimado			$ 4.460

8.7 IMPLEMENTACIÓN DE PROCEDIMIENTO DE SELECCIÓN DE PERSONAL PARA ACTIVIDADES CRÍTICAS

8.7.1 OBJETIVO

Actualizar y documentar el procedimiento de selección de personal existente con el fin de contemplar controles específicos de seguridad para el caso de la contratación de empleados

que tendrán acceso a información de alta sensibilidad de la organización y sus clientes. Algunos de los controles adicionales que se contemplan son: Visita domiciliaria, verificación de antecedentes, pruebas de polígrafo y pruebas técnicas específicas. Estos controles se suman a aquellos ya contemplados en el procedimiento como la validación de las referencias personales, laborales, los exámenes de aptitud médica y la entrevista. Adicionalmente, se ajustarán las descripciones de cargo y los acuerdos de confidencialidad.

8.7.2 CRONOGRAMA

Implementación de procedimiento de selección de personal para actividades críticas	19 días	lun 12/08/19	jue 5/09/19
Revisión y ajustar el procedimiento de selección de	4 días	lun 12/08/19	jue 15/08/19
Definición los cargos de actividades críticas	1 día	vie 16/08/19	vie 16/08/19
Definición los componentes del estudio de seguric	1 día	lun 19/08/19	lun 19/08/19
Revisión y ajustar el acuerdo de confidencialidad	5 días	mar 20/08/19	lun 26/08/19
Revisión y ajustar las descripciones de cargo existe	5 días	mar 27/08/19	lun 2/09/19
Divulgación del procedimiento y las responsabilida	3 días	mar 3/09/19	jue 5/09/19

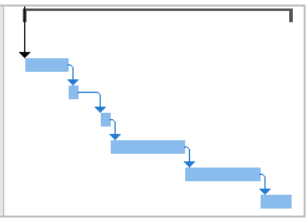


Imagen 8-8 Cronograma de ejecución estimado

8.7.3 COSTOS

Costos de personal			
Personal involucrado	**Horas**	**Costo por hora (USD)**	**Costo total**
Consultor de seguridad	32	$ 35	$ 1.120
Director Administrativo	96	$ 60	$ 5.760
Director de operaciones	28	$ 60	$ 1.680
Director general	4	$ 110	$ 440
Costos de infraestructura/software/licencias			
Ítem	**Unidades**	**Costo unitario (USD)**	**Costo total**
	0	$ 0	$ 0
	0	$ 0	$ 0
Costo total estimado			$ 9.000

8.8 FORTALECIMIENTO DE PROTECCIÓN CONTRA AMENAZAS FÍSICAS Y AMBIENTALES

8.8.1 OBJETIVO

Evaluar y mejorar las condiciones de protección física con las que cuenta la organización en la actualidad, con el fin de mitigar los riesgos identificados en relación con posibles afectaciones a la confidencialidad, integridad o disponibilidad de la información causadas por amenazas de origen físico. Los aspectos fundamentales son el control de acceso físico y la protección contra amenazas medioambientales (como los incendios o las inundaciones), incluyendo los posibles desastres de origen industrial.

8.8.2 CRONOGRAMA

Fortalecimiento de protección contra amenazas físicas y ambientales	**31 días**	**mar 14/01/20**	**mar 25/02/20**
Definición de la política de acceso físico	**7 días**	**mar 14/01/20**	**mié 22/01/20**
Documentación	2 días	mar 14/01/20	mié 15/01/20
Revisión	2 días	jue 16/01/20	vie 17/01/20
Divulgación	3 días	lun 20/01/20	mié 22/01/20
Revisión de los perímetros de seguridad física y sus	4 días	jue 23/01/20	mar 28/01/20
Implementar los libros de registro de acceso a la of	1 día	mié 29/01/20	mié 29/01/20
Adquisición de un sistema de extinción de incendi	**19 días**	**jue 30/01/20**	**mar 25/02/20**
Definición de requerimientos	1 día	jue 30/01/20	jue 30/01/20
Recepción de propuestas	5 días	vie 31/01/20	jue 6/02/20
Selección de solución a instalar	3 días	vie 7/02/20	mar 11/02/20
Instalación	10 días	mié 12/02/20	mar 25/02/20

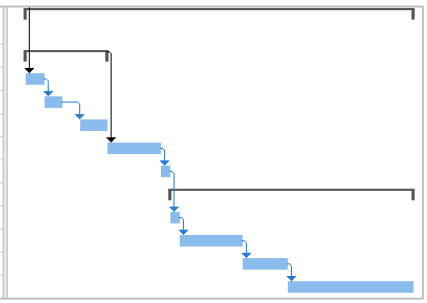


Imagen 8-9 Cronograma de ejecución estimado

8.8.3 COSTOS

Costos de personal			
Personal involucrado	**Horas**	**Costo por hora (USD)**	**Costo total**
Consultor de seguridad	33,6	$ 35	$ 1.176
Director Administrativo	61,6	$ 60	$ 3.696
Director de operaciones	37,6	$ 60	$ 2.256
Director general	8	$ 110	$ 880
Costos de infraestructura/software/licencias			
Ítem	**Unidades**	**Costo unitario (USD)**	**Costo total**
Sistema de protección contra incendios	1	$ 4.500	$ 4.500
Instalación y servicios	1	$ 7.000	$ 7.000
Costo total estimado			$ 19.508

8.9 PLAN DE MANTENIMIENTO Y ACTUALIZACIÓN

8.9.1 OBJETIVO

Establecer un plan de mantenimiento y actualización para la infraestructura y los sistemas de información de la organización, de manera que se cuente con una estrategia para mantenerlos en un estado óptimo de actualización y tomar las acciones de mantenimiento preventivo y correctivo necesarias. Se contempla en este proyecto la revisión y actualización de los contratos de soporte y garantía con los fabricantes.

8.9.2 CRONOGRAMA

Plan de mantenimiento y actualización	**18 días**	**mié 26/02/20**	**vie 20/03/20**
Definición del alcance del plan	1 día	mié 26/02/20	mié 26/02/20
Documentación	5 días	jue 27/02/20	mié 4/03/20
Revisión	3 días	jue 5/03/20	lun 9/03/20
Divulgación	1 día	mar 10/03/20	mar 10/03/20
Revisión y actualización de contratos de soporte y g	5 días	mié 11/03/20	mar 17/03/20
Diagnóstico del estado actual del software y hardw	3 días	mié 18/03/20	vie 20/03/20

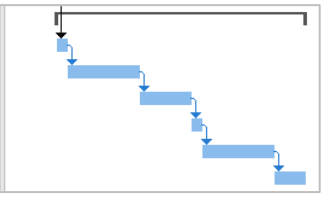


Imagen 8-10 Cronograma de ejecución estimado

8.9.3 COSTOS

Costos de personal			
Personal involucrado	**Horas**	**Costo por hora (USD)**	**Costo total**

Director de operaciones	14,4	$ 60	$ 864
Ingeniero de soporte	100,8	$ 25	$ 2.520
Costos de infraestructura/software/licencias			
Ítem	**Unidades**	**Costo unitario (USD)**	**Costo total**
Contratos de soporte	4	$ 1.000	$ 4.000
Costo total estimado			$ 7.384

8.10 IMPLEMENTACIÓN DE CIFRADO DE INFORMACIÓN CONFIDENCIAL

8.10.1 OBJETIVO

Seleccionar e implementar la tecnología más apropiada para realizar el cifrado de discos en los equipos de usuario final, cifrado de información confidencial, dispositivos móviles y medios extraíbles. Este proyecto permite proteger la información confidencial de la organización y los clientes frente a la divulgación accidental o intencionada. Se contempla en el proyecto la selección de la tecnología a implementar y su posterior despliegue, en el cual se deben tomar todas las precauciones para evitar la pérdida de información durante el proceso de cifrado y se debe diseñar una estrategia adecuada para la gestión de llaves de cifrado de manera que se proteja no solo la confidencialidad sino la disponibilidad de la información.

8.10.2 CRONOGRAMA

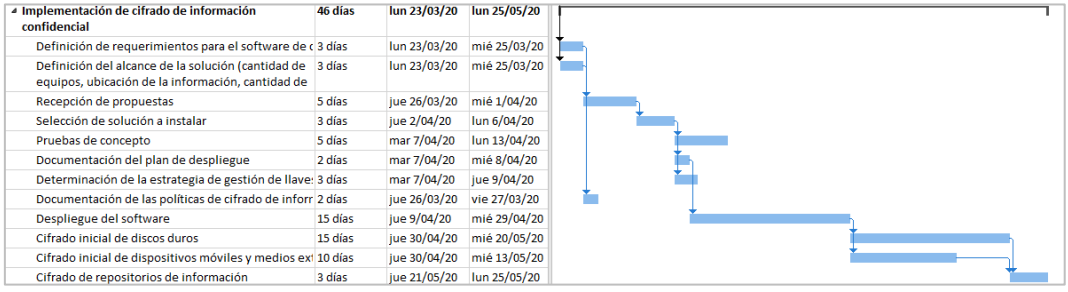


Imagen 8-11 Cronograma de ejecución estimado

8.10.3 COSTOS

Costos de personal			
Personal involucrado	**Horas**	**Costo por hora (USD)**	**Costo total**
Consultor de seguridad	73,6	$ 35	$ 2.576
Director Administrativo	18,4	$ 60	$ 1.104
Director de operaciones	18,4	$ 60	$ 1.104
Director general	8	$ 110	$ 880
Ingeniero de soporte	240,8	$ 25	$ 6.020
Costos de infraestructura/software/licencias			
Ítem	**Unidades**	**Costo unitario (USD)**	**Costo total**
Software de cifrado	1	$ 1.500	$ 1.500
Servicio de implementación	1	$ 3.000	$ 3.000
Costo total estimado			$ 16.184

8.11 IMPLEMENTACIÓN DE MONITOREO Y PROTECCIÓN DE LA RED CORPORATIVA

8.11.1 OBJETIVO

Adquirir, desplegar y configurar dos herramientas tecnológicas orientadas a optimizar el monitoreo de la red, con el fin de detectar posibles incidentes de seguridad de la información relacionados con las comunicaciones en la red. Las herramientas seleccionadas para ser implementadas en el proyecto son: un IDS y un SIEM, el primero permite monitorizar la red frente a posibles ataques informáticos o intentos de explotación de vulnerabilidades y el segundo permite correlacionar los eventos de seguridad de múltiples plataformas con el fin de identificar actividades sospechosas en el entorno de la red.

8.11.2 CRONOGRAMA

Implementación de monitoreo y protección de la red corporativa	**63 días**	**mar 26/05/20**	**jue 20/08/20**
Implementación SIEM	**39 días**	**mar 26/05/20**	**vie 17/07/20**
Definición de requerimientos software de moni	1 día	mar 26/05/20	mar 26/05/20
Recepción de propuestas	5 días	mié 27/05/20	mar 2/06/20
Selección de solución a instalar	3 días	mié 3/06/20	vie 5/06/20
Instalación	5 días	lun 8/06/20	vie 12/06/20
Configuración de fuentes de información	10 días	lun 15/06/20	vie 26/06/20
Diseño de las reglas de correlación	15 días	lun 29/06/20	vie 17/07/20
Implementación IDS	**24 días**	**lun 20/07/20**	**jue 20/08/20**
Definición de requerimientos software de moni	1 día	lun 20/07/20	lun 20/07/20
Recepción de propuestas	5 días	mar 21/07/20	lun 27/07/20
Selección de solución a instalar	3 días	mar 28/07/20	jue 30/07/20
Instalación	5 días	vie 31/07/20	jue 6/08/20
Diseño de las reglas de IDS	10 días	vie 7/08/20	jue 20/08/20

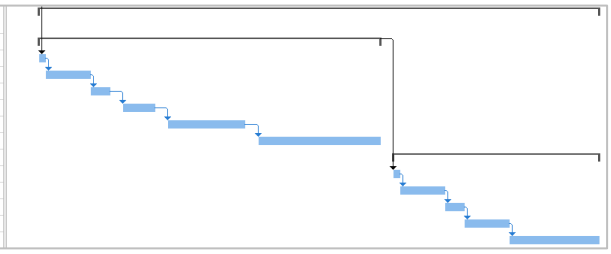


Imagen 8-12 Cronograma de ejecución estimado

8.11.3 COSTOS

Costos de personal			
Personal involucrado	**Horas**	**Costo por hora (USD)**	**Costo total**
Consultor de seguridad	100,8	$ 35	$ 3.528
Director de operaciones	25,2	$ 60	$ 1.512
Ingeniero de soporte	352,8	$ 25	$ 8.820
Costos de infraestructura/software/licencias			
Ítem	**Unidades**	**Costo unitario (USD)**	**Costo total**
Licencia de IDS	1	$ 2.300	$ 2.300
Licencia de SIEM	1	$ 1.800	$ 1.800
Servicio de implementación	1	$ 1.200	$ 1.200
Costo total estimado			$ 19.160

8.12 PLANES DE CONTINGENCIA

8.12.1 OBJETIVO

Diseñar y documentar los planes de contingencia que permitan a la organización, y específicamente a los procesos críticos, contar con protocolos precisos y documentados para atender emergencias que pongan en riesgo la continuidad de los servicios que se prestan. Durante el proyecto se ha planteado la identificación de actividades, información e infraestructura críticas para mantener la disponibilidad de los procesos. Así mismo, se identificarán los tiempos RTO y RPO para que los planes de contingencia estén alineados con los tiempos máximos de indisponibilidad permitidos y los planes de respaldo estén alineados con la cantidad de información cuya pérdida es tolerable.

8.12.2 CRONOGRAMA

Planes de contingencia	19 días	vie 21/08/20	mié 16/09/20
Identificación de las actividades críticas de los proc	2 días	vie 21/08/20	lun 24/08/20
Identificación de la infraestructura crítica	2 días	mar 25/08/20	mié 26/08/20
Identificación de información y servicios críticos pa	2 días	jue 27/08/20	vie 28/08/20
Identificación de los indicadores RTO y RPO	3 días	lun 31/08/20	mié 2/09/20
Documentación de los planes	5 días	jue 3/09/20	mié 9/09/20
Pruebas de los planes	5 días	jue 10/09/20	mié 16/09/20

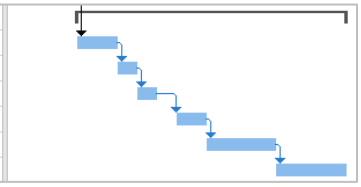


Imagen 8-13 Cronograma de ejecución estimado

8.12.3 COSTOS

Costos de personal			
Personal involucrado	**Horas**	**Costo por hora (USD)**	**Costo total**
Consultor de seguridad	76	$ 35	$ 2.660
Director de operaciones	45,6	$ 60	$ 2.736
Director administrativo	30,4	$ 60	$ 1.824
Director general	15,2	$ 110	$ 1.672
Ingeniero de soporte	106,4	$ 25	$ 2.660
Costos de infraestructura/software/licencias			
Ítem	**Unidades**	**Costo unitario (USD)**	**Costo total**
		$ 0	$ 0
		$ 0	$ 0
		$ 0	$ 0
Costo total estimado			$ 11.552

8.13 HACKING ÉTICO E INGENIERÍA SOCIAL

8.13.1 OBJETIVO

Contratar un proveedor experto en la ejecución de pruebas de hacking ético e ingeniería social, con el fin de realizar un ejercicio para identificar las vulnerabilidades presentes en la infraestructura tecnológica y su impacto real en caso de ser explotadas. Así mismo, se pretende identificar el grado de sensibilización por parte de los empleados de la organización frente a amenazas como la ingeniería social a través de la ejecución de pruebas de simulación de ataques de este tipo.

8.13.2 CRONOGRAMA

Hacking ético e ingeniería social	36 días	jue 17/09/20	jue 5/11/20
Establecer el alcance de las pruebas	1 día	jue 17/09/20	jue 17/09/20
Definir los requerimientos técnicos para las pruebas	1 día	vie 18/09/20	vie 18/09/20
Recibir las ofertas de servicio	5 días	lun 21/09/20	vie 25/09/20
Seleccionar al proveedor	3 días	lun 28/09/20	mié 30/09/20
Desarrollar la planeación de las pruebas	4 días	jue 1/10/20	mar 6/10/20
Ejecutar las pruebas	5 días	mié 7/10/20	mar 13/10/20
Presentar los resultados obtenidos	2 días	mié 14/10/20	jue 15/10/20
Remediar las vulnerabilidades explotadas	15 días	vie 16/10/20	jue 5/11/20

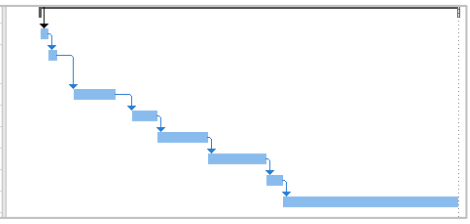


Imagen 8-14 Cronograma de ejecución estimado

8.13.3 COSTOS

Costos de personal			
Personal involucrado	**Horas**	**Costo por hora (USD)**	**Costo total**
Consultor de seguridad	72	$ 35	$ 2.520

Director de operaciones	14,4	$ 60	$ 864
Director general	4	$ 110	$ 440
Costos de infraestructura/software/licencias			
Ítem	**Unidades**	**Costo unitario (USD)**	**Costo total**
Consultoría de pruebas de hacking ético e ingeniería social	1	$ 5.000	$ 5.000
		$ 0	$ 0
		$ 0	$ 0
Costo total estimado			$ 8.824

9 IMPACTO DE LOS PROYECTOS SOBRE LA SEGURIDAD

9.1 MADUREZ DE LOS CONTROLES DE SEGURIDAD

En el documento Anexo 5 - *Análisis diferencial (Después de proyectos).xlsx* se realizó la estimación del avance con respecto al nivel de madurez de los controles de seguridad después de la ejecución de los proyectos. Para esto se generó un cruce entre los proyectos y los controles que apoyarán su ejecución como se presenta en la siguiente tabla:

Proyecto	Control (ISO 27002:2013)	
Implementación de un sistema de prevención de fuga de información (DLP)	A.6.2.2	Teletrabajo
	A.8.2.2	Etiquetado de la información
	A.8.2.3	Manejo de activos
	A.8.3.1	Gestión de medios removibles
	A.13.2.3	Mensajería electrónica
	A.18.1.4	Privacidad y protección de información de datos personales
Implementación de procedimientos de gestión de acceso lógico a la red, sistemas y aplicaciones	A.9.1.1	Política de control de acceso
	A.9.1.2	Acceso a redes y a servicios en red
	A.9.2.1	Registro y cancelación del registro de usuarios
	A.9.2.2	Suministro de acceso de usuarios
	A.9.2.3	Gestión de derechos de acceso privilegiado
	A.9.2.4	Gestión de información de autenticación secreta de usuarios
	A.9.2.5	Revisión de los derechos de acceso de usuarios
	A.9.2.6	Retiro o ajuste de los derechos de acceso
	A.9.3.1	Uso de información de autenticación secreta
	A.9.4.1	Restricción de acceso a la información
	A.9.4.2	Procedimiento de ingreso seguro
	A.9.4.3	Sistema de gestión de contraseñas
	A.11.2.8	Equipos de usuario desatendido
	A.13.1.1	Controles de redes
	A.13.1.2	Seguridad de los servicios de red

Proyecto	Control (ISO 27002:2013)	
Implementación de procedimiento de gestión de cambios	A.12.1.2	Gestión de cambios
Implementación de estrategia de gestión de vulnerabilidades técnicas	A.12.6.1	Gestión de las vulnerabilidades técnicas
Plan de sensibilización y capacitación	A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información
	A.11.2.9	Política de escritorio limpio y pantalla limpia
	A.16.1.1	Responsabilidades y procedimientos
	A.16.1.2	Reporte de eventos de seguridad de la información
	A.16.1.3	Reporte de debilidades de seguridad de la información
Implementación de estrategia de copias de respaldo de la información	A.12.3.1	Respaldo de la información
Implementación de procedimiento de selección de personal para actividades críticas	A.7.1.1	Selección
	A.7.1.2	Términos y condiciones del empleo
	A.7.2.3	Proceso disciplinario
	A.7.3.1	Terminación o cambio de responsabilidades de empleo
Fortalecimiento de protección contra amenazas físicas y ambientales	A.11.1.1	Perímetro de seguridad física
	A.11.1.2	Controles de acceso físicos
	A.11.1.3	Seguridad de oficinas, recintos e instalaciones
	A.11.1.4	Protección contra amenazas externas y ambientales
	A.11.1.5	Trabajo en áreas seguras
	A.11.1.6	Áreas de despacho y carga
Plan de mantenimiento y actualización	A.11.2.2	Servicios de suministro
	A.11.2.4	Mantenimiento de equipos
	A.11.2.5	Retiro de activos
	A.11.2.7	Disposición segura o reutilización de equipos
	A.12.1.3	Gestión de capacidad
Implementación de cifrado de información confidencial	A.10.1.1	Política sobre el uso de controles criptográficos
	A.10.1.2	Gestión de llaves
	A.18.1.5	Reglamentación de controles criptográficos
	A.8.3.3	Transferencia de medios físicos
Implementación de monitoreo y protección de la red corporativa	A.12.4.1	Registro de eventos
	A.12.4.2	Protección de la información de registro
	A.12.4.3	Registros del administrador y del operador
Planes de contingencia	A.17.1.1	Planificación de la continuidad de la seguridad de la información
	A.17.1.2	Implementación de la continuidad de la seguridad de la información

Proyecto	Control (ISO 27002:2013)	
	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información
Hacking ético e ingeniería social	A.12.6.1	Gestión de las vulnerabilidades técnicas
	A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información
	A.11.2.9	Política de escritorio limpio y pantalla limpia

Tabla 9-1 Controles de seguridad por proyecto

En la siguiente gráfica se resume el impacto de la ejecución de los proyectos en el estado de madurez por dominio de la guía GTC-ISO-IEC 27002:2013, este instrumento se debe actualizar una vez se avance con la implementación de cada proyecto para identificar si se logró el avance esperado.

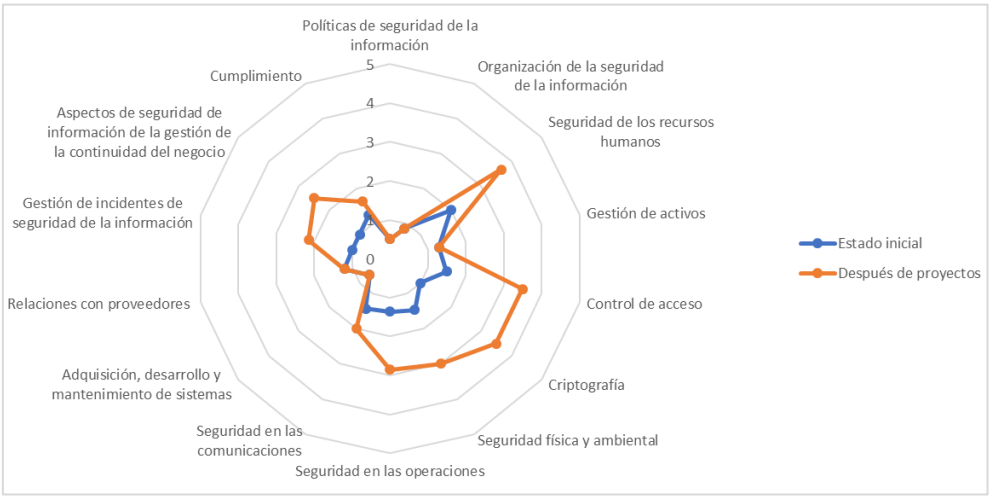


Imagen 9-1 Evolución de la madurez de los controles de seguridad

9.2 RIESGO RESIDUAL

Posterior a la ejecución de los proyectos descritos, se espera una disminución considerable del nivel de riesgo al que está expuesta la organización. Esta estimación se realiza previendo el impacto que tendrán los controles implementados en la probabilidad de ocurrencia de los riesgos identificados. El detalle de este análisis se encuentra en el Anexo 6 - *Matriz de Riesgo Residual.xlsx* y en la siguiente gráfica se presenta el resultado esperado con respecto a la disminución de los 83 escenarios de riesgo con valoración *A: importante* en la evaluación de riesgo inherente.

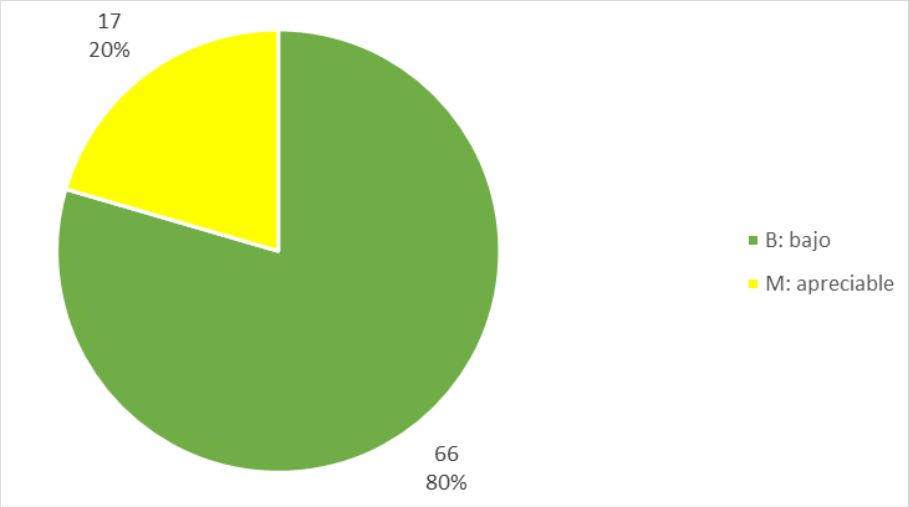


Imagen 9-2 Distribución de los 83 riesgos importantes después de la implementación de los proyectos

De acuerdo con lo anterior es posible estimar el escenario global de riesgos con la nueva distribución después de aplicar los controles. Esta distribución se puede observar detalladamente en la siguiente gráfica.

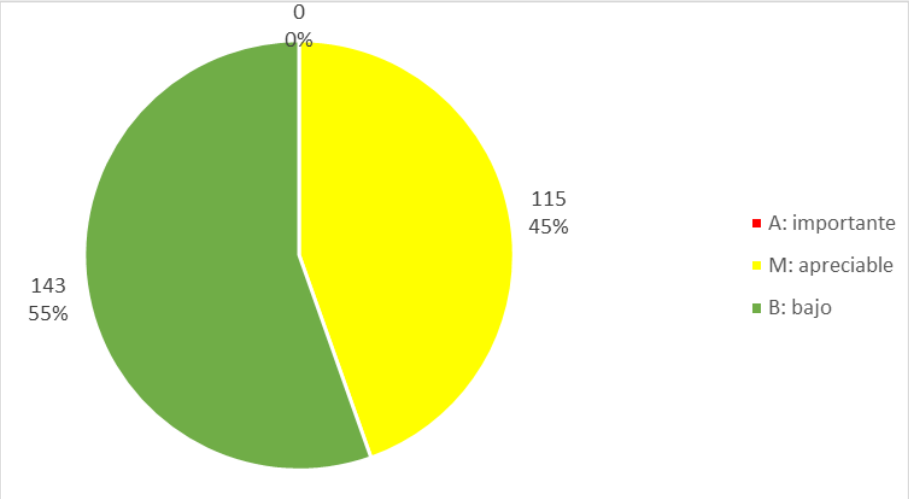


Imagen 9-3 Distribución total de los riesgos residuales

10 AUDITORÍA DE CUMPLIMIENTO

De acuerdo con el procedimiento de auditorías internas definido, se planificó la ejecución de la primera auditoría para la semana del 6 al 10 de mayo de 2019. En este caso, debido a que se trataba de la primera ejecución de la auditoría se seleccionó la totalidad de controles incluidos en la declaración de aplicabilidad para ser contemplados en el ejercicio de auditoría. A continuación, se presenta el contenido del plan de auditoría elaborado:

10.1 PLAN DE AUDITORÍA

Proceso por auditar	Operaciones de seguridad informática. Gestión de proyectos.
Nombre del auditor líder y del equipo auditor (si aplica)	Jorge Correa
Listado de controles que serán incluidos en la auditoría	Se auditará la totalidad de los controles incluidos en la declaración de aplicabilidad
Criterios de la auditoría	Durante la auditoría se identificarán o conformidades mayores, menores y observaciones con respecto a la norma NTC-ISO-IEC 27001:2013, de acuerdo con la siguiente descripción: **No conformidad mayor:** Incumplimiento en relacionar cualquier cláusula de la norma u otros criterios contra los cuales se está realizando la auditoria. (Araque, 2017) **No conformidad menor:** Un único lapso, caso, ocurrencia o falta parcial observada en la aplicación práctica de un procedimiento durante una auditoria. (Araque, 2017) **Observación:** Catalogación interna de las debilidades en el sistema que encuentra el auditor y que no pueden ser soportadas contra la norma y/o contra los documentos definidos en el Sistema. (Araque, 2017)
Fecha, hora y lugar de la auditoría	La auditoría se realizará del 6 al 10 de mayo de 2019 en las instalaciones de Consultora JC S.A.S. iniciando el 6 de mayo a las 10 a.m. y realizando la reunión de cierre el 10 de mayo a las 4 p.m.
Auditado(s) responsable(s)	Director general. Director administrativo y financiero. Director de operaciones. Gerentes de proyecto. Personal del SOC.

10.2 ANÁLISIS DEL NIVEL DE CUMPLIMIENTO DE LOS REQUISITOS

Durante la auditoría se verificó el nivel de implementación de los requisitos de la norma y se agregaron las observaciones correspondientes en cada caso.

SECCIÓN	REQUISITO	ESTADO	OBSERVACIONES
4	Contexto de la organización	Implementado	Se evidencia la documentación del contexto de la organización actualizado, la identificación de necesidades y expectativas de las partes interesadas, el alcance del SGSI y el establecimiento del SGSI. Es necesario definir algún mecanismo para asegurar la revisión y mejora continua de estos elementos

SECCIÓN	REQUISITO	ESTADO	OBSERVACIONES
5	Liderazgo	Implementado	Se ha evidenciado el liderazgo por parte de la alta dirección, la documentación y divulgación de las políticas de seguridad de la información y la definición de roles y responsabilidades. Aún no se ha cerrado el primer ciclo de revisión puesto que recién se implementaron
6	Planificación	Implementado	Se evidencia la existencia de un plan de implementación del Sistema, así como la metodología de riesgos (diseñada de acuerdo con lo exigido en el requisito). Con base en esto se evidencia la existencia de objetivos de seguridad medibles y concretos y su plan de implementación
7	Soporte	Implementado	Se evidencia la disposición de recursos para la operación del Sistema, incluyendo una persona 100% dedicada a la operación del sistema, el apoyo de todas las áreas dentro del alcance del Sistema, la sensibilización de todo el personal en relación a su rol con respecto a la seguridad y la disposición adecuada de la información documentada necesaria
8	Operación	Implementado	Se ha evidenciado el funcionamiento del procedimiento de gestión de riesgos y la existencia de planes concretos de tratamiento de los riesgos identificados. Aún no se ha cerrado la primera ejecución del procedimiento de gestión de riesgos, se encuentra en fase de tratamiento
9	Evaluación del desempeño	Implementado	Se evidencia la definición de indicadores para evaluar el desempeño del sistema, así mismo se han definido estrategias de monitoreo para el seguimiento del cumplimiento de los objetivos definidos y la revisión en conjunto con la alta dirección para tomar las medidas necesarias para mantener un desempeño adecuado. Se cuenta con un procedimiento de auditoría y se ha realizado el primer ejercicio de auditoría interna
10	Mejora	Implementado	Se ha evidenciado la existencia de procedimientos de revisión y atención de las no conformidades, aunque debido a que no se ha culminado el primer ciclo de ejecución de Sistema no se evidencia la documentación aún de acciones correctivas. Se espera que al culminar la auditoría interna se puedan documentar acciones pertinentes para atender los hallazgos

10.3 ANÁLISIS DEL NIVEL DE MADUREZ DE LOS CONTROLES DE SEGURIDAD

La revisión de los 114 controles del anexo A de la norma NTC-ISO-IEC 27001:2013 se realizó de acuerdo con la siguiente tabla, la cual está basada en el modelo de madurez de la capacidad (CMM):

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	L0	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
10%	L1	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	L2	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	L3	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	L4	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	L5	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

En la siguiente tabla se presenta el resultado de la revisión de los 114 controles de seguridad.

Referencia Anexo A	Control	Efectividad	Estado	Observación
A.5	Políticas de seguridad de la información			
A5.1	Dirección de Gestión de Seguridad de la Información			
A.5.1.1	Políticas de seguridad de la información	L3 - Proceso definido	En cumplimiento	Las políticas se han definido y se ha iniciado su proceso de comunicación por los procesos de negocio
A.5.1.2	Revisión de las políticas de seguridad de la información	L3 - Proceso definido	En cumplimiento	La primera versión de las políticas de seguridad se ha revisado por parte de la alta dirección
A.6	Organización de la seguridad de la información			
A.6.1	Organización interna			
A.6.1.1	Roles y responsabilidades en seguridad de la información	L2 - Reproducible, pero intuitivo	Observación	Existen algunos roles y responsabilidades establecidos, pero en su mayoría los procesos dependen del compromiso de cada involucrado

Referencia Anexo A	Control	Efectividad	Estado	Observación
A.6.1.2	Segregación de funciones	L2 - Reproducible, pero intuitivo	Observación	No se ha documentado formalmente la separación de las funciones en los procesos críticos, algunas tareas críticas sí se realizan por parte de diferente personal, aunque no en todos los casos
A.6.1.3	Contacto con autoridades	L2 - Reproducible, pero intuitivo	Observación	El contacto con las autoridades no se encuentra formalmente definido, aunque sí la responsabilidad de realizarlo
A.6.1.4	Contacto con grupos de interés especial	L2 - Reproducible, pero intuitivo	Observación	El contacto con grupos de interés no se encuentra formalmente definido, aunque sí la responsabilidad de realizarlo
A.6.1.5	Seguridad de la información en la gestión de proyectos	L3 - Proceso definido	En cumplimiento	Se cuenta con un proceso formal de gestión de proyectos en el cual se contemplan los requisitos de seguridad de la información
A.6.2	Dispositivos móviles y teletrabajo			
A.6.2.1	Política de dispositivos móviles	L3 - Proceso definido	En cumplimiento	Se cuenta con una política formalmente definida para la gestión de dispositivos móviles
A.6.2.2	Teletrabajo	L3 - Proceso definido	En cumplimiento	Se cuenta con una política formalmente definida para el teletrabajo
A.7	Seguridad de los recursos humanos			
A.7.1	Antes del empleo			
A.7.1.1	Selección	L3 - Proceso definido	En cumplimiento	Se cuenta con un procedimiento formalmente definido para la selección de personal donde se contemplan los aspectos de seguridad de la información
A.7.1.2	Términos y condiciones del empleo	L3 - Proceso definido	En cumplimiento	A nivel contractual se han definido los términos y condiciones del empleo y los aspectos de seguridad de la información más relevantes
A.7.2	Durante el empleo			
A.7.2.1	Responsabilidades de la Alta Dirección	L4 - Gestionado y medible	En cumplimiento	Se ha establecido la responsabilidad de la alta dirección en relación con el liderazgo en la gestión de seguridad de la información, se evidencia la realización de reuniones de seguimiento y sensibilización por parte de la ata dirección
A.7.2.2	Concientización, educación y formación en seguridad de la información	L3 - Proceso definido	En cumplimiento	Se cuenta con un programa de capacitación y sensibilización para todo el personal de la empresa

Referencia Anexo A	Control	Efectividad	Estado	Observación
A.7.2.3	Proceso disciplinario	L3 - Proceso definido	En cumplimiento	Se cuenta con un proceso disciplinario documentado y acorde con los requisitos legales, en el cual se contemplan las faltas relacionadas con la protección de la información
A.7.3	Terminación y cambio de empleo			
A.7.3.1	Terminación o cambio de responsabilidades de empleo	L3 - Proceso definido	En cumplimiento	El proceso de recursos humanos contempla las medidas de seguridad para la terminación o cambio de empleo. Sin embargo, no se cuenta con evidencia de su medición o mejora
A.8	Gestión de activos			
A.8.1	Responsabilidad de activos			
A.8.1.1	Inventario de activos	L3 - Proceso definido	En cumplimiento	Se ha documentado un inventario de activos, sin embargo, no se cuenta con un procedimiento que evidencie la actualización constante del inventario
A.8.1.2	Propiedad de activos	L4 - Gestionado y medible	En cumplimiento	La responsabilidad con respecto a los activos de información se encuentra documentada, y se cuenta con evidencia con respecto al conocimiento de los propietarios y su responsabilidad con respecto a la protección de la información
A.8.1.3	Uso aceptable de activos	L3 - Proceso definido	En cumplimiento	Se cuenta con una política de uso aceptable de los activos, la cual ha sido divulgada a todo el personal de la empresa
A.8.1.4	Devolución de activos	L3 - Proceso definido	En cumplimiento	En la política de uso aceptable de los activos se contempla lo relacionado con la devolución de los activos de información
A.8.2	Clasificación de información			
A.8.2.1	Clasificación de información	L3 - Proceso definido	En cumplimiento	Se cuenta con una política y un procedimiento de clasificación de información. No se evidencia la medición del control ni su mejora continua a través del tiempo
A.8.2.2	Etiquetado de información	L2 - Reproducible, pero intuitivo	No conformidad menor	No se evidencia la presencia de un control documentado, bien sea manual o automático para el etiquetado de la información. Se menciona en la política de clasificación de información, ciertos documentos lo tienen
A.8.2.3	Manejo de activos	L1 - Inicial/Ad-hoc	No conformidad menor	No se evidencian prácticas o procedimientos para el manejo de los activos
A.8.3	Manipulación medios			

Referencia Anexo A	Control	Efectividad	Estado	Observación
A.8.3.1	Gestión de medios removibles	L1 - Inicial/Ad-hoc	No conformidad menor	No se evidencian prácticas o procedimientos para la gestión segura de los medios removibles
A.8.3.2	Eliminación de medios	L2 - Reproducible, pero intuitivo	No conformidad menor	La eliminación de los medios no sigue prácticas documentadas y aunque se ejecuta, depende del personal a cargo que se lleve a cabo
A.8.3.3	Transferencia de medios físicos	L1 - Inicial/Ad-hoc	No conformidad menor	No se evidencian prácticas o procedimientos para la transferencia segura de los medios físicos
A.9	Control de acceso			
A.9.1	Requerimientos de control de acceso del negocio			
A.9.1.1	Política de control de acceso	L3 - Proceso definido	En cumplimiento	Se cuenta con una política de control de acceso lógico y físico documentada que ha sido divulgada a todo el personal de la empresa, de lo cual se tiene evidencia
A.9.1.2	Acceso a redes y servicios de red	L3 - Proceso definido	En cumplimiento	Se cuenta con un procedimiento para el control de acceso a la red y la habilitación de acceso a servicios. Adicionalmente se cuenta con controles técnicos para asegurar que no existan dispositivos con acceso no autorizado. Sin embargo, no se evidencia la revisión o seguimiento sobre los accesos otorgados
A.9.2	Administración de acceso de usuarios			
A.9.2.1	Registro y cancelación de registro del usuario	L2 - Reproducible, pero intuitivo	Observación	No se evidencia la existencia de un proceso para la gestión de usuarios y asignación de contraseñas en los sistemas. Se siguen buenas prácticas, pero se depende enteramente del personal a cargo del acceso a los sistemas
A.9.2.2	Aprovisionamiento de acceso del usuario	L2 - Reproducible, pero intuitivo	Observación	No se evidencia la existencia de un proceso para la gestión de usuarios y asignación de contraseñas en los sistemas. Se siguen buenas prácticas, pero se depende enteramente del personal a cargo del acceso a los sistemas
A.9.2.3	Gestión de derechos de acceso privilegiado	L2 - Reproducible, pero intuitivo	Observación	No se evidencia la existencia de un proceso para la gestión de usuarios y asignación de contraseñas en los sistemas. Se siguen buenas prácticas, pero se depende enteramente del personal a cargo del acceso a los sistemas

Referencia Anexo A	Control	Efectividad	Estado	Observación
A.9.2.4	Gestión de información secreta de autenticación de usuarios	L2 - Reproducible, pero intuitivo	Observación	No se evidencia la existencia de un proceso para la gestión de usuarios y asignación de contraseñas en los sistemas. Se siguen buenas prácticas, pero se depende enteramente del personal a cargo del acceso a los sistemas
A.9.2.5	Revisión de los derechos de acceso del usuario	L2 - Reproducible, pero intuitivo	Observación	No se evidencia la existencia de un proceso para la gestión de usuarios y asignación de contraseñas en los sistemas. Se siguen buenas prácticas, pero se depende enteramente del personal a cargo del acceso a los sistemas
A.9.2.6	Eliminación o ajuste de los derechos de acceso	L2 - Reproducible, pero intuitivo	Observación	No se evidencia la existencia de un proceso para la gestión de usuarios y asignación de contraseñas en los sistemas. Se siguen buenas prácticas, pero se depende enteramente del personal a cargo del acceso a los sistemas
A.9.3	Responsabilidades del usuario			
A.9.3.1	Uso de información secreta de autenticación	L2 - Reproducible, pero intuitivo	Observación	Se cuenta con una política en la cual se menciona la responsabilidad de los usuarios con respecto al uso de la información secreta. Sin embargo, no se realizan más actividades relacionadas con el control de esta información
A.9.4	Control de Acceso a Sistemas y aplicaciones.			
A.9.4.1	Restricción de acceso a información	L2 - Reproducible, pero intuitivo	No conformidad menor	No se evidencia una práctica transversal a los procesos en relación con la restricción de acceso a la información o funcionalidades en los sistemas. Se depende de la gestión que realiza el administrador de cada una de ellas
A.9.4.2	Procedimientos de inicio de sesión seguros	L1 - Inicial/Ad-hoc	No conformidad menor	No se evidencian prácticas o procedimientos para asegurar que los inicios de sesión en todas las aplicaciones se realizan de forma segura
A.9.4.3	Sistema de gestión de contraseñas	L1 - Inicial/Ad-hoc	No conformidad menor	No se evidencian prácticas o procedimientos para la gestión segura de contraseñas a parte de las gestionadas en el directorio activo
A.9.4.4	Uso de utilidades privilegiadas	L2 - Reproducible, pero intuitivo	No conformidad menor	No se evidencia la implementación de una práctica transversal para la protección de los equipos y servidores para evitar el uso de utilidades privilegiadas. Existen

Referencia Anexo A	Control	Efectividad	Estado	Observación
				múltiples usuarios con permisos para usarlas y no se evidencia la documentación de los riesgos o las responsabilidades asociadas
A.9.4.5	Control de acceso al código fuente del programa	N/A	N/A	No está contemplado en la declaración de aplicabilidad
A.10	Criptografía			
A.10.1	Controles criptográficos			
A.10.1.1	Política sobre el uso de controles criptográficos	L3 - Proceso definido	En cumplimiento	Se evidencia el establecimiento y comunicación de la política de uso de controles criptográficos. No se cuenta con controles técnicos robustos para dar seguimiento a la gestión de estos controles
A.10.1.2	Gestión de claves	L1 - Inicial/Ad-hoc	No conformidad menor	La gestión de claves es manual y depende de cada usuario y cada proyecto, no se cuenta con políticas o procedimientos transversales para su manejo
A.11	Seguridad física y ambiental			
A.11.1	Áreas seguras			
A.11.1.1	Perímetro de seguridad física	L3 - Proceso definido	En cumplimiento	Se han definido los perímetros de las áreas de las oficinas, se evidencia la documentación de los planos de estas y la definición de las áreas seguras. Se evidencia el uso de controles de acceso físico y la documentación de los visitantes a las instalaciones y las áreas seguras
A.11.1.2	Controles de entrada física	L3 - Proceso definido	En cumplimiento	Se han definido los perímetros de las áreas de las oficinas, se evidencia la documentación de los planos de estas y la definición de las áreas seguras. Se evidencia el uso de controles de acceso físico y la documentación de los visitantes a las instalaciones y las áreas seguras
A.11.1.3	Protección de oficinas, salas e instalaciones	L3 - Proceso definido	En cumplimiento	Se han definido los perímetros de las áreas de las oficinas, se evidencia la documentación de los planos de estas y la definición de las áreas seguras. Se evidencia el uso de controles de acceso físico y la documentación de los visitantes a las instalaciones y las áreas seguras
A.11.1.4	Protección contra amenazas externas y ambientales	L1 - Inicial/Ad-hoc	No conformidad menor	No se evidencian controles físicos para la protección contra amenazas medio ambientales

Referencia Anexo A	Control	Efectividad	Estado	Observación
A.11.1.5	Trabajo en zonas seguras	L1 - Inicial/Ad-hoc	No conformidad menor	No se evidencian prácticas o procedimientos para el trabajo en las zonas que se han identificado como de alta seguridad. No se evidencia que estas zonas sean protegidas de forma especial con respecto al resto de las instalaciones
A.11.1.6	Áreas de carga y descarga	L3 - Proceso definido	En cumplimiento	Se evidencia la documentación de las áreas de carga y descarga, así como las políticas establecidas por la administración del edificio con respecto a su uso correcto
A.11.2	Equipo			
A.11.2.1	Protección y ubicación de equipo	L1 - Inicial/Ad-hoc	No conformidad menor	Las condiciones de protección de los equipos de cómputo, especialmente los servidores, no corresponde con lo establecido en la política de seguridad. No se evidencia la implementación de controles orientados a garantizar la seguridad de estos equipos. Con respecto a los equipos de usuario final tampoco se cuenta con controles físicos para su protección
A.11.2.2	Servicios de soporte	L2 - Reproducible, pero intuitivo	Observación	Los servicios de soporte de energía y comunicaciones se encuentran mencionados en las políticas de seguridad y se cuenta con algunos controles técnicos puntuales como las UPS y el canal de comunicaciones de backup. Sin embargo, no se evidencia un dimensionamiento adecuado de los controles ni existen procedimientos de actuación para la operación en caso de falla de algún suministro, lo cual ha sido definido como crítico por el tipo de servicios prestados
A.11.2.3	Seguridad del cableado	L3 - Proceso definido	En cumplimiento	Se evidencia la documentación acerca de las condiciones de seguridad del cableado desde el momento que se instaló al acondicionar la oficina, se evidencia la separación del cableado eléctrico del de datos. No se evidencia la ejecución de revisiones posteriores o mantenimientos del cableado. El cableado del rack no se encuentra etiquetado
A.11.2.4	Mantenimiento del equipo	L2 - Reproducible, pero intuitivo	Observación	No se evidencia la existencia de un plan de mantenimiento. Se han realizado actividades de mantenimiento correctivo cuando

Referencia Anexo A	Control	Efectividad	Estado	Observación
				se requiere, pero no se evidencian actividades preventivas
A.11.2.5	Eliminación de activos	L1 - Inicial/Ad-hoc	No conformidad menor	No se evidencian prácticas o procedimientos para la eliminación adecuada de los activos de información cuando se dan de baja
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	L2 - Reproducible, pero intuitivo	Observación	Se evidencia la implementación del cifrado para algunos equipos de cómputo que se utilizan con frecuencia fuera de las instalaciones de la empresa, no se encuentra documentación de alguna política o procedimiento para garantizar que este control sea aplicado en el 100% de los casos y depende del administrador su ejecución
A.11.2.7	Eliminación segura o reutilización de los equipos	L1 - Inicial/Ad-hoc	No conformidad menor	No se evidencian prácticas o procedimientos para la eliminación o protección de los equipos cuando se dan de baja o se reasignan
A.11.2.8	Equipo de usuario desatendido	L3 - Proceso definido	En cumplimiento	Se evidencia la política de directorio activo para el bloqueo de los equipos de usuario desatendidos y la divulgación de estas mediante charlas y envío de correo electrónico
A.11.2.9	Política de escritorio y pantalla limpia	L3 - Proceso definido	En cumplimiento	Se evidencia la política de escritorio y pantalla limpia y la divulgación de estas mediante charlas y envío de correo electrónico
A.12	Seguridad en las operaciones			
A.12.1	Procedimientos y responsabilidades operacionales			
A.12.1.1	Procedimientos operacionales documentados	L3 - Proceso definido	En cumplimiento	Se evidencia la documentación de los procedimientos para la operación de la plataforma tecnológica que soporta la ejecución de las actividades del proceso
A.12.1.2	Gestión de cambios	L3 - Proceso definido	En cumplimiento	Se evidencia la documentación de la política y el procedimiento de gestión de cambios a las plataformas. Así mismo, se evidencia la ejecución de las reuniones del comité de cambios de la empresa
A.12.1.3	Gestión de capacidad	L3 - Proceso definido	En cumplimiento	Se cuenta con un plan de gestión de la capacidad para los servidores y la infraestructura que presta servicios de cara al cliente

Referencia Anexo A	Control	Efectividad	Estado	Observación
A.12.1.4	Separación de entornos de desarrollo, prueba y operación	N/A	N/A	No está contemplado en la declaración de aplicabilidad
A.12.2	Protección contra código malicioso			
A.12.2.1	Controles contra código malicioso	L3 - Proceso definido	En cumplimiento	Se evidencia la implementación de controles técnicos contra código malicioso y la documentación de los procedimientos de despliegue en los equipos cuando son entregados a cada usuario. La desactivación del control requiere de contraseña y no se cuenta con más controles en este sentido
A.12.3	Respaldo			
A.12.3.1	Respaldo de información	L3 - Proceso definido	En cumplimiento	Se cuenta con procedimientos de respaldo de la información, tanto para los servidores como para los equipos de usuario final. No se realizan pruebas de las copias de respaldo tomadas
A.12.4	Registro y monitoreo			
A.12.4.1	Registro de eventos	L3 - Proceso definido	En cumplimiento	Se cuenta con un procedimiento y una herramienta de software en la cual se centralizan los eventos de los servidores para asegurar su protección, se verifican a través del SIEM para identificar incidentes de seguridad. Sin embargo, no se han establecido las políticas sobre lo que debe ser revisado y alertado
A.12.4.2	Protección de los registros de información	L2 - Reproducible, pero intuitivo	Observación	Se cuenta con un procedimiento y una herramienta de software en la cual se centralizan los eventos de los servidores para asegurar su protección
A.12.4.3	Registros de administrador y operados	L1 - Inicial/Ad-hoc	No conformidad menor	No se evidencian prácticas o procedimientos para la revisión de los registros de administradores y operadores de las plataformas informáticas que se utilizan en los procesos
A.12.4.4	Sincronización de reloj	L2 - Reproducible, pero intuitivo	Observación	La sincronización depende de la configuración de cada sistema de manera independiente y de acuerdo con la configuración que realiza cada administrador. No se cuenta con una política o procedimiento transversal
A.12.5	Control de software operacional			
A.12.5.1	Instalación de software en los sistemas operativos	L3 - Proceso definido	En cumplimiento	En el procedimiento de despliegue de sistemas se han definido políticas y actividades específicas para la instalación de software, se

Referencia Anexo A	Control	Efectividad	Estado	Observación
				cuenta con una lista de software permitido y un inventario de licenciamiento adquirido
A.12.6	Administración de vulnerabilidades técnicas			
A.12.6.1	Gestión de vulnerabilidades técnicas	L2 - Reproducible, pero intuitivo	Observación	No se evidencia una estrategia corporativa para la gestión de las vulnerabilidades técnicas. Se realizan escaneos esporádicos y no se realiza seguimiento a los hallazgos
A.12.6.2	Restricciones en la instalación de software	L2 - Reproducible, pero intuitivo	Observación	Se cuenta con un control técnico a través del directorio activo para evitar que los usuarios regulares puedan instalar software en los sistemas operativos. Se cuenta con múltiples usuarios con permisos de instalación sin que se evidencie la documentación de los riesgos asociados
A.12.7	Consideraciones sobre auditoría de los sistemas de información			
A.12.7.1	Controles de auditoría de sistemas de información	L1 - Inicial/Ad-hoc	No conformidad menor	No se evidencia la ejecución o documentación de controles relacionados con la auditoría de sistemas de información
A.13	Seguridad en las comunicaciones			
A.13.1	Administración de seguridad de red			
A.13.1.1	Controles de red	L2 - Reproducible, pero intuitivo	Observación	Se cuenta con algunos controles técnicos para la protección de la red como Firewall, IDS y control de contenido. Sin embargo, no se han documentado políticas o procedimientos al respecto
A.13.1.2	Seguridad de los servicios de red	L1 - Inicial/Ad-hoc	Observación	Se cuenta con algunos controles técnicos para la protección de la red como Firewall, IDS y control de contenido. Sin embargo, no se han documentado políticas o procedimientos al respecto
A.13.1.3	Segregación en las redes	L3 - Proceso definido	En cumplimiento	Las redes se encuentran segregadas y documentado el mapa de red con los direccionamientos y los componentes de seguridad existentes
A.13.2	Transferencia de información			
A.13.2.1	Políticas y procedimientos de transferencia de información	L3 - Proceso definido	En cumplimiento	Se cuenta con una política y un procedimiento relacionado con la transferencia de información,

Referencia Anexo A	Control	Efectividad	Estado	Observación
				específicamente con aquella que se comparte con los clientes
A.13.2.2	Acuerdos sobre la transferencia de información	L1 - Inicial/Ad-hoc	No conformidad menor	No se evidencian prácticas o procedimientos para generar acuerdos adecuados de transferencia de información con terceros
A.13.2.3	Mensajería electrónica	L3 - Proceso definido	En cumplimiento	Se cuenta con una política y un procedimiento relacionado con la mensajería electrónica. Sin embargo, no se cuenta con controles técnicos para aplicar las directivas establecidas por la empresa
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	L3 - Proceso definido	En cumplimiento	Se evidencia la existencia de los acuerdos de confidencialidad y no divulgación en los contratos de los empleados y en aquellos que se firman con los clientes
A.14	Adquisición, desarrollo y mantenimiento de sistemas			
A.14.1	Requisitos de seguridad de los sistemas de información			
A.14.1.1	Análisis y especificaciones de los requisitos de seguridad de la información	L3 - Proceso definido	En cumplimiento	Se cuenta con un procedimiento para el análisis de seguridad del software a adquirir, así como con un listado de requerimientos generales para cualquier caso que se evalúa y se toma en cuenta al momento de seleccionar un proveedor
A.14.1.2	Protección de los servicios de aplicaciones en las redes públicas	L1 - Inicial/Ad-hoc	No conformidad menor	Se evidencia el uso de servicios de aplicación en redes públicas, pero aún no se establecen los controles necesarios mínimos para su protección
A.14.1.3	Protección de transacciones de servicios de aplicación	N/A	N/A	No está contemplado en la declaración de aplicabilidad
A.14.2	Seguridad en los procesos de desarrollo y soporte			
A.14.2.1	Política de desarrollo seguro	N/A	N/A	No está contemplado en la declaración de aplicabilidad
A.14.2.2	Procedimientos de control de cambios del sistema	N/A	N/A	No está contemplado en la declaración de aplicabilidad
A.14.2.3	Revisión técnica de las aplicaciones después de implementar cambios de plataforma	L3 - Proceso definido	En cumplimiento	Se cuenta con un protocolo de revisión técnica a seguir posterior a la ejecución de cambios en las plataformas de software
A.14.2.4	Restricción de cambios en los paquetes de software	N/A	N/A	No está contemplado en la declaración de aplicabilidad
A.14.2.5	Principios de ingeniería de sistemas seguros	N/A	N/A	No está contemplado en la declaración de aplicabilidad

Referencia Anexo A	Control	Efectividad	Estado	Observación
A.14.2.6	Entorno de desarrollo seguro	N/A	N/A	No está contemplado en la declaración de aplicabilidad
A.14.2.7	Desarrollo subcontratado	N/A	N/A	No está contemplado en la declaración de aplicabilidad
A.14.2.8	Pruebas de seguridad del sistema	N/A	N/A	No está contemplado en la declaración de aplicabilidad
A.14.2.9	Pruebas de aceptación del sistema	N/A	N/A	No está contemplado en la declaración de aplicabilidad
A.14.3	Datos de prueba			
A.14.3.1	Protección de datos de prueba	N/A	N/A	No está contemplado en la declaración de aplicabilidad
A.15	Relaciones con proveedores			
A.15.1	Seguridad de la información en las relaciones con proveedores			
A.15.1.1	Política de seguridad de información para las relaciones con proveedores	L3 - Proceso definido	En cumplimiento	Se evidencia la existencia y divulgación de la política de seguridad en las relaciones con los proveedores, aún no se evidencia mejora de esta o los acuerdos contractuales
A.15.1.2	Manejo de seguridad dentro de los acuerdos con proveedores	L3 - Proceso definido	En cumplimiento	Se evidencia la existencia y divulgación de la política de seguridad en las relaciones con los proveedores, aún no se evidencia mejora de esta o los acuerdos contractuales
A.15.1.3	Cadena de suministro en tecnología de la información y comunicaciones	L2 - Reproducible, pero intuitivo	Observación	No es evidente la identificación de la cadena de suministro de la tecnología ni la definición de ciertas políticas o procedimientos específicos al respecto. Se maneja según cada caso
A.15.2	Administración de entrega de servicios de proveedores			
A.15.2.1	Seguimiento y revisión de los servicios de proveedores	L3 - Proceso definido	En cumplimiento	En la política existente se definen las responsabilidades de revisión y seguimiento sobre los servicios de los proveedores
A.15.2.2	Gestión de cambios en los servicios de proveedores	L2 - Reproducible, pero intuitivo	Observación	La gestión de los cambios en los servicios no se lleva según un control estricto ni documentado. Depende de la gestión del líder del proyecto o área relacionada
A.16	Gestión de incidentes de seguridad de la información			
A.16.1	Gestión de incidentes de seguridad de la información y las mejoras			
A.16.1.1	Responsabilidades y procedimientos	L3 - Proceso definido	En cumplimiento	Se evidencia la existencia y divulgación del procedimiento de gestión de incidentes, con sus

Referencia Anexo A	Control	Efectividad	Estado	Observación
				respectivas responsabilidades, mecanismo de reporte (incluyendo las debilidades), los criterios de evaluación, los mecanismos de respuesta y las responsabilidades de aprendizaje posterior. Adicionalmente, se evidencia la atención de múltiples situaciones como posibles incidentes de seguridad
A.16.1.2	Reporte de eventos de seguridad de la información	L3 - Proceso definido	En cumplimiento	Se evidencia la existencia y divulgación del procedimiento de gestión de incidentes, con sus respectivas responsabilidades, mecanismo de reporte (incluyendo las debilidades), los criterios de evaluación, los mecanismos de respuesta y las responsabilidades de aprendizaje posterior. Adicionalmente, se evidencia la atención de múltiples situaciones como posibles incidentes de seguridad
A.16.1.3	Reporte de debilidades de seguridad de la información	L3 - Proceso definido	En cumplimiento	Se evidencia la existencia y divulgación del procedimiento de gestión de incidentes, con sus respectivas responsabilidades, mecanismo de reporte (incluyendo las debilidades), los criterios de evaluación, los mecanismos de respuesta y las responsabilidades de aprendizaje posterior. Adicionalmente, se evidencia la atención de múltiples situaciones como posibles incidentes de seguridad
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	L3 - Proceso definido	En cumplimiento	Se evidencia la existencia y divulgación del procedimiento de gestión de incidentes, con sus respectivas responsabilidades, mecanismo de reporte (incluyendo las debilidades), los criterios de evaluación, los mecanismos de respuesta y las responsabilidades de aprendizaje posterior. Adicionalmente, se evidencia la atención de múltiples situaciones como posibles incidentes de seguridad
A.16.1.5	Respuesta a incidentes de seguridad de la información	L3 - Proceso definido	En cumplimiento	Se evidencia la existencia y divulgación del procedimiento de gestión de incidentes, con sus respectivas responsabilidades, mecanismo de reporte (incluyendo las debilidades), los criterios de evaluación, los mecanismos de respuesta y las responsabilidades

Referencia Anexo A	Control	Efectividad	Estado	Observación
				de aprendizaje posterior. Adicionalmente, se evidencia la atención de múltiples situaciones como posibles incidentes de seguridad
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	L3 - Proceso definido	En cumplimiento	Se evidencia la existencia y divulgación del procedimiento de gestión de incidentes, con sus respectivas responsabilidades, mecanismo de reporte (incluyendo las debilidades), los criterios de evaluación, los mecanismos de respuesta y las responsabilidades de aprendizaje posterior. Adicionalmente, se evidencia la atención de múltiples situaciones como posibles incidentes de seguridad
A.16.1.7	Recolección de evidencia	L2 - Reproducible, pero intuitivo	No conformidad menor	La recolección de evidencia se realiza de manera aislada y sin implementar prácticas para protegerla ante la manipulación o daño. No se cuenta con herramientas ni documentación sobre cómo ejecutar el proceso
A.17	Aspectos de seguridad de información de la gestión de la continuidad del negocio			
A.17.1	Continuidad de seguridad de información			
A.17.1.1	Planeación de la continuidad de seguridad de la información	L3 - Proceso definido	En cumplimiento	Existe un plan de continuidad del negocio en el cual se contempla asegurar que no se degrade la seguridad en la información y los procesos. Sin embargo, este plan aún no ha sido probado
A.17.1.2	Implementación de la continuidad de seguridad de la información	L2 - Reproducible, pero intuitivo	No conformidad menor	Existe un plan de continuidad del negocio en el cual se contempla asegurar que no se degrade la seguridad en la información y los procesos. Sin embargo, este plan aún no ha sido probado ni ha ocurrido algún evento adverso que lo iniciase
A.17.1.3	Verifica, revisa y evalúa la continuidad de seguridad de la información	L1 - Inicial/Ad-hoc	No conformidad menor	No se evidencian prácticas o procedimientos para la revisión de la seguridad en escenarios de contingencia
A.17.2	Redundancias			
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	L3 - Proceso definido	En cumplimiento	En el plan de continuidad se cuenta con un apartado en el cual se establecen las contingencias a nivel de las instalaciones de procesamiento de información. Estas se respaldan en las sedes

Referencia Anexo A	Control	Efectividad	Estado	Observación
				alternas de la empresa. Sin embargo, no se ha realizado pruebas de paso a contingencia
A.18	Cumplimiento			
A.18.1	Cumplimiento de los requisitos legales y contractuales			
A.18.1.1	Identificación de la legislación y requerimientos contractuales aplicables	L2 - Reproducible, pero intuitivo	No conformidad menor	No se evidencia un procedimiento formal para la verificación y cumplimiento del control. Se depende enteramente de la gestión de cada líder de proyecto o área
A.18.1.2	Derechos de propiedad intelectual	L2 - Reproducible, pero intuitivo	No conformidad menor	No se evidencia un procedimiento formal para la verificación y cumplimiento del control. Se depende enteramente de la gestión de cada líder de proyecto o área
A.18.1.3	Protección de registros	L2 - Reproducible, pero intuitivo	No conformidad menor	No se evidencia un procedimiento formal para la verificación y cumplimiento del control. Se depende enteramente de la gestión de cada líder de proyecto o área
A.18.1.4	Privacidad y protección de datos personales	L2 - Reproducible, pero intuitivo	No conformidad menor	No se evidencia un procedimiento formal para la verificación y cumplimiento del control. Se depende enteramente de la gestión de cada líder de proyecto o área
A.18.1.5	Regulación de controles criptográficos	N/A	N/A	No está contemplado en la declaración de aplicabilidad
A.18.2	Revisiones de Seguridad de la información			
A.18.2.1	Revisión independiente de la seguridad de la información	L3 - Proceso definido	En cumplimiento	Se cuenta con un plan de auditoria y revisión interna de la operación de los controles y el SGSI por un ente externo a los procesos contemplados en el alcance
A.18.2.2	Cumplimiento con las políticas y estándares de seguridad	L3 - Proceso definido	En cumplimiento	Se revisan periódicamente los indicadores con respecto al desempeño de los controles y el cumplimiento de las políticas por parte de la dirección general. Se evidencia la realización de múltiples reuniones orientadas a esta verificación
A.18.2.3	Revisión de cumplimiento técnico	L3 - Proceso definido	En cumplimiento	Se revisan periódicamente los indicadores con respecto al desempeño de los controles y el cumplimiento de las políticas por parte de la dirección general. Se evidencia la realización de

Referencia Anexo A	Control	Efectividad	Estado	Observación
				múltiples reuniones orientadas a esta verificación

10.4 DIAGRAMA DE RADAR REVISIÓN DE CONTROLES DE SEGURIDAD

En la siguiente imagen se observan los resultados obtenidos (rojo) durante la auditoría con respecto a los resultados esperados (verde).

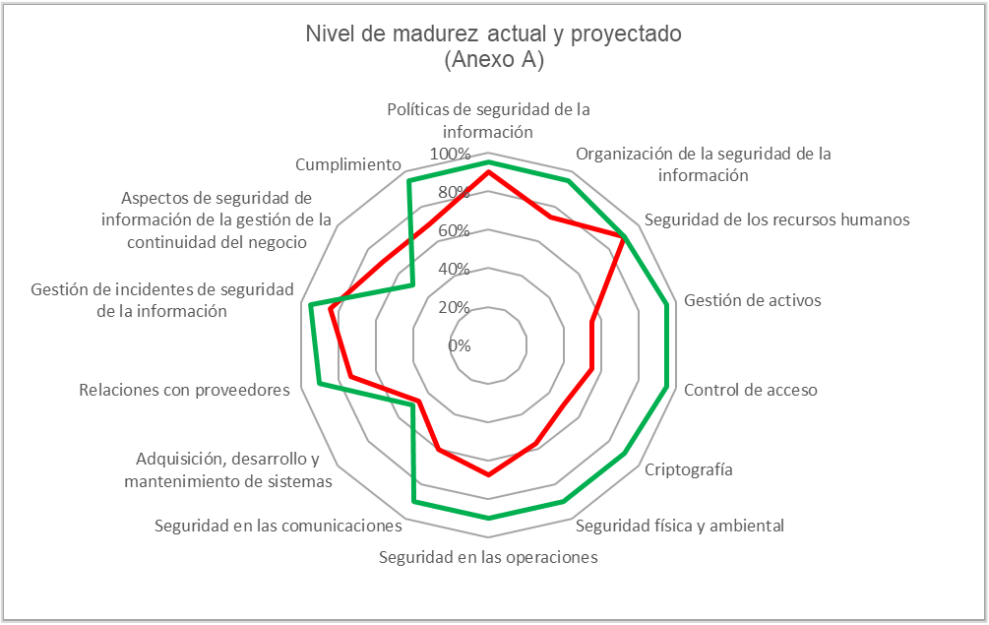


Imagen 10-1 Resultados de la revisión de controles de seguridad

10.5 CANTIDAD DE HALLAZGOS DE LA AUDITORÍA

En la siguiente imagen se puede observar la estadística relacionada con los hallazgos de auditoría.

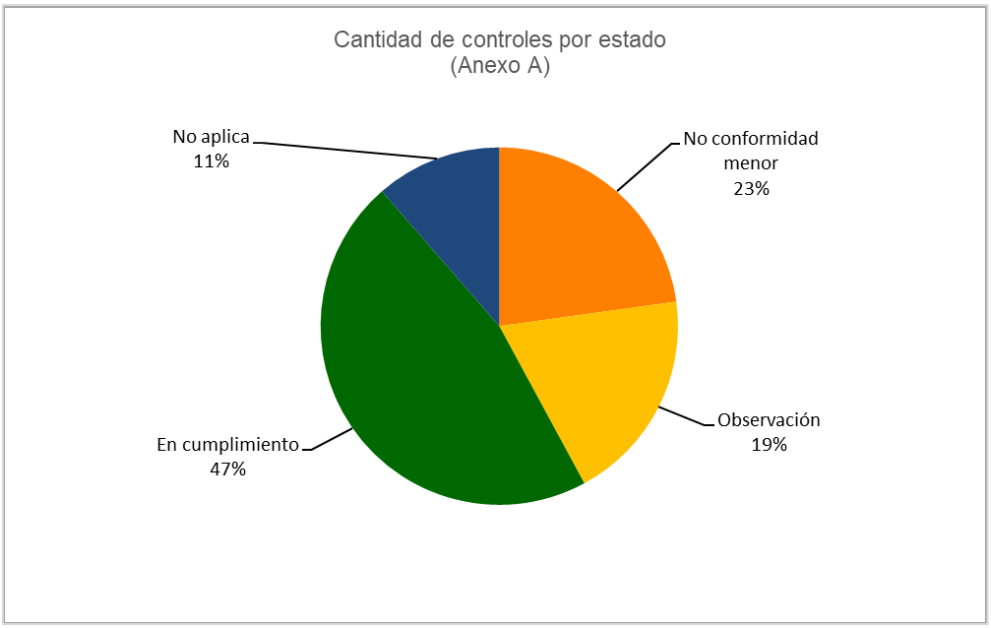


Imagen 10-2 Cantidad de hallazgos en los controles

De acuerdo con lo anterior, se evidencia el bajo nivel de madurez actual de la organización con respecto a la implementación de varios de los controles de seguridad de acuerdo con su declaración de aplicabilidad. Esto se debe a que la organización se encuentra en una etapa inicial de implementación, y aunque ha avanzado de forma importante en la documentación de políticas y procedimientos, y ha realizado múltiples sesiones de divulgación y sensibilización, aún existen múltiples controles de seguridad en un estado inicial de implementación.

10.6 CONCLUSIONES DE AUDITORÍA

Tras la conclusión del ejercicio de auditoría se identificaron múltiples oportunidades de mejora que deben ser tenidas en cuenta, puesto que serán objeto de la siguiente revisión de auditoría.

Durante la auditoría se identificaron 17 controles en estado Inicial/ad hoc y 31 en estado Reproducible pero intuitivo. En estos casos no se evidencia su documentación o implementación consistente a través de los procesos incluidos en el alcance del Sistema.

En el 23% de los controles auditados se presenta una No conformidad menor, es decir que se identificaron casos puntuales de incumplimiento, o una observación que generar una oportunidad de mejora para el Sistema de Gestión.

Durante la auditoría se evidenció la ejecución del análisis de riesgo y la existencia del plan de tratamiento correspondiente. Así mismo, se evidencia del seguimiento a dicho plan y el resultado reflejado en el avance de implementación de controles de seguridad.

11 CONCLUSIONES

El Plan Director desarrollado traza una hoja ruta para la estrategia de seguridad de la empresa Consultora JC S.A.S., y cuenta con los elementos necesarios para que su funcionamiento cuente con los elementos de mejora continua requeridos por la norma NTC-ISO-IEC-27001:2013.

El alcance definido para el Plan Director de Seguridad de la Información es adecuado para lograr los objetivos establecidos. Sin embargo, los controles de seguridad que puedan ser adoptados de forma transversal por procesos fuera del alcance se deberían adoptar, aprovechando los esfuerzos de implementación y los beneficios con respecto a la protección de la información.

La implementación del SGSI será un factor estratégico para la compañía que seguramente estará en capacidad de satisfacer los requisitos de los clientes, proveedores y empleados, así como las leyes relacionadas con la protección de la información.

Un adecuado ejercicio de análisis de riesgo permitió obtener resultados aterrizados a la realidad de la organización y plantear los proyectos de inversión más adecuados y eficientes para asegurar sus activos de información.

La elaboración cuidadosa de la declaración de aplicabilidad, a partir del conocimiento de los procesos y los resultados del análisis de riesgo, fue fundamental para lograr una gestión de la seguridad de la información en la cual se tiene un equilibrio entre la protección de la información y los costos asociados.

12 ANEXOS

Anexo 1 - Análisis diferencial

Anexo 2 - Declaración de aplicabilidad SGSI

Anexo 3 - Matriz de Riesgo Inherente

Anexo 4 - Cronograma de trabajo (Propuestas de proyectos)

Anexo 5 - Análisis diferencial (Después de proyectos)

Anexo 6 - Matriz de Riesgo Residual

Anexo 7 - Auditoría de Cumplimiento

13 REFERENCIAS

Acerta. (14 de Marzo de 2019). *Acerta Comunicaciones*. Obtenido de Análisis del contexto de la empresa: http://acertacomunicaciones.com/analisis-de-contexto-la-empresa/

Araque, J. O. (2017). *Auditoría al Sistema de Gestión de Seguridad Informácion en el proceso de desarrollo de software de acuerdo a la norma ISO/IEC 27001:2013 en la empresa IT Stefanini Colombia.* Bogotá: Universidad Nacional Abierta y a Distancia –UNAD.

GTC-ISO-IEC 27002. (2013). *Código de práctica para controles de seguridad de la información.* Bogotá: ICONTEC.

ISACA. (2012). *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de la Empresa.* Rolling Meadows.

ISO-IEC 27000. (2014). *Sistemas de Gestión de Seguridad de la información - Resumen y vocabulario.* Ginebra: ISO.

ISOTOOLS. (16 de Marzo de 2019). *Blog Calidad y Excelencia*. Obtenido de ¿Cuál es el funcionamiento del Anexo SL?: https://www.isotools.org/2017/03/14/funcionamiento-anexo-sl/

ISOTools Excellence. (16 de Marzo de 2019). *PMG SSI - ISO 27001*. Obtenido de La NCh ISO 27001. Origen y evolución.: https://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/

Ministerio de Hacienda y Administraciones Públicas. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid.

National Institute of Standards and Technology (NIST). (2013). *Glossary of Key Information Security Terms Rev. 2.* Gaithersburg: NIST.

NTC-ISO 31000. (2009). *Gestión del Riesgo - principios y Directrices.* Bogota: ICONTEC.

NTC-ISO-IEC 27001. (2013). *Sistemas de Gestión de Seguridad de la Información, Requisitos.* Bogotá: ICONTEC.