FACULTAD DE POSGRADOS

PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) APLICADO A LA ORGANIZACIÓN “ABC”.

AUTOR

EDISON XAVIER SAFLA ARANHA

AÑO

2021

FACULTAD DE POSGRADOS

PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) APLICADO A LA ORGANIZACIÓN “ABC”.

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Magíster en Gestión de la Seguridad de la Información.

Autor

Edison Xavier Safla Aranha

Año

2021

AGRADECIMIENTOS

Agradezco eternamente a mis padres por haberme forjado como la persona que soy en la actualidad; todos mis logros se los debo a ustedes entre los cuales incluye este. Formándome con sueños y con aspiraciones, motivándome constantemente para alcanzar mis anhelos. Los amo para toda la eternidad.

DEDICATORIA

El presente trabajo de titulación va dedicado a mis padres, mi esposa y sobre todo a mi hijo, Emilio eres lo más hermoso que me ha podido pasar en la vida. Doy gracias a Dios por permitirme ser tu papá, eres la razón y mi motivación para seguir creciendo. Te amo Emilio.

RESUMEN

En toda organización existe una gran cantidad de desafíos relacionados con la seguridad de la información, el asegurar y proteger cada uno de los activos de información con los que cuentan las organizaciones es el primer paso. Los planes de acción y buenas prácticas permiten mitigar las vulnerabilidades que puedan existir y corromper la información de la organización.

Establecer un programa de seguridad de la información en toda entidad sea pública o privada debe ser considerado como primer paso para las áreas de IT, un sistema de gestión de seguridad de la información permite mantener una completa integridad, disponibilidad, confidencialidad y privacidad en los datos de la organización.

Un sistema estructurado permite a las organizaciones evitar interrupciones en sus operaciones y a su vez pérdidas financieras, lo cual es de suma importancia para toda organización existente. El análisis en el transcurso de este proyecto permitirá identificar los riesgos y vulnerabilidades asociadas a la organización de estudio, permitiendo de esta forma diseñar un programa de gestión de seguridad de la información que ayudará a madurar los procesos internos dentro de cada una de las áreas asociadas.

ABSTRACT

In any organization there are a large number of challenges related to information security, securing and protecting each of the information assets that organizations have it is the first step. Action plans and good practices make it possible to mitigate any vulnerabilities that may exist and corrupt the information of the organization.

Establishing an information security program in any entity, whether public or private, should be considered as a first step for IT areas, an information security management system allows to maintain complete integrity, availability, confidentiality and privacy in the data. of the organization.

A structured system allows organizations to avoid interruptions in their operations and in turn financial losses, which is of the utmost importance for any existing organization. The analysis in the course of this project will allow identifying the risks and vulnerabilities associated with the study organization, thus allowing the design of an information security management program that will help to mature the internal processes within each of the associated areas.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Introducción

Este programa propone a la organización ABC un modelo de Sistema de Gestión de la Seguridad de la Información donde permitirá fortalecer su actual programa de seguridad, aumentando su productividad y disminuyendo sus vulnerabilidades detectadas en el transcurso de los análisis realizados.

El programa beneficiará a la organización permitiendo madurar sus procesos de negocio y fortaleciendo los mismos, con esto asegurará a cada uno de sus activos de información una alta integridad, confiabilidad, disponibilidad y privacidad permitiendo elevar sus estándares en base a los indicadores de éxito recopilados en la organización

El programa consiste en una identificación del sistema actual de gestión de seguridad de información, analizando la información para posteriormente clasificarla e identificar los activos de información críticos. Con esto se propondrá diversas políticas de alto nivel para consecuentemente evaluar los riesgos de los activos críticos. Permitiendo así, definir nuevos planes de acción que puede tomar la organización para elevar sus procesos y mejorarlos continuamente.

La organización estudiada en el transcurso de este proyecto se detalla como una compañía perteneciente a la nueva era digital, llevando en el mercado corportivo 37 años de experiencia que le han permitido crecer y desarrollar a las organizaciones del sector mediante consultoría estratégica, de magnitud nacional e internacional. Basados en valores éticos y excelencia, en conjunto a sus productos ofertados de alta gama que permiten el apoyo a la resolución de adversidades de manera disruptiva.

1. DESARROLLO DEL PROGRAMA

1.1. Objetivo

La organización cuenta con un programa de seguridad de información en estado inicial el cual no permite gestionar, analizar y manipular de forma adecuada los activos de información. Toda actividad relacionada con los activos de información es manejada con base en la experiencia y conocimiento del equipo técnico. Esto nos muestra que no se acoge a un plan estricto basado en directrices, por lo tanto, debido a que la organización ABC maneja información crítica, la cual es de gran valor es necesario implementar un plan de seguridad de información.

El alcance de este objetivo permite mitigar los diversos riesgos a los cuales la información está expuesta, garantizando de esta manera obtener alta confidencialidad, integridad, disponibilidad y privacidad en sus activos de información.

La información que es manejada en la organización ABC es de alta criticidad, la misma se encuentra alojada en los servidores ubicados en el DataCenter de la empresa. Esta información es respaldada de manera autónoma bajo un programa de software libre directamente a un servidor CORE.

1.2. Metodología

Para el desarrollo de este programa de seguridad de la información se usará una metodología que permita visualizar y recolectar datos sobre su actual estado del programa actual de seguridad, tanto físico como lógico y poder alinearlos en base al estándar de la ISO 27001 en conjunto al Anexo A, para de esta manera mitigar posibles ataques y vulneraciones a la integridad, disponibilidad, confidencialidad y privacidad de los datos en el área de sistemas de la organización.

1.3. Diagnóstico

Para obtener el diagnóstico del estado actual del SGSI de la organización es importante tener en cuenta las normas y estándares establecidos para poder alinearlos correctamente al enfoque de la organización. Como se indicó en la metodología el estándar en el cual se realizará el diagnóstico es la norma ISO27001 en conjunto con el Anexo A.

1.3.1. ¿Qué es la ISO 27001?

La norma ISO 27001 es un estándar internacional que garantiza a las organizaciones la confidencialidad, integridad, disponibilidad y privacidad de los datos y de la información, como tambien de los diversos sistemas que procesan estos datos. (ISOTools, 2021)

El uso del estándar ISO 27001 permite a los sistemas de gestión de seguridad de la información contar con evaluaciones de riesgo los mismos que permitirán la aplicación de controles los cuales son de vital importancia para erradicar o mitigar estos fallos en los sistemas de seguridad de las organizaciones. (Brenner, 2007)

1.3.2. Estado de implementación actual

La realización del estado actual de la implementación del estándar ISO 27001 se llevó a cabo en base a las normas de inspección propias del estándar en conjunto con adaptaciones propuestas para la organización. Entre ellas podemos encontrar las actividades de mejora con sus respectivos códigos de actividad y una calificación a estas actividades. La calificación de las activdades permitirá otorgar un concepto claro del avance de madurez que otorgará la actividad para el requerimiento obtenido del estándar como se puede observar en la Figura 1.

Estado de Implementación ISO 27001						
Sección	Requerimientos ISO 27001	Calificación actual	Estado actual	Código actividad	Actividades para mejora	n mejorada
4	Contexto de la organización					
4.1	Comprensión de la organización y de su contexto					
4.1	Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia	Inicial	La organización comenzó con su proceso de identificación de objetivos para su SGSI	4.1.1	Definir y acordar con todas las partes interesadas los objetivos del SGSI precautelando su eficacia durante la implementación.	Alto
4.2	expectativas de las partes interesadas					
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	Medio	La organización tiene identificado a las partes interesadas.	4.2.1	Analizar e identificar los factores internos y externos (obligaciones legales, regulatorias y contractuales), así como las tendencias en el entorno de negocio que pueden influir en el programa.	Optimizado
4.2 (b)	Determinar los requerimientos y oblicaciones relevantes de seguridad de la información	Medio	La organización ha determinado los requerimientos relevantes de seguridad de la información que piden sus partes interesadas	4.2.2	Analizar los diversos requerimientos obtenidos, madurar cada requerimiento conforme a las obligaciones que competen al mismo.	Optimizado
4.3	Determinación del alcance del SGSI					
4.3	Determinar y documentar el alcande del SGSI	Inicial	La organización a comenzado a determinar un alcance para un posible SGSI	4.3.1	Evaluar y determinar directrices para el cumplimiento del alcance propuesto.	Alto
4.4	SGSI					
4.4	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estandar	Inexistente	La organización no cuenta con un SGSI	4.4.1	Validar y ejecutar el programa propuesto en la organización permitiendo de esta forma obtener un programa SGSI acorde a las necesidades de la	Optimizado

Figura 1 Estado de implementación ISO27001: Sección 4

En la Figura 2 podemos observar la sección 5 del estándar ISO27001 donde nos indica el estado actual de liderazgo de la organización.

5	Liderazgo					
5.1	Liderazgo y compromiso					
5.1	La administración debe demostrar liderazgo y compromiso por el SGSI	Alto	Las partes están interesadas en implementar un SGSI han firmado un acta de compromiso y revisión	5.1.1	Mantener una constante supervisión del programa SGSI para su mejora continua en base a las directrices establecidas.	Optimizado
5.2	Política					
5.2	Documentar la Política de Seguridad de la Informacion	Inicial	La organización tiene documentación de ciertas políticas que llevan a cabo	5.2.1	Establecer las directrices de comportamiento para proteger la información, sistemas e infraestructura	Alto
5.3	Roles, responsabilidades y autoridades en la organización					
5.3	Asignar y comunicar los roles y responsabilidades de seguridad de la información	Inicial	La organización cuenta con roles y organización para el acceso a su información de parte del área técnica	5.3.1	Establecer, acordar y comunicar los roles y responsabilidades relacionadas con I&T a todo el personal de la empresa, de acuerdo con las	Alto

Figura 2 Estado de implementación ISO27001: Sección 5

Como podemos observar en la Figura 3 se indica el estado actual de planificación de la organización, siendo una de las secciones con mayor riesgo con base en su calificación obtenida durante la revisión de los requerimientos detallados.

6	Planificación					
6.1	Acciones para tratar los riesgos y oportunidades					
6.1.1	Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportinidades	Inexistente	La organización no cuenta con un SGSI	6.1.1.1	Definir el alcance y los límites del sistema de gestión de seguridad de la información (SGSI) en términos de las características de la empresa, organización, ubicación, activos y tecnología.	Alto
6.1.2	Definir e implementar un proceso de análisis de riesgos de seguridad de la información	Inexistente	La organización no cuenta con un SGSI	6.1.2.2	Definir el alcance adecuado de los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y/o la criticidad de los activos	Alto
6.1.3	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información	Inexistente	La organización no cuenta con un SGSI	6.1.3.3	Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con objetivos estratégicos y la arquitectura empresarial. Asegurar que el plan identifique las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, responsabilidades y prioridades	Alto
6.2	información y planificación para su consecución					
6.2	Establecer y documentar los planes y objetivos de la seguridad de la información	Inexistente	La organización no cuenta con un SGSI	6.2.1	Definir el alcance y los límites del sistema de gestión de seguridad de la información (SGSI) en términos de las características de la empresa, organización, ubicación, activos y tecnología.	Alto

Figura 3 Estado de implementación ISO27001: Sección 6

En la Figura 4 encontramos la sección de soporte de la organización, el requerimiento documentado nos permite evaluar a la organización sobre sus recursos, competencia, concienciación, comunicación e información documentada. La información documentada es uno de las salvaguardas mas importantes durante este programa de seguridad de la información.

7	Soporte					
7.1	Recursos					
7.1	Determinar y asignar los recursos necesarios para el SGSI	Medio	La organización tiene una asignación de recursos para el área	7.1.1	Llevar a cabo las actualizaciones y reformas programadas basadas en los directrices	Alto
7.2	Competencia					
7.2	Determinar, documentar hacer disponibles las competencias necesarias	Inexistente	No cuentan con documentación de SGSI referentes a aplicar	7.2.1	Alinear los objetivos de la empresa basándose en la mejora continua y capacitación constante al personal para obtener trabajadores competentes	Optimizado
7.3	Concienciación					
7.3	Implementar un programa de concianciación de seguridad	Medio	Cuentan con un programa básico de concientización basado por el COVID 19	7.3.1	Preparar un programa de comunicación que presente el plan de forma eficaz usando los medios de comunicación y tecnologías	Alto
7.4	Comunicación					
7.4	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI	Inexistente	La organización no cuenta con un SGSI	7.4.1	Mantener los principios para la comunicación con partes interesadas externas e internas, incluidos formatos y canales de comunicación, así como la aceptación y firma de informes de las partes	Alto
7.5	Información documentada					
7.5.1	Proveer documentacion requerida por el estándar más la requerida por la organización	Inicial	La organización está comprometida en proveer la información necesaria para la implementación de un SGSI	7.5.1.1	Formular y evaluar un plan de gestión de documentación basandose en perfiles y roles dentro de la organización para control de activos	Alto
7.5.2	Proveer un titulo, autor, formato consistente, revisión y aprobación a los documentos	Inicial	La organización está comprometida en proveer la información necesaria para la implementación de un SGSI	7.5.2.2	Determinar y alinear directrices basadas en el comité de revisión para la aprobación de documentos.	Alto
7.5.3	Mantener un control adecuado de la documentación	Inicial	La organización está comprometida en proveer la información necesaria para la implementación de un SGSI		Determinar un plan de tratamiento de documentación, procurando su confidencialidad, integridad, confidencialidad y privacidad.	Alto

Figura 4 Estado de implementación ISO27001: Sección 7

La sección de operación que observamos en la Figura 5 permite observar que la ogranización cuenta con grandes brechas de seguridad de la información, no

abstante estos riesgos cuentan con actividades de mejora que llevarán estos procesos a madurar de forma que la organización cuente con tratamientos de riesgos de la seguridad de la información de forma optimizada.

8	Operación					
8.1	Planificación y control operacional					
8.1	Planificar, implementar, controlar y documentar el proceso de gestión de riesgos del SGSI (Tratamiento de riesgos)	Inexistente	La organización no cuenta con un SGSI	8.1.1	Determinar normas y directrices para el proceso de gestión de riesgos y su tratamiento respectivo.	Alto
8.2	Apreciación de los riesgos de seguridad de la información					
8.2	Evaluar y documentar los riesgos de seguridad regularmente y cuando hay cambios	Inexistente	La organización no cuenta con un SGSI	8.2.1	Documentar los cambios, reevaluar y priorizar el portafolio para garantizar el alineamiento con el programa de SGSI resguardando la seguridad de	Alto
8.3	Tratamiento de los riesgos de seguridad de la información					
8.3	Implementar un plan de tratamiento de riesgos y documentar los resultados	Inexistente	La organización no cuenta con un SGSI	8.3.1	Mantener, como parte de la arquitectura de la empresa, un inventario de los componentes de la solución establecida para gestionar los riesgos	Optimizado

Figura 5 Estado de implementación ISO27001: Sección 8

En la Figura 6 podemos observar la evaluación de desempeño de la organización, como se observa las auditorías, revisiones y seguimientos son nulos, esto no impide que el programa propuesto mitige estos requerimientos con base en las actividades propuestas. Las actividades propuestas permitirán a la organización tener métricas y directrices aptas para el cumplimiento de auditorías y revisiones que sean requeridas por parte de las entidades reguladoras.

9	Evaluación del desempeño					
9.1	Seguimiento, medición, análisis y evaluación					
9.1	Realizar un seguimiento, medición, análisis y evaluación del SGSI y los controles	Inexistente	La organización no cuenta con un SGSI	9.1.1	Implementar métricas y directrices para hacer un seguimiento de cómo se alcanzan los beneficios, cómo evolucionan a lo largo del ciclo de vida del	Alto
9.2	Auditoría interna					
9.2	Planificar y realizar una auditoria interna del SGSI	Inexistente	La organización no cuenta con un SGSI	9.2.1	Determinar y documentar un proceso de auditoria interna anula en base a las auditorías	Alto
9.3	Revisión por la dirección					
9.3	La administración realiza una revisión periódica del SGSI	Inexistente	La organización no cuenta con un SGSI	9.3.1	Revisar de forma regular los planes de continuidad para considerar el impacto del actual SGSI en base a nuevas amenzas y procesos que	Optimizado

Figura 6 Estado de implementación ISO27001: Sección 9

En la Figura 7 podemos observar el requerimiento de mejora propuesto por la ISO27001, esta sección permite recolectar normas correctivas y planes de mejora continua, cabe recalcar que la ISO27001 es una norma que permite a las organizaciones mejorar continuamente a lo largo del tiempo. (Ladino, Villa, & López, 2011)

10	Mejora					
10.1	correctivas					
10.1	Identificar, arreglar y reaccionar ante no conformidades para evitar su recurrencia documentando todas las acciones	Inexistente	La organización no cuenta con un SGSI	10.1.1	Establecer una plataforma para compartir buenas prácticas y captar información sobre los defectos y errores para permitir el aprendizaje a	Optimizado
10.2	Mejora continua					
10.2	Mejora continua del SGSI	Inexistente	La organización no cuenta con un SGSI	10.2.1	Identificar los procesos críticos para el negocio basado en los motivadores de rendimiento y conformidad y el riesgo relacionado. Evaluar la capacidad e identificar los objetivos de mejora. Analizar las brechas de capacidad y control. Identificar opciones para mejorar o rediseñar el proceso.	Alto

Figura 7 Estado de implementación ISO27001: Sección 10

La continuación del estado de implementación ISO27001 referente al Anexo A lo podemos encontrar en la sección de ANEXOS.

1.3.3. Conclusión

Para concluir con el estado actual del estado de implementación ISO27001 en la organización se tomará en cuenta la siguiente tabla:

Estado SGSI		
Estado	Estado Actual	Estado Esperado
Inexistente	28%	0%
Inicial	30%	0%
Medio	24%	0%
Alto	18%	75%
Optimizado	0%	25%

Figura 8 Estado de implementación Actual-Esperado

Como se observa en la Figura 8 tenemos una apreciación sobre el estado actual de implementación de la ISO27001, considerando en esta rúbrica el Anexo A del estándar.

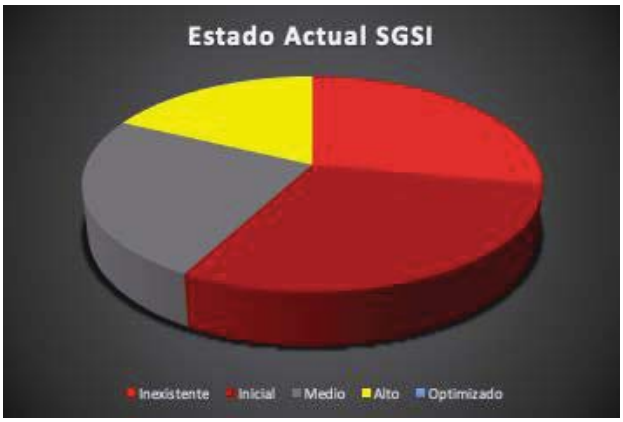

Figura 9 Estado de implementación Actual

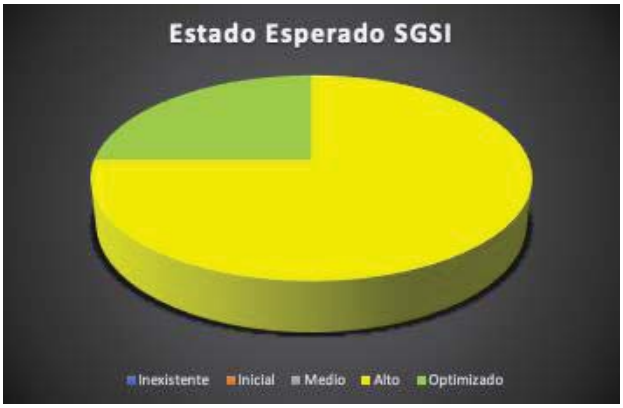

Figura 10 Estado de implementación Esperado

Se puede concluir que el estado actual del SGSI de la organización se encuentra en un estado inicial, hay muchas prácticas las cuales están en proceso de implementación sin embargo existen grandes oportunidades de mejora las cuales permitirán madurar los procesos de la organización.

1.4. Clasificación de la información

La clasificación de la información es un paso fundamental y de alta importancia para la evaluación de riesgos. La clasificación de la información permite al programa de seguridad de la información tener claro el panorama de los activos de información de las organizaciones con el fin de poder obtener una identificación de activos críticos clara y concisa. (Sosa, 2012)

La clasificación de los tipos de información es un proceso constante, día a día las organizaciones adquieren nuevos tipos de información en sus repositorios. Es por este motivo que la clasificación de la información en una organización es constante y no se detiene. Una de las caracterísiticas de la clasificación de los tipos de información es que permite a las organizaciones calificar cada activo de información basándose mediante:

1. Confidencialidad
2. Integridad
3. Disponibilidad
4. Privacidad

Para la clasificación de los tipos de información es importante empezar con el modulador de tipos de impacto que puede sufrir la organización. A continuación, en la Figura 11 se indica el modulador propuesto en base a los requerimientos de la organización para la clasificación de sus activos de información.

Tipología de impacto	Aversión	Neutral	Agresivo
Pérdidas financieras	x		
Interrupción de operaciones parciales y/o totales	x	x	
Pérdida / Degradación de la Imagen institucional		x	
Demandas judicial, afectación Legal	x	x	
Afectación al clima laboral		x	x

Figura 11 Tipología de impacto

Basados en la tipología de impacto obtenida se podrá obtener la matriz de impacto de cada uno de ellos basados en los estándares que maneja la organización, estos valores son recolectados en conjunto con la organización y sus perdidas estimadas para cada tipo de impacto como se detalla en la Figura 12.

IMPACTO	Alto	Medio	Bajo	Nulo
Pérdidas financieras	Mas de 50.000 dólares	Entre 10.000 a 50.000 dólares	Entre 5.000 a 10.000 dólares	Ente 1 a 5.000 dólares
Interrupción de operaciones parciales y/o totales	Más de 3 horas	Entre 2 horas a 3 horas	Entre 1 hora hasta 2 horas	Menor a 1 hora
Pérdida / Degradación de la Imagen institucional	Cancelación de contratos totales	Clientes antiguos detienen procesos con la empresa	Cancelación parcial de contratos nuevos	
Demandas judicial, afectación Legal	Procesos legales que generan la perdida total de contratos con el sector público y privado.	Procesos legales que perjudican a la organización en la participación de contratos dentro del sector público y privado		
Afectación al clima laboral		Mediana evidencia de conflictos laborales que afectan a la organización	Baja evidencia de conflictos que afectan a la organización	Sin evidencias de conflictos dentro de la organización

Figura 12 Tipología de impacto aplicado a la organización ABC

Como se puede observar en la Figura 13, la clasificación de los tipos de información de la organización ABC han sido evaluados en base a los criterios de impacto partiendo de los criterios de confidencialidad, integridad, disponibilidad y privacidad de la organización ABC.

No.	Nombre de la Entidad	Nombre del Tipo de Información	Definición del tipo de Información	Dueño de la Entidad	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	PRIVACIDAD	Calificación
					PROMEDIO	PROMEDIO	PROMEDIO	PROMEDIO	CRITICIDAD
1	Tecnologías de la información	Ordenes de trabajo	Documentación pertinente a los trabajos realizados como su información de registro de horas atendidas y asignación de personal	Gerente Soporte	Bajo	Nulo	Nulo	Nulo	Nulo
2	Tecnologías de la información	Actas de instalación y soporte	Actas de reunión realizadas con los clientes en base a las ordenes de instalación y soporte	Gerente Soporte	Nulo	Nulo	Nulo	Nulo	Nulo
3	Tecnologías de la información	Informes incidentes	Informe de incidentes previos con los clientes	Gerente Soporte	Nulo	Bajo	Nulo	Nulo	Nulo
4	Tecnologías de la información	Informe de instalación	Informes de instalación de IT	Gerente Soporte	Nulo	Nulo	Nulo	Nulo	Nulo
5	Tecnologías de la información	Informe de inspección	Informes de inspección a clientes	Gerente Soporte	Nulo	Nulo	Nulo	Nulo	Nulo
6	Tecnologías de la información	Proveedores	Documentación acorde a los contratos con los proveedores	Gerente Sistemas	Bajo	Nulo	Nulo	Nulo	Nulo
7	Tecnologías de la información	Partner	Documentación pertinente a los convenios con Partners	Gerente Sistemas	Bajo	Nulo	Nulo	Nulo	Nulo
8	Tecnologías de la información	Diseños técnicos	Documentos correspondiente a los diseños de arquitectura de IT hacia los clientes	Gerente Sistemas, Gerente de Soporte	Bajo	Nulo	Nulo	Bajo	Nulo
9	Clientes	Información del cliente	Datos de información básicos sobre el cliente donde se puede encontrar datos como: Razón social, RUC, Contactos	Financiero	Bajo	Nulo	Nulo	Nulo	Nulo
10	Clientes	Investigación y Desarrollo	Información que nos permita identificar avances en desarrollos de productos del cliente	Financiero	Nulo	Nulo	Nulo	Nulo	Nulo
11	Clientes	Posicionamiento financiero	Información relacionada con los estados financieros del cliente como tambien su nivel de venta y patrimonios	Financiero	Bajo	Bajo	Nulo	Bajo	Bajo
12	Clientes	Estrategia comercial	Acciones que pone en práctica el cliente para dar a conocer un nuevo producto, para aumentar su cuota de venta o de participación de mercado.	Analista Financiero, Marketing	Nulo	Nulo	Nulo	Nulo	Nulo
13	Empleado	Descripción laboral	Informacion relacionada que describa acerca del empleado y sus funciones.	Recursos Humanos	Nulo	Bajo	Nulo	Nulo	Bajo
14	Empleado	Información médica	Informacion relacionada al estado de salud y en la condicion que se encuentra el o los empleados.	Recursos Humanos	Nulo	Nulo	Nulo	Nulo	Nulo
15	Empleado	Seguro social	Toda informacion relacionada y necesaria al seguro social (IESS).	Recursos Humanos	Bajo	Bajo	Nulo	Nulo	Nulo
16	Empleado	Ámbito financiero	Informacion relacionada a un metodo donde el o los empleados puedan tener acceso a su remuneracion laboral.	Recursos Humanos	Bajo	Nulo	Nulo	Nulo	Nulo
17	Empleado	Experiencia laboral	Informacion relacionada a la experiencia laboral que ha ejercido el empleado.	Recursos Humanos	Bajo	Bajo	Nulo	Nulo	Nulo
18	Empleado	Formación académica	Informacion relacionada a la formacion academica del empleado, estudios de pregrado, posgrados, cursos, entre otros.	Recursos Humanos	Nulo	Nulo	Nulo	Nulo	Nulo
19	Empleado	Referencias personales	Informacion relacionada con el o los empleados en cuanto se refiero a contactos en la formacion profesional o academica.	Recursos Humanos	Nulo	Nulo	Nulo	Nulo	Nulo
20	Jurídico	Documentación legal	Documentación relevante sobre el tipo de contrato del cliente y sus normas de cumplimiento legales	Representante Legal	Bajo	Bajo	Nulo	Bajo	Nulo
21	Jurídico	Procesos judiciales	Acción de tutela, acciones públicas populares y acciones de cumplimiento	Representante Legal	Bajo	Bajo	Nulo	Nulo	Bajo
22	Jurídico	Procesos jurídicos	Procesos contencioso administrativo, civiles, laborales y ejecutivos contra y por la entidad.	Representante Legal	Bajo	Bajo	Nulo	Nulo	Bajo
23	Documentación del sistema	Registros logs clientes	Documentación con la información de los registros Logs de cada cliente referente a sus sistemas instalados proporcionados por la organización.	Gerente Sistemas, Gerente de Soporte	Bajo	Bajo	Nulo	Bajo	Bajo
24	Documentación del sistema	Inventario de servidores	Documentación con la característica de cada servidor de la organización.	Gerente Sistemas, Gerente de Soporte	Nulo	Nulo	Nulo	Medio	Bajo
25	Documentación del sistema	Inventario de licencias	Documentación con las características de las licencias de software de la organización.	Gerente Sistemas, Gerente de Soporte	Nulo	Nulo	Nulo	Medio	Bajo
26	Documentación del sistema	Documentación Storage de la organización	Información relacionada con el Storage propio de la organización.	Gerente Sistemas, Gerente de Soporte	Nulo	Bajo	Nulo	Bajo	Bajo
27	Documentación del sistema	Documentación Backup de la organización	Información relacionada con el respaldo de los sistemas de información propio de la organización.	Gerente Sistemas, Gerente de Soporte	Medio	Medio	Medio	Alto	Alto
28	Documentación del sistema	Información del servidor de correo	Información relacionada con la información del servidor de correo electrónico de la organización.	Gerente de sistemas	Alto	Medio	Alto	Alto	Alto
29	Documentación del sistema	Información de accesos al servidor de desarrollo	Información relacionada con la información del servidor de desarrollo de sistemas informáticos de la organización.	Gerente de sistemas	Medio	Medio	Bajo	Alto	Medio
30	Documentación del sistema	información de accesos al servidor de pruebas	Información relacionada con la información del servidor de prueba de sistemas informáticos de la organización.	Gerente de sistemas	Medio	Medio	Medio	Nulo	Bajo

Figura 13 Clasificación de los tipos de Información

1.4.1. Conclusión Tipos de información

En base a los resultados obtenidos mediante la clasificación de los tipos de información de la organización ABC, se obtuvo los índices de criticidad de cada uno de ellos, esto permitirá identificar de cierta forma que tipos de información

están relacionados con los activos de información más críticos de la organización.

1.5. Identificación de activos críticos

La identificación de los activos críticos va de la mano con los tipos de información identificados de la organización. Un activo de información crítico basado en el estándar de la ISO27001 nos indica que es un bien que la organización valora y por esta razón se debe proteger, minimizando sus vulnerabilidades y debilidades. (Estupiñan, Pulido, & Jaime, 2013)

La realización de la matriz que permite identificar los activos críticos de información está basada en conjunto al modulador de criticidad de la entidad, esto permitirá obtener resultados con mayor exactitud contribuyendo posteriormente a la evaluación de riesgos. A continuación, en la Tabla 1 se observa el modulador usado para la calificación de la criticidad de las entidades evaluadas.

Tabla 1 Modulador activos críticos de información.

Valor		Criterio
Alto	Entre 4 a 5	Daño muy grave
Medio	Entre 3 a 4	Daño importante
Bajo	Entre 2 a 3	Daño menor
Nulo	Entre 1 a 2	Daño irrevelante

En las siguientes tablas se podrá observar los activos de información identificados en el transcurso del análisis e inspección a la organización ABC.

Tabla 2 Activo de información 1.

No Activo	Nombre Activo	Formato Activo	Nombre del Tipo de Información	Definición del tipo de Información	Criticidad Entidad	Propietario	Criticidad Activo
1	CRM	Digital	Ordenes de trabajo	Documentación pertinente a los trabajos realizados como su información de registro de horas atendidas y asignación de personal	Nulo	Gerente Soporte	Nulo
			Actas de instalación y soporte	Actas de reunión realizadas con los clientes en base a las ordenes de instalación y soporte	Nulo	Gerente Soporte	
			Informes incidentes	Informe de incidentes previos con los clientes	Nulo	Gerente Sistemas, Gerente de Soporte	
			Informe de instalación	Informes de instalación de IT	Nulo	Gerente Sistemas, Gerente de Soporte	
			Informe de inspección	Informes de inspección a clientes	Nulo	Gerente Sistemas, Gerente de Soporte	
			Diseños técnicos	Documentos correspondiente a los diseños de arquitectura de IT hacia los clientes	Nulo	Gerente Soporte	
			Información del cliente	Datos de información básicos sobre el cliente donde se puede encontrar datos como: Razón social, RUC, Contactos	Nulo	Financiero	
			Posicionamiento financiero	Información relacionada con los estados financieros del cliente como tambien su nivel de venta y patrimonios	Bajo	Financiero	
			Estrategia comercial	Acciones que pone en práctica el cliente para dar a conocer un nuevo producto, para aumentar su cuota de venta o de participación de mercado.	Nulo	Analista Financiero, Marketing	
			Registros logs clientes	Documentación con la información de los registros Logs de cada cliente referente a sus sistemas instalados proporcionados por la organización.	Bajo	Gerente Sistemas, Gerente de Soporte	

Tabla 3 Activo de información 2.

2	ERP	Digital	Proveedores	Documentación acorde a los contratos con los proveedores	Nulo	Gerente Sistemas	Nulo
			Partner	Documentación pertinente a los convenios con Partners	Nulo	Gerente Sistemas	
			Investigación y Desarrollo	Información que nos permita identificar avances en desarrollos de productos del cliente	Nulo	Financiero	
			Descripción laboral	Informacion relacionada que describa acerca del empleado y sus funciones.	Bajo	Recursos Humanos	
			Información médica	Informacion relacionada al estado de salud y en la condicion que se encuentra el o los empleados.	Nulo	Recursos Humanos	
			Seguro social	Toda informacion relacionada y necesaria al seguro social (IESS).	Nulo	Recursos Humanos	
			Ámbito financiero	Informacion relacionada a un metodo donde el o los empleados puedan tener acceso a su remuneracion laboral.	Nulo	Recursos Humanos	
			Experiencia laboral	Informacion relacionada a la experiencia laboral que ha ejercido el empleado.	Nulo	Recursos Humanos	
			Formación académica	Informacion relacionada a la formacion academica del empleado, estudios de pregrado, posgrados, cursos, entre otros.	Nulo	Recursos Humanos	
			Referencias personales	Informacion relacionada con el o los empleados en cuanto se refiero a contactos en la formacion profesional o academica.	Nulo	Recursos Humanos	
			Documentación legal	Documentación relevante sobre el tipo de contrato del cliente y sus normas de cumplimiento legales	Nulo	Representante Legal	
			Procesos judiciales	Acción de tutela, acciones públicas populares y acciones de cumplimiento	Bajo	Representante Legal	
			Procesos jurídicos	Procesos contencioso administrativo, civiles, laborales y ejecutivos contra y por la entidad.	Bajo	Representante Legal	
			Información de accesos al servidor de desarrollo	Información relacionada con la información del servidor de desarrollo de sistemas informáticos de la organización.	Medio	Gerente Sistemas	
			información de accesos al servidor de pruebas	Información relacionada con la información del servidor de prueba de sistemas informáticos de la organización.	Bajo	Gerente Sistemas	

Tabla 4 Activo de información 3.

3	Servidor CORE	Digital	Ordenes de trabajo	Documentación pertinente a los trabajos realizados como su información de registro de horas atendidas y asignación de personal	Nulo	Gerente Soporte	Alto
			Actas de instalación y soporte	Actas de reunión realizadas con los clientes en base a las ordenes de instalación y soporte	Nulo	Gerente Soporte	
			Informe de inspección	Informes de inspección a clientes	Nulo	Gerente Soporte	
			Inventario de servidores	Documentación con la característica de cada servidor de la organización.	Bajo	Gerente Sistemas, Gerente de Soporte	
			Inventario de licencias	Documentación con las características de las licencias de software de la organización.	Bajo	Gerente Sistemas, Gerente de Soporte	
			Documentación Storage de la organización	Información relacionada con el Storage propio de la organización.	Bajo	Gerente Soporte	
			Documentación Backup de la organización	Información relacionada con el respaldo de los sistemas de información propio de la organización.	Alto	Gerente Soporte	
			Información del servidor de correo	Información relacionada con la información del servidor de correo electrónico de la organización.	Alto	Gerente Sistemas	
			Información de accesos al servidor de desarrollo	Información relacionada con la información del servidor de desarrollo de sistemas informáticos de la organización.	Medio	Gerente Sistemas	
			información de accesos al servidor de pruebas	Información relacionada con la información del servidor de prueba de sistemas informáticos de la organización.	Bajo	Gerente Sistemas	

Tabla 5 Activo de información 4.

4	Servidor WEB	Digital	Informe de instalación	Informes de instalación de IT	Nulo	Gerente Soporte	Alto
			Informe de inspección	Informes de inspección a clientes	Nulo	Gerente Soporte	
			Información del cliente	Datos de información básicos sobre el cliente donde se puede encontrar datos como: Razón social, RUC, Contactos	Nulo	Financiero	
			Investigación y Desarrollo	Información que nos permita identificar avances en desarrollos de productos del cliente	Nulo	Financiero	
			Documentación Storage de la organización	Información relacionada con el Storage propio de la organización.	Bajo	Gerente Soporte	
			Documentación Backup de la organización	Información relacionada con el respaldo de los sistemas de información propio de la organización.	Alto	Gerente Sistemas	
			Información del servidor de correo	Información relacionada con la información del servidor de correo electrónico de la organización.	Alto	Gerente Sistemas	
			Información de accesos al servidor de desarrollo	Información relacionada con la información del servidor de desarrollo de sistemas informáticos de la organización.	Medio	Gerente Sistemas	
			información de accesos al servidor de pruebas	Información relacionada con la información del servidor de prueba de sistemas informáticos de la organización.	Bajo	Gerente Sistemas	

Tabla 6 Activo de información 5.

5	Servidor App	Digital	Investigación y Desarrollo	Información que nos permita identificar avances en desarrollos de productos del cliente	Nulo	Financiero	Alto
			Registros logs clientes	Documentación con la información de los registros Logs de cada cliente referente a sus sistemas instalados proporcionados por la organización.	Bajo	Gerente Sistemas, Gerente de Soporte	
			Documentación Storage de la organización	Información relacionada con el Storage propio de la organización.	Bajo	Gerente Soporte	
			Documentación Backup de la organización	Información relacionada con el respaldo de los sistemas de información propio de la organización.	Alto	Gerente Soporte	
			Información del servidor de correo	Información relacionada con la información del servidor de correo electrónico de la organización.	Alto	Gerente Sistemas	
			Información de accesos al servidor de desarrollo	Información relacionada con la información del servidor de desarrollo de sistemas informáticos de la organización.	Medio	Gerente Sistemas	
			información de accesos al servidor de pruebas	Información relacionada con la información del servidor de prueba de sistemas informáticos de la organización.	Bajo	Gerente Sistemas	

Tabla 7 Activo de información 6.

6	Sistema de archivos	Digital	Ordenes de trabajo	Documentación pertinente a los trabajos realizados como su información de registro de horas atendidas y asignación de personal	Nulo	Gerente Soporte	Nulo
			Actas de instalación y soporte	Actas de reunión realizadas con los clientes en base a las ordenes de instalación y soporte	Nulo	Gerente Soporte	
			Informe de instalación	Informes de instalación de IT	Nulo	Gerente Soporte	
			Proveedores	Documentación acorde a los contratos con los proveedores	Nulo	Gerente Sistemas	
			Diseños técnicos	Documentos correspondiente a los diseños de arquitectura de IT hacia los clientes	Nulo	Gerente Soporte	
			Información del cliente	Datos de información básicos sobre el cliente donde se puede encontrar datos como: Razón social, RUC, Contactos	Nulo	Financiero	
			Investigación y Desarrollo	Información que nos permita identificar avances en desarrollos de productos del cliente	Nulo	Financiero	
			Documentación legal	Documentación relevante sobre el tipo de contrato del cliente y sus normas de cumplimiento legales	Nulo	Representante Legal	
			Procesos judiciales	Acción de tutela, acciones públicas populares y acciones de cumplimiento	Bajo	Representante Legal	
			Procesos jurídicos	Procesos contencioso administrativo, civiles, laborales y ejecutivos contra y por la entidad.	Bajo	Representante Legal	
			Inventario de servidores	Documentación con la característica de cada servidor de la organización.	Bajo	Gerente Sistemas, Gerente de Soporte	
			Inventario de licencias	Documentación con las características de las licencias de software de la organización.	Bajo	Gerente Sistemas, Gerente de Soporte	
			Documentación Storage de la organización	Información relacionada con el Storage propio de la organización.	Bajo	Gerente Sistemas	

Tabla 8 Activo de información 7.

7	Servidor de reportes	Digital	Ordenes de trabajo	Documentación pertinente a los trabajos realizados como su información de registro de horas atendidas y asignación de personal	Nulo	Gerente Soporte	Nulo
			Actas de instalación y soporte	Actas de reunión realizadas con los clientes en base a las ordenes de instalación y soporte	Nulo	Gerente Soporte	
			Informes incidentes	Informe de incidentes previos con los clientes	Nulo	Gerente Soporte	
			Informe de instalación	Informes de instalación de IT	Nulo	Gerente Soporte	
			Informe de inspección	Informes de inspección a clientes	Nulo	Gerente Soporte	
			Registros logs clientes	Documentación con la información de los registros Logs de cada cliente referente a sus sistemas instalados proporcionados por la organización.	Bajo	Gerente Sistemas, Gerente de Soporte	

1.5.1. Conclusión Activos de información

Como podemos observar a lo largo de las matrices los activos de información contienen información de vital importancia para el giro de negocio de la organización ABC, sin embargo, podemos apreciar en la Tabla 4 que el activo de información es uno de los más críticos. Para la continuación de este programa de seguridad de la información se seleccionará este activo crítico de información

con base en que los tipos de información que contiene son de alta importancia para la organización.

1.6. Desarrollo de Políticas de Alto Nivel

El desarrollo de políticas de alto nivel permite al programa alinear los objetivos de mitigación de vulnerabilidades en base a los riesgos obtenidos durante el análisis de los activos críticos de la organización. Una correcta calificación de la política permitirá a la organización tomar en cuenta la fortaleza de la misma.

A continuación, en la Tabla 9 se indica un extracto de uno de los riesgos identificados para el activo en análisis y sus correspondientes políticas de alto nivel. La matriz completa se podrá encontrar en los ANEXOS.

Tabla 9 Políticas de Alto Nivel

Nombre Activo	Riesgos	Objetivo	Código actividad	Política de Alto Nivel	Calificación
Servidor CORE	Escapes de información	El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.	A16.1.1.1	Crear un documento de responsabilidades y procedimientos en gestión de incidentes.	Alto
			A16.1.2.1	Documentar la notificación de los eventos de seguridad de la información para que la directiva esté al tanto.	Alto
			A16.1.3.1	Notificar al personal del área técnica sobre los puntos débiles de la seguridad para de esa manera poder documentarlos e implementar mejoras.	Alto
			A16.1.4.1	Implementar la evaluación y decisión sobre los eventos de seguridad de información.	Alto
			A16.1.5.1	Tener una respuesta efectiva a incidentes de seguridad de la información, documentando y notificando a la directiva.	Alto
			A16.1.6.1	Implementar un ciclo de aprendizaje de los incidentes de seguridad de la información.	Alto
			A16.1.7.1	Implementar un método de recopilación de evidencias.	Alto

1.6.1. Conclusión

Podemos concluir que el desarrollo de políticas de Alto nivel va ligado directamente del análisis de vulnerabilidades sobre los activos de información de

la organización. La implementación de las políticas permitirá a la organización alinear sus objetivos con base a los riesgos identificados.

1.7. Modelo Operacional del SGSI

El modelo operacional permite a la organización mantener definido el conjunto de funciones y categorías que permitirán un enfoque en los objetvos planteados para la ejecución del programa de seguridad de la información. Una identificación clara y concisa de los pasos a seguir para la ejecución es fundamental para alcanzar los objetivos propuestos.

El marco de referencia NIST nos provee de funciones y categorías que son de fácil entendimiento permitiendo gestionar y expresar los riesgos para la seguridad de la información. Este marco de referencia provee de cinco funciones que permiten al programa de seguridad alinear sus objetivos de tal manera que sea sencilla su implementación. (Shen, 2014)

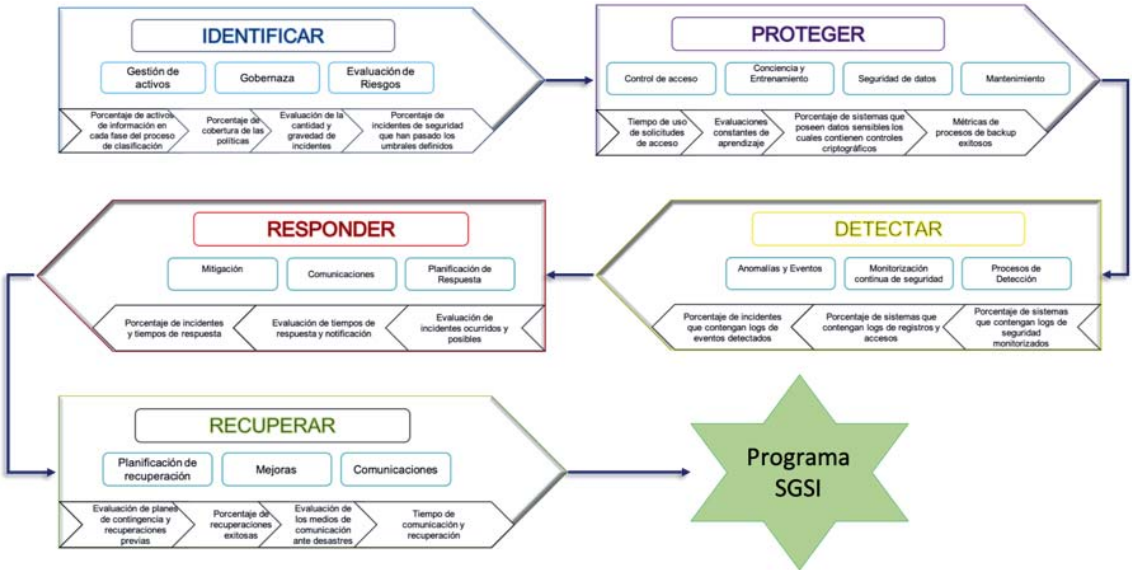

Figura 14 Modelo operacional

Como se observa en la Figura 14 se encuentra el modelo operacional a seguir para la ejecución de este programa de seguridad. Las cinco funciones permitirán un desarrollo de implementación alineada a los objetivos, cada función contiene las categorías identificadas que beneficiarán al programa. Es importante identificar las métricas para cada categoría identificada, las mismas serán de

gran utilidad para calificar el estado de cada uno de estos componentes y conocer el estado de maduración del proceso a lo largo de la implementación del programa de seguridad propuesto.

1.7.1. Conclusión

El desarrollo del modelo operacional y las métricas de los procesos permiten conseguir una correcta alineación de los pasos a implementar para conseguir los objetivos del programa propuesto. Es importante mencionar que las métricas de evaluación para las categorías identificadas son de gran ayuda para la maduración de procesos y actividades que se realizan durante la implementación del programa de seguridad propuesto.

1.8. Evaluación de Riesgos

La evaluación de riesgos es un proceso clave para un correcto programa de seguridad de la información. Este es el proceso mediante el cual la organización indentifica los diversos riesgos de seguridad de la información que posee, permitiendo determinar su probabilidad, impacto y severidad. (Solarte, Rosero, & Benavides, 2015)

La evaluación de riesgos tiene como finalidad permitir a la organización identificar los controles necesarios para mitigar y reducir el riesgo de ocurrencia de los mismos. Estos controles permitirán alimentar a los planes de acción de la organización contribuyendo a un sistema de gestión de la seguridad de la información con mayor robustez. A continuación, se indica en la Tabla 10 y Tabla 11 una adaptación de la matriz propuesta por la metodología MARGERIT para el análisis de la probabilidad e impacto.

Tabla 10 Matriz de probabilidad

Probabilidad	
Raro	2%
Poco probable	5%
Posible	25%
Probable	75%
Casi Certeza	100%

Tabla 11 Matriz de impacto

Impacto	
INSIGNIFICANTE	2%
MENOR	5%
MODERADO	25%
MAYOR	75%
CATASTRÓFICO	100%

Para la evaluación del riesgo inherente de la evaluación de riesgos de la organización cabe recalcar el uso de un mapa de calificación para la severidad de riesgos, el mismo ha sido diseñado con base en el impacto y probabilidad adaptándolo de la metodología MARGERIT. A continuación, se indica en la Tabla 12 el mapa de calificación de severidad de riesgo para la evaluación a realizar.

Tabla 12 Severidad de Riesgo

MAPA DE CALIFICACIÓN SEVERIDAD DE RIESGO						
		IMPACTO				
		INSIGNIFICANTE	**MENOR**	**MODERADO**	**MAYOR**	**CATASTRÓFICO**
Probabilidad	**RARO**	Bajo	Bajo	Moderado	Moderado	Alto
	POCO PROBABLE	Bajo	Bajo	Moderado	Alto	Alto
	POSIBLE	Bajo	Moderado	Moderado	Alto	Crítico
	PROBABLE	Bajo	Moderado	Alto	Crítico	Crítico
	CASI CERTEZA	Moderado	Moderado	Alto	Crítico	Crítico

Para la evaluación de riesgos de la organización se tomará el activo previamente identificado como crítico. El análisis de la evaluación de riesgo del activo contempla el uso de salvaguardas proporcionadas por MARGERIT, las mismas serán adaptadas como se puede observar en la *Figura 15*.

Nombre Activo	Tipo Activo	Criticidad del Activo	Propietario	Procesos	Componente	Salvaguardas
Servidor CORE	Digital	Alto	Gerente Sistemas, Gerente de Soporte	Integración de servicios e infraestructura	Base de datos	H.IA Identificación y autenticación. H.IR Gestión de incidencias. H.tools Herramientas de seguridad. H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión. H.tools.TM Herramienta de monitorización de tráfico. D Protección de la Información. D.A Copias de seguridad de los datos (backup). D.C Cifrado de la información. K Gestión de claves criptográficas. S.A Aseguramiento de la disponibilidad. S Protección de los Servicios. BC.DRP Plan de Recuperación de Desastres (DRP).

Figura 15 Evaluación de riesgos - Parte 1

Las amenazas, vulnerabilidades, impacto y riesgo inherente completos de la organización se pueden encontrar en los ANEXOS del documento, a continuación, en la Figura 16 se indican las amenzas que poseen un riesgo inherente con severidad Alta.

Amenazas	Vulnerabilidades	Impacto	Riesgo Inherente		
			Impacto	Probabilidad	Severidad
[N] Desastres naturales	No existe un DRP asociado a desastres naturales. El personal no está especializado ante un desastre natural. Las copias de seguridad no tienen una frecuencia a corto plazo. Los sistemas no cuentan con una ruta backup para las comunicaciones.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional.	CATASTRÓFICO	RARO	Alto
[E.4] Errores de configuración	El personal no tiene la suficiente especialización para la configuración de los sistemas e integración de los mismos. Las copias de seguridad no tienen una frecuencia a corto plazo. No hay una correcta gestión de cambio en los sistemas integradores.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional. Demandas judicial, afectación Legal.	CATASTRÓFICO	RARO	Alto
[E.14] Escapes de información	La cultura de aprendizaje a los usuarios no es muy efectiva. No existe una correcta manipulación de la información. Los sistemas no cuentan con un software para mitigar el uso de BYOD.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional. Demandas judicial, afectación Legal. Afectación al clima laboral.	MAYOR	POCO PROBABLE	Alto
[E.21] Errores de mantenimiento / actualización de programas (software)	No hay una correcta gestión de cambio en los sistemas integradores. No existe un protocolo en caso de fallo durante un mantenimiento en los programas. Las copias de seguridad no tienen una frecuenca a corto plazo. Los sistemas no cuentan con una ruta backup para las comunicaciones.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional. Demandas judicial, afectación Legal.	CATASTRÓFICO	POCO PROBABLE	Alto
[E.24] Caída del sistema por agotamiento de recursos	No hay un correcto uso de los canales de distribución de procesos. No hay una correcta asignación de recursos a los sistemas. No hay personal especializado para distribución y dimensionamiento de aplicativos.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional. Demandas judicial, afectación Legal. Afectación al clima laboral.	CATASTRÓFICO	POCO PROBABLE	Alto
[A.4] Manipulación de la configuración	No se cuenta con un correcto control de roles a los usuarios. No hay una correcta gestión de cambio en los sistemas integradores. Las copias de seguridad no tienen una frecuencia a corto plazo. No hay un software de registro de accesos.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional. Demandas judicial, afectación Legal.	CATASTRÓFICO	RARO	Alto
[A.11] Acceso no autorizado	No hay un software de registro de accesos. No se cuenta con un correcto control de roles a los usuarios. No hay una correcta gestión de cambio en los sistemas integradores. Las copias de seguridad no tienen una frecuencia a corto plazo. No existe una correcta manipulación de la información. Los sistemas no cuentan con un software para mitigar el uso de BYOD. La cultura de aprendizaje a los usuarios no es muy efectiva.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional. Demandas judicial, afectación Legal. Afectación al clima laboral.	CATASTRÓFICO	RARO	Alto
[A.6] Abuso de privilegios de acceso	No hay un software de registro de accesos. No se cuenta con un correcto control de roles a los usuarios. No hay una correcta gestión de cambio en los sistemas integradores. Las copias de seguridad no tienen una frecuencia a corto plazo. No existe un compromiso de confidencialidad especifico para cada sistema.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional. Demandas judicial, afectación Legal. Afectación al clima laboral.	CATASTRÓFICO	RARO	Alto

Figura 16 Evaluación de riesgos - Parte 2

Con las amenzas identificadas y su riesgo inherente se puede continuar el análisis para determinar los controles a implementar. Los objetivos de control nos permitirán planificar e identificar las mitigaciones a implementar mediante actividades, estas actividades se pueden calificar para obtener un indice de fortaleza del control. La fortaleza de control permite evaluar si el control mitigará los riesgos evaluados. A continuación, en la Figura 17 se indican los controles identificados en base a los riesgos obtenidos previamente los cuales cuentan con una fortaleza de control Alta.

Objetivo de Control	Controles	Tipo de Control	Clasificación de Control	Frecuencia de Control	Fortaleza de Control
Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional.	Identificar los posibles escenarios de desastres naturales posibles en la ubicación de la organización.	Manual	Preventivo	Anual	Alto
Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional. Mitigar posibles demandas judiciales, afectación Legal.	Identificar si las comunicaciones cuentan con rutas alternas. Verificar si las comunicaciones cuentan con directrices pre establecidas para tolerancia a fallos.	Manual	Preventivo Detectivo	Mensual	Alto
Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la afectación al clima laboral.	Identificar los roles asociados a cada usuario. Verificar si las políticas del servidor están anexadas a los usuarios activos.	Automático	Detectivo	Mensual	Alto
Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional. Mitigar posibles demandas judiciales, afectación Legal.	Identificar la integridad de los logs del servidor. Verificar la lista de control de acceso al servidor.	Manual	Detectivo	Mensual	Alto
Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional. Mitigar posibles demandas judiciales, afectación Legal. Mitigar la afectación al clima laboral.	Identificar si los cambios en la información realizados en el servidor cuentan con respaldo en la lista de control de acceso y logs.	Automático	Preventivo Detectivo	Mensual	Alto
Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional. Mitigar posibles demandas judiciales, afectación Legal. Mitigar la afectación al clima laboral.	Verificar que el servidor cuente con los recursos necesarios para un funcionamiento eficaz.	Automático	Preventivo Detectivo	Trimestral	Alto
Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional. Mitigar posibles demandas judiciales, afectación Legal.	Identificar las listas de control de acceso al servidor. Verificar que los logs de configuración esten correctamente respaldados y contengan información periódica.	Manual	Preventivo	Mensual	Alto
Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional. Mitigar posibles demandas judiciales, afectación Legal. Mitigar la afectación al clima laboral.	Identificar que el acceso al servidor sea bajo normas y directrices previamente aprobadas y supervisadas.	Automático	Preventivo Detectivo	Mensual	Alto
Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional. Mitigar posibles demandas judiciales, afectación Legal. Mitigar la afectación al clima laboral.	Identificar que las actividades realizadas en el servidor cuenten con un registro en los logs de acceso. Identificar que las actividades realizadas sean realizadas por los administradores del servidor.	Automático	Preventivo Detectivo	Mensual	Alto

Figura 17 Objetivos de Control

Las actividades por implementar en los controles y la matriz completa de controles se la pueden encontrar en los ANEXOS.

1.8.1. Conclusión

Con base en los resultados obtenidos podemos apreciar que los riesgos que presenta la organización son de alta severidad, sin embargo es importante recalcar que la identificación de las amenzas permite al programa mitigar las mismas mediante planes de acción y actividades que se proponen a lo largo del presente programa de seguridad de la información.

1.9. Roadmap de Planes de Acción

Elaborar un plan de acción o roadmap es un paso importante en el programa de seguridad de la información pues nos permite estar listos para la implementación. Es importante tomar en cuenta que el plan de acción esta alimentado por los controles obtenidos a lo largo del análisis de amenazas y las actividades de mejora obtenidos durante la evaluación del estado actual del sistema de gestión de seguridad de la información de la organización. (Yasin, Arman, Edward, & Shalannanda, 2020)

La elaboración del roadmap para este programa de seguridad de la información está compuesto por los códigos de aplicación, las actividades o acciones a implementar, el responsable de la ejecución, costo de la ejecución, estado de la acción y por último el tiempo de ejecución. El tiempo de ejecución se encuentra divido en cuatro partes, las mismas han sido analizadas en conjunto con la organización para una implementación segmentada.

A continuación en la se puede apreciar un extracto del plan de acción a seguir para la implementación de este programa de seguridad de la información. La matriz completa se puede encontrar en los ANEXOS.

Tabla 13 Extracto del plan de acción

Código	Acción	Responsable	Costo	Q1	Q2	Q3	Q4	Estado
PA1	Definir y acordar con todas las partes interesadas los objetivos del SGSI precautelando su eficacia durante la implementación.	Gerente Sistemas	Tiempo laboral	x				N/A
PA2	Analizar e identificar los factores internos y externos (obligaciones legales, regulatorias y contractuales), así como las tendencias en el entorno de negocio que pueden influir en el programa.	Gerente Sistemas	Tiempo laboral	x	x			N/A
PA3	Analizar los diversos requerimientos obtenidos, madurar cada requerimiento conforme a las obligaciones que competen al mismo.	Coordinador Sistemas	Tiempo laboral	x	x	x	x	N/A
PA4	Evaluar y determinar directrices para el cumplimiento del alcance propuesto.	Gerente Sistemas	Tiempo laboral	x				N/A
PA5	Validar y ejecutar el programa propuesto en la organización permitiendo de esta forma obtener un programa SGSI acorde a las necesidades de la empresa.	Gerente Sistemas	Tiempo laboral	x				N/A

1.9.1. Conclusión

El plan de acción propuesto permite a la organización mantener alineados sus objetivos a lo largo de este programa de seguridad de la información, un análisis constante de las amenazas y vulnerabilidades permitirá obtener actividades de mejora continua que ayuden al programa a mantener mejoras continuas.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- El desarrollo de este sistema de gestión de seguridad de la información permitió identificar grandes falencias en la organización evaluada, estas brechas de seguridad han sido identificadas a lo largo de la información recabada y permitiendo a la organización contemplar sus activos de información y clasificar los tipos de información que poseen.
- La identificación y clasificación de los activos de información en la organización han permitido a la organización priorizar la ejecución del programa propuesto, el valor de la información identificada es de vital importancia para la organización por esta razón se ha tomado medidas estricta y necesarias para la maduración de los procesos de seguridad que actualmente posee la organización.
- El uso de marcos de referencia han aportado en gran medida en el desarrollo de este programa de seguridad, la adaptación de estos marcos y la experiencia de los participantes son de gran importancia para la alineación de los objetivos propuestos.
- Los planes de acción propuestos permiten a la organización obtener buenas prácticas y consigo desminuir las brechas de seguridad identificadas durante los análisis realizados, es por esta razón que un correcto análisis inicial en conjunto con el levantamiento de riesgos y vulnerabilidades nos darán como resultado actividades que permitan madurar los procesos de seguridad de la organización.

Recomendaciones

- Es importante contar con las actualizaciones de los marcos de referencia que se usa durante el análisis e identificación de los objetivos de control, cabe recalcar que en cada actualización de los marcos de referencia podemos encontrar mejores prácticas que contribuiran con la alineación de los objetivos.

- La identificación constante de los activos de información es de suma importancia, día a día las organizaciones resguardan mayor cantidad de información a lo largo de sus procesos internos y externos, es por esta razón que una actualización constante de los activos e identificación de vulnerabilidades ayudarán a las organizaciones mantener sus brechas de seguridad lo más cerradas posibles.
- La adaptación de los marcos de referencia en base a las organizaciones es un paso vital para un análisis con mayor efectividad, los marcos de referencia permiten obtener buenas prácticas durante los análisis sin embargo las exigencias de las organizaciones se deben ajustar a un marco adaptativo donde contemplen las necesidades de la organización.

REFERENCIAS

Brenner, J. (Enero de 2007). ISO 27001 risk management and compliance. *Risk Management(Vol. 54, Issue 1)*. Obtenido de https://link.gale.com/apps/doc/A157587924/AONE?u=anon~c46883db&sid=googleScholar&xid=6deeb54b

Estupiñan, A. d., Pulido, J. A., & Jaime, J. A. (2013). Análisis de riesgos en seguridad de la información. En *Ciencia, Innovación Y Tecnología* (págs. 40-53). Juan D Castellanos.

ISOTools. (2021). *Software ISO Riesgos y Seguridad*. Obtenido de https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Ladino, M., Villa, P., & López, A. (2011). *Fundamentos de iso 27001 y su aplicación en las empresas.* Scientia Et Technica.

Shen, L. (2014). *The NIST cybersecurity framework: Overview and potential impacts.* Scitech Lawyer.

Solarte, F. N., Rosero, E. R., & Benavides, M. d. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica - ESPOL*.

Sosa, J. (2012). *Clasificación de la Información.*

Yasin, M., Arman, A. A., Edward, I. J., & Shalannanda, W. (2020). *Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ)*. Obtenido de IEEE: https://ieeexplore.ieee.org/abstract/document/9310875

ANEXOS

Anexo 1: Estado de implementación ISO27001: Anexo A

A5	**Políticas de seguridad de la información**					
A5.1	**Directrices de gestión de la seguridad de la información**					
A5.1.1	Políticas para la seguridad de la información	Inicial	La organización cuenta con diversas políticas de seguridad de la información, basadas en criterio del personal técnico.	A5.1.1.1	Alinear la gestión de identidades y derechos de acceso con los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad-de-tener y necesidad-de-conocer.	Alto
A5.1.2	Revisión de las políticas para la seguridad de la información	Inicial	La organización cuenta con una revisión trimestral de sus políticas de seguridad de la información llevada a cabo por su personal técnico.	A5.1.1.2	Determinar un periodo constante de revisión de políticas con la finalidad de conocer y prevenir vulnerabilidades y/o amenazas.	Alto
A6	**Organización de la seguridad de la información**					
A6.1	**Organización interna**					
A6.1.1	Roles y responsabilidades en seguridad de la información	Inicial	La organización cuenta con personas capacitadas que conocen cuales son sus	A6.1.1.1	Establecer, acordar y comunicar los roles y responsabilida	Alto

			roles, basadas en el criterio del personal técnico de la empresa		des relacionadas con I&T a todo el personal de la empresa, de acuerdo con las necesidades y objetivos de la empresa	
A6.1.2	Segregación de tareas	Inicial	Se segregan tareas de acuerdo con la necesidad que se tenga en ese momento en el área técnica	A6.1.2.1	Asignar roles para actividades sensibles para que haya una clara segregación de funciones.	Alto
A6.1.3	Contacto con las autoridades	Inicial	El personal mantiene el contacto con las autoridades de la empresa de una forma directa para situaciones relacionadas a la misma	A6.1.3.1	Establecer una comunicación formal con las autoridades de la empresa, documentando las comunicaciones con la finalidad de tener respaldos de las acciones tomadas en caso de necesitarlo.	Alto
A6.1.4	Contacto con grupos de interés especial	Medio	La organización cuenta con un contacto formalizado con grupos de interés especial mediante medios electrónicos.	A6.1.4.1	Mantener un contacto con grupos de interés manejando procedimientos previamente establecidos para de esa manera documentar	Alto

					de una mejor manera todo lo que se lleva a cabo en la empresa.	
A6.1.5	Seguridad de la información en la gestión de proyectos	Inicial	La organización cuenta con diversas políticas de seguridad de la información, basadas en criterio del personal técnico para la gestión de proyectos.	A6.1.5.1	Mantener y hacer cumplir una estrategia estándar de gestión de proyectos, alineada con el entorno específico de la empresa y con las buenas prácticas, conforme a procesos definidos y al uso de la tecnología correcta, aplicando diversas políticas de seguridad de la información.	Alto
A6.2	**Los dispositivos móviles y el teletrabajo**					
A6.2.1	Política de dispositivos móviles	Inicial	La organización cuenta con una política de distribución y entrega de dispositivos móviles para los empleados para su uso interno.	A6.2.1.1	Mantener documentación formal en donde se indique los dispositivos móviles entregados a las diferentes personas de la organización, dejando en claro las condiciones	Alto

					para el uso del equipo en cuestión.	
A6.2.2	Teletrabajo	Medio	La organización cuenta con un control interno de la realización de actividades diarias relacionadas a las diferentes áreas de trabajo.	A6.2.2.1	Tener documentados los accesos de cada persona de la organización y mantener un control remoto de las actividades de los miembros de la organización con la finalidad de dar un buen uso al tiempo y recursos.	Alto
A7	**Seguridad relativa a los recursos humanos**					
A7.1	**Antes del empleo**					
A7.1.1	Investigación de antecedentes	Medio	La organización cuenta con una investigación de antecedentes, donde se piden certificados de las entidades respectivas y de esa manera el departamento de TTHH realiza la verificación respectiva de la información.	A7.1.1.1	Incluir verificaciones de antecedentes en el proceso de contratación de TI para empleados, contratistas y terceros. El alcance y frecuencia de estas verificaciones debe depender de la sensibilidad	Optimizado

					y/o criticidad de la función.	
A7.1.2	Términos y condiciones del empleo	Alto	La organización cuenta con documentación formal en donde se indican los términos y condiciones del empleo.	A7.1.2.1	Proporciona directrices para la gestión de contratos (p. ej., términos y condiciones, supervisión de contratos).	Optimizado
A7.2	**Durante el empleo**					
A7.2.1	Responsabilidades de gestión	Inicial	La organización cuenta con responsabilidades de gestión asignados por el personal técnico.	A7.2.1.1	Considerar y definir claramente los roles las responsabilidades de todas las partes involucradas	Alto
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Inicial	La organización cuenta con Concienciación, educación y capacitación en seguridad de la información en el área técnica	A7.2.2.1	Realizar formación sobre concienciación de la seguridad de la información de forma regular a todo el personal de la empresa.	Alto
A7.2.3	Proceso disciplinario	Alto	La organización cuenta con un proceso disciplinario riguroso a ser aplicado según sea el caso.	A7.2.3.1	Implementar y comunicar un proceso disciplinario, dando a conocer a todos los empleados de la organización.	Optimizado

A7.3	**Finalización del empleo o cambio en el puesto de trabajo**					
A7.3.1	Responsabilidades ante la finalización o cambio	Medio	La organización sabe como actuar en caso de finalización del empleo o cambios en el puesto de trabajo.	A7.3.1.1	Capacitar al personal de manera regular, sobre los pasos a seguir y responsabilidades que conlleva la finalización del empleo o cambios en el puesto de trabajo	Alto
A8	**Gestión de activos**					
A8.1	**Responsabilidad sobre los activos**					
A8.1.1	Inventario de activos	Alto	La organización cuenta con un inventario actualizado de los activos, permitiendo así mantener un control estricto de los mismos.	A8.1.1.1	Mantener un inventario de información (sistemas y datos) que incluyan una lista de Dueños, custodios y clasificaciones. Incluir sistemas que sean externalizados y aquellos cuya propiedad debería estar dentro de la empresa	Optimizado
A8.1.2	Propiedad de los activos	Alto	La organización cuenta con un registro de la propiedad de los activos, mismos que	A8.1.2.1	Revisar periódicamente el registro de propiedad de los activos	Optimizado

			están disponibles por parte del área técnica.		para saber los movimientos que se producen con los mismos y así mantener el registro actualizado.	
A8.1.3	Uso aceptable de los activos	Alto	La organización es consciente del estado debido al uso aceptable de los activos por parte de los trabajadores.	A8.1.3.1	Capacitar al personal de manera periódica con el fin de que los mismos sepan como manipular de manera adecuada los activos de la organización.	Optimizado
A8.1.4	Devolución de activos	Alto	La organización, tiene un procedimiento a seguir para la devolución de activos en el caso de cambio de puesto de trabajo y/o salida de la empresa.	A8.1.4.1	Dar a conocer todo el proceso que se debe seguir al momento de devolución de activos a cada uno de los miembros de la organización, de igual forma capacitar al área técnica para que sepan los pasos correctos a seguir en estos casos	Optimizado
A8.2	**Clasificación de la información**					
A8.2.1	Clasificación de la información	Alto	La organización posee toda la información clasificada,	A8.2.1.1	Proporcionar las directrices para	Optimizado

			siendo accesible para las personas autorizadas.		garantizar la clasificación adecuada y consistente de los elementos de información en toda la empresa	
A8.2.2	Etiquetado de la información	Alto	La organización cuenta con el proceso de etiquetado de información basado en las directrices y aprobaciones de la directiva	A8.2.2.1	Idear e implementar un esquema para gestionar el conocimiento no estructurado que no está disponible a través de fuentes formales.	Optimizado
A8.2.3	Manipulado de la información	Inicial	La organización cuenta con un manipulado de la información inicial.	A8.2.3.1	Proporcionar los accesos necesarios a las personas autorizadas para de esa manera garantizar que la información sea resguardada de manera adecuada y así evitar posible fuga de información.	Alto
A8.3	**Manipulación de los soportes**					
A8.3.1	Gestión de soportes extraíbles	Inexistente	La organización no cuenta con una correcta gestión de soportes extraíbles, la	A8.3.1.1	Implementar un conjunto de directrices y normas basados en los	Alto

			información puede ser manipulada.		sistemas de gestión para el uso adecuado de dispositivos extraíbles, permitiendo de esta manera mitigar la manipulación de la información.	
A8.3.2	Eliminación de soportes	Inexistente	La organización no cuenta con un proceso de eliminación de soportes acorde a lo reglamentado.	A8.3.2.1	Idear e implementar normas de eliminación de soportes aprobados por la directiva de seguridad.	Alto
A8.3.3	Soportes físicos en tránsito	Medio	La organización mantiene el uso de soportes externos en tránsito basados en la nueva era de trabajo asignada (teletrabajo).	A8.3.3.1	Implementar un conjunto de normas que permitan tener un control estricto sobre los soportes físicos que mantiene cada miembro de la organización.	Alto
A9	**Control de acceso**					
A9.1	**Requisitos de negocio para el control de acceso**					
A9.1.1	Política de control de acceso	Alto	La organización cuenta con una política de control de acceso, de esa manera, se garantiza que todas las actividades de los	A9.1.1.1	Implementar una política de control de acceso más moderno para de esa manera aumentar la seguridad de	Optimizado

			trabajadores queden registradas.		la organización.	
A9.1.2	Acceso a las redes y a los servicios de red	Alto	La organización cuenta con acceso a las redes y los servicios de red, por parte del personal técnico.	A9.1.2.1	Dar a conocer quienes son las personas autorizadas a acceder a las redes y los servicios de red para de esa manera garantizar un buen manejo de los recursos.	Optimizado
A9.2	**Gestión de acceso de usuario**					
A9.2.1	Registro y baja de usuario	Alto	El registro y baja de usuarios está correctamente formalizado y aprobado por un comité de la organización.	A9.2.1.1	Identificar el proceso de registro y baja de usuario automatizado, basando en métricas de uso del directorio activo de la organización.	Optimizado
A9.2.2	Provisión de acceso de usuario	Inicial	El provisionamiento temporal de acceso de usuarios no está registrado y no se lleva un control de estos.	A9.2.2.1	Implementar un conjunto de normas para los provisionamientos temporales de acceso basándose en los roles otorgados al mismo.	Alto
A9.2.3	Gestión de privilegios de acceso	Alto	La gestión de privilegios de acceso esta correctamente	A9.2.3.1	Identificar y diseñar un proceso	Optimizado

			formalizado y aprobado por una directiva en base a los roles asignados al individuo.		automatizado de gestión de privilegios basados en el rol de desempeño el mismo deberá ser aprobado por un comité técnico.	
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Alto	La gestión de seguridad de autenticación de usuarios se lleva acorde a los programas de seguridad que mantiene la organización (Azure, office 365, Active Director)	A9.2.4.1	Diseñar un proceso de gestión automática de autenticación de los usuarios, evitando de está manera el contacto directo de claves con el personal técnico.	Optimizado
A9.2.5	Revisión de los derechos de acceso de usuario	Inexistente	La organización no cuenta con una revisión de los derechos de acceso para los usuarios.	A9.2.5.1	Implementar una revisión periódica de los derechos de acceso de los usuarios.	Alto
A9.2.6	Retirada o reasignación de los derechos de acceso	Medio	La organización no tiene un proceso formalizado para la reasignación de los derechos de acceso, los mismos son basados en pedidos no formales de las áreas participes.	A9.2.6.1	Implementar un proceso formalizado de reasignación de derechos de acceso, notificando a los participes y a la directiva sobre los cambios.	Alto
A9.3	**Responsabilidades del usuario**					

A9.3.1	Uso de la información secreta de autenticación	Alto	La organización ha capacitado e informado a cada uno de los usuarios acerca del manejo de la información secreta de autenticación es de responsabilidad propia y bajo ningún concepto transferible.	A9.3.1.1	Implementar un curso de concientización para toda la organización con la finalidad de mostrar de los peligros y riesgos existentes de compartir información secreta de autenticación con terceras personas.	Optimizado
A9.4	**Control de acceso a sistemas y aplicaciones**					
A9.4.1	Restricción del acceso a la información	Alto	La organización cuenta con restricciones aplicadas por el personal técnico, con la finalidad de garantizar que los usuarios accedan solo a información que les compete.	A9.4.1.1	Implementar un mayor nivel de restricciones de acceso a la información para que la misma solo sea accedida por las personas autorizadas y con ello resguardar la información.	Optimizado
A9.4.2	Procedimientos seguros de inicio de sesión	Alto	La organización cuenta con procedimientos seguros de inicio de sesión que es de conocimiento exclusivo de cada uno de los usuarios, de esa manera se puede acceder a los recursos	A9.4.2.1	Capacitar al personal para que los mismos apliquen procedimientos seguros de inicio de sesión, y sean responsables y conscientes	Optimizado

			necesarios para el desempeño de las actividades.		que la información que se reguarda es el activo más importante que existe.	
A9.4.3	Sistema de gestión de contraseñas	Medio	La organización cuenta con un sistema de gestión de contraseñas para acceder a todos los recursos de la empresa, mismos a los cuales están alojados en un servidor y solo tiene acceso el personal técnico.	A9.4.3.1	Proponer una mejora sobre el sistema donde se alojan todas las contraseñas, para de esa manera tener una segunda opción de alojamiento y de esa forma aumentar el nivel de seguridad.	Alto
A9.4.4	Uso de utilidades con privilegios del sistema	Medio	La organización cuenta con el uso de utilidades con privilegios del sistema realizados en base a la experiencia del personal técnico.	A9.4.4.1	Implementar el uso de utilidades con privilegios del sistema y que los mismos sean aprobados por el comité.	Alto
A10	**Criptografía**					
A10.1	**Controles criptográficos**					
A10.1.1	Política de uso de los controles criptográficos	Medio	La organización cuenta con políticas de gestión de los controles criptográficos basados en a la experiencia del personal técnico, el	A10.1.1.1	Implementar un conjunto de normas y directrices para el cambio, renovación y gestión de los	Alto

			proceso no es formalizado ni aprobado por un comité.		controles criptográficos para que puedan ser aprobados y revisados por un comité.	
A10.1.2	Gestión de claves	Medio	La organización cuenta con un proceso de gestión de claves, validado por los técnicos pero no aprobado por una directiva ni correctamente formalizado	A10.1.2.1	Implementar directrices de revisión y aprobación para la correcta gestión de claves de la organización.	Alto
A11	**Seguridad física y del entorno**					
A11.1	**Áreas seguras**					
A11.1.1	Perímetro de seguridad física	Inicial	Los perímetros de seguridad física no están debidamente marcados o son inexistentes.	A11.1.1.1	Se deben implementar perímetros de seguridad física para precautelar la integridad física de todo el personal de la organización y saber como actuar de manera adecuada en caso de emergencia.	Alto
A11.1.2	Controles físicos de entrada	Medio	Se posee con controles físicos de entrada tales cómo: llaves físicas, carnet de identificación,	A11.1.2.1	Se debe modernizar los controles físicos de entrada para de esa manera, tener	Alto

			alarmas, para el ingreso a oficinas.		mayor seguridad y proteger las oficinas de la organización de acceso no autorizado.	
A11.1.3	Seguridad de oficinas, despachos y recursos	Medio	La seguridad de las oficinas, despachos y recursos, pueden ser accedidos por todos los miembros de la organización.	A11.1.3.1	Se debe mejorar la seguridad de oficinas, despachos y recursos para que solo el personal autorizado de cada área pueda acceder a las oficinas según sea la necesidad.	Optimizado
A11.1.4	Protección contra las amenazas externas y ambientales	Inicial	La organización cuenta con protección contra amenazas y ambientales de una manera no documentada ni aprobada por un comité.	A11.1.4.1	Capacitar al personal para que de esa manera sepan como actuar de manera correcta ante las diferentes amenazas externas y ambientales que puedan presentarse.	Alto
A11.1.5	El trabajo en áreas seguras	Medio	La organización cuenta con espacios adecuados para el desempeño de las actividades diarias de todo su personal.	A11.1.5.1	Mejorar la distribución de espacios para que todo el personal de la organización se sienta a gusto en el lugar de trabajo y	Optimizado

					pueda desempeñar sus funciones de manera eficiente y eficaz.	
A11.1.6	Áreas de carga y descarga	Inexistente	La organización no cuenta con área de carga y descarga.	A11.1.6.1	Implementar un área de carga y descarga segura con la finalidad de tener un mejor manejo por parte de todo el personal de la organización.	Alto
A11.2	**Seguridad de los equipos**					
A11.2.1	Emplazamiento y protección de equipos	Alto	Los equipos de la organización se encuentran correctamente localizados en un DataCenter bajo todas las normas y aprobaciones necesarias para su correcto funcionamiento. Los equipos de uso de la organización se mantienen en los hogares de estos basados en el Teletrabajo, pero se ha asignado el uso correcto de ventiladores suministrados por la organización.	A11.2.1.1	Determinar e identificar el correcto uso de los equipos personales de la organización con el fin de evitar daños y mal funcionamiento de los dispositivos.	Alto

A11.2.2	Instalaciones de suministro	Alto	Los equipos personales de los miembros de la organización se encuentran bajo responsabilidad de los usuarios basados en el teletrabajo, cada equipo fue asignado suministros de protección para el uso correcto y preventivo de los equipos.	A11.2.2.1	Determinar el uso del computador e identificar posibles escenarios de falla de los suministros basados en los cuidados que mantiene el miembro de la organización.	Optimizado
A11.2.3	Seguridad del cableado	Medio	Los equipos que se encuentran bajo la modalidad de Teletrabajo cuentan con peligro de seguridad de cableado ya que no se tiene en cuenta el cableado de los hogares de cada miembro de la organización.	A11.2.3.1	Identificar la seguridad del cableado de los hogares y proponer actividades de cambio y mejora para la seguridad de los empleados.	Alto
A11.2.4	Mantenimiento de los equipos	Alto	La organización cuenta con un plan de mantenimiento trimestral de los equipos, aprobado y revisado por una directiva.	A11.2.4.1	Identificar las mejoras potenciales basándose en métricas de productividad y de fallos registrados en los equipos.	Optimizado
A11.2.5	Retirada de materiales propiedad de la empresa	Alto	La organización cuenta con una correcta retirada de materiales propios, una vez dados de baja y revisado por las áreas	A11.2.5.1	Identificar basado en métricas posibles mejoras y alargar los años	Optimizado

			correspondientes.		productivos de los materiales de la empresa.	
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Medio	La organización no cuenta con un seguro para los equipos que se encuentran fuera de la instalación.	A11.2.6.1	Identificar e implementar un seguro para los equipos que se encuentren fuera de las instalaciones, previniendo cualquier tipo de afectación a la organización.	Alto
A11.2.7	Reutilización o eliminación segura de equipos	Medio	La organización cuenta con una correcta eliminación de equipos una vez han sido dados de baja.	A11.2.7.1	Determinar los tiempos de vida útil de los equipos de la organización para permitir una eliminación segura aprobada por la directiva y no de último momento.	Alto
A11.2.8	Equipo de usuario desatendido	Medio	La organización cuenta con políticas para el bloqueo de los equipos desatendidos por un periódo de tiempo, el mismo fue basado en la experiencia del equipo técnico.	A11.2.8.1	Determinar los tiempos de uso de los equipos e implementar una regla para equipos desatendidos basados en métricas y aprobaciones de la directiva.	Optimizado
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Medio	La organización no cuenta con una política de pantalla limpia.	A11.2.9.1	Determinar e implementar políticas de	Alto

					trabajo despejado y pantalla limpia en la organización basándose en el uso de Active Directory	
A12	**Seguridad de las operaciones**					
A12.1	**Procedimientos y responsabilidades operacionales**					
A12.1.1	Documentación de procedimientos operacionales	Medio	La organización cuenta con una correcta documentación de procedimientos operacionales, a seguir por los miembros de la organización.	A12.1.1.1	Determinar todos los procedimientos operacionales a seguir en cada una de las áreas, y que sea de conocimiento de todos los miembros de la organización.	Alto
A12.1.2	Gestión de cambios	Medio	La gestión de cambios en las operaciones se basa en torno a la experiencia del personal técnico.	A12.1.2.1	Identificar e implementar una serie de pasos a seguir en la gestión de cambios de las operaciones y que sea conocido por el personal técnico.	Alto
A12.1.3	Gestión de capacidades	Medio	La gestión de capacidades se basa en torno a la experiencia	A12.1.3.1	Identificar e implementar una serie de pasos a seguir en la gestión	Alto

			del personal técnico.		de capacidades de las operaciones y que sea conocido por el personal técnico.	
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	Alto	La organización cuenta con una separación de los recursos de desarrollo, prueba y operación y han sido aprobados por el comité.	A12.1.4.1	Determinar las diferentes fases con las que cuentan los recursos para que las mismas sean claras y plenamente identificadas por parte del personal técnico de la organización.	Optimizado
A12.2	**Protección contra el software malicioso (malware)**					
A12.2.1	Controles contra el código malicioso	Alto	Todos los ordenadores portátiles de cada uno de los miembros de la organización cuentan con antivirus instalado en cada una de sus máquinas para prevenir malware.	A12.2.1.1	Dar mantenimiento preventivo cada cierto tiempo en cada uno de los ordenadores, ejecutando análisis de malware para de esa manera evitar infecciones de las máquinas y prevenir desastres.	Optimizado
A12.3	**Copias de seguridad**					

A12.3.1	Copias de seguridad de la información	Medio	Considerando que se está en teletrabajo, las copias de seguridad de la información quedan a criterio de cada miembro de la organización.	A12.3.1.1	Elaborar un cronograma bien establecido y generar un registro de las copias de seguridad de la información de cada uno de los miembros de la organización para poder acceder a la información cuando sea requerido.	Alto
A12.4	**Registros y supervisión**					
A12.4.1	Registro de eventos	Inicial	La organización cuenta con un registro de eventos, mismo que es realizado por el personal técnico.	A12.4.1.1	Elaborar un registro de eventos documentado y aprobado por el comité, con la finalidad de saber los eventos que han sucedido por cada uno de los eventos de la organización.	Alto
A12.4.2	Protección de la información del registro	Inicial	La organización cuenta con una protección de la información del registro, mismo que es realizado por	A12.4.2.1	Elaborar un registro de la protección de la información del registro documentado y aprobado por el comité, con la	Alto

			el personal técnico.		finalidad de saber los eventos que han sucedido por cada uno de los eventos de la organización.	
A12.4.3	Registros de administración y operación	Inicial	La organización cuenta con un registro de administración y operación, mismo que es realizado por el personal técnico.	A12.4.3.1	Elaborar un registro de administración y operación documentado y aprobado por el comité, con la finalidad de saber los eventos que han sucedido por cada uno de los eventos de la organización.	Alto
A12.4.4	Sincronización del reloj	Inicial	La organización cuenta con la sincronización del reloj, mismo que es realizado por el personal técnico.	A12.4.4.1	Elaborar un registro de la sincronización del reloj aunque esto no es estrictamente necesario.	Alto
A12.5	**Control del software en explotación**					
A12.5.1	Instalación del software en explotación	Inexistente	La organización no cuenta con software en explotación.	A.12.5.1.1	Se debe instalar software en explotación con la finalidad de poder simular ataques controlados y conocer sobre las	Alto

					vulnerabilidades existentes.	
A12.6	**Gestión de la vulnerabilidad técnica**					
A12.6.1	Gestión de las vulnerabilidades técnicas	Inicial	La organización cuenta con protocolos para vulnerabilidades técnicas, las mismas no han sido documentadas ni aprobadas.	A12.6.1.1	Identificar y analizar la gestión de vulnerabilidades técnicas documentando los procesos y evaluar las acciones en el directivo.	Alto
A12.6.2	Restricción en la instalación de software	Medio	La organización cuenta con limitantes para la instalación de software el mismo es basado en los roles del usuario, no mantiene una documentación ni aprobación	A12.6.2.1	Determinar de mejores maneras los roles y uso de aplicaciones para la limitación de software y permitir basado en métricas la instalación de software de terceros a usuarios con roles administrativos.	Alto
A12.7	**Consideraciones sobre la auditoria de sistemas de información**					
A12.7.1	Controles de auditoría de sistemas de información	Inicial	La organización no cuenta con controles de auditoria de sistemas de información.	A12.7.1.1	Contar con una auditoria de sistemas de información cada cierto tiempo y llevar un registro para	Alto

					su debido control.	
A13	**Seguridad de las comunicaciones**					
A13.1	**Gestión de la seguridad de las redes**					
A13.1.1	Controles de red	Medio	La organización cuenta con controles de red, permitiendo tener identificado las áreas de red y sus accesos.	A13.1.1.1	Documentar los controles de red, creando manuales de control permitiendo tener métricas de evaluación continua.	Alto
A13.1.2	Seguridad de los servicios de red	Medio	La organización cuenta con diversos sistemas de seguridad de los servicios de red, los mismos no han sido documentados pero si aprobados por un comité.	A13.1.2.1	Determinar los responsables de la documentación de la seguridad en los servicios de red para tener una aprobación por parte de un comité e implementar una revisión continua de los mismos.	Alto
A13.1.3	Segregación en redes	Medio	La organización no tiene una segregación de redes definidas, se maneja una segregación básica implementad	A13.1.3.1	Identificar las áreas de red e implementar una nueva segregación permitiendo obtener un control de red mas	Alto

			a desde sus inicios.		transparente y escalable.	
A13.2	**Intercambio de información**					
A13.2.1	Políticas y procedimientos de intercambio de información	Medio	La organización cuenta con políticas y procedimientos de intercambio de información a criterio del personal técnico.	A13.2.1.1	Documentar las políticas y procedimientos de intercambio de información y que esté al alcance de todos los miembros de la organización.	Alto
A13.2.2	Acuerdos de intercambio de información	Medio	La organización cuenta con acuerdos de intercambio de información a criterio del personal técnico.	A13.2.2.1	Documentar los acuerdos de intercambio de información y que esté al alcance de todos los miembros de la organización.	Alto
A13.2.3	Mensajería electrónica	Alto	La organización cuenta con software licenciado destinado exclusivamente para el uso de mensajería electrónica.	A13.2.3.1	Actualizar periódicamente el software de mensajería electrónica más aun ahora que es de uso primordial en la modalidad de teletrabajo.	Optimizado
A13.2.4	Acuerdos de confidencialidad o no revelación	Alto	La organización cuenta con acuerdos de	A13.2.4.1	Capacitar a todo el personal de la organización	Optimizado

			confidencialidad o no revelación y que están al tanto por parte de todos los empleados.		acerca de las consecuencias en caso de romper los acuerdos de confidencialidad o no revelación.	
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**					
A14.1	**Requisitos de seguridad en los sistemas de información**					
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Inicial	La organización no cuenta con un análisis de requisitos para la seguridad de la información pero se ha manejado basado en la experiencia del grupo técnico, estos procedimientos no han sido documentados ni aprobados por un comité.	A14.1.1.1	Identificar los requisitos y especificaciones de la seguridad de la información basándose en normas orientadas a las buenas prácticas, documentado el proceso y verificando los mismos con un comité.	Alto
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Inexistente	La organización no cuenta con aseguramiento de las aplicaciones en redes públicas.	A14.1.2.1	Determinar e identificar los servicios de aplicaciones que usen redes públicas para mejorar su operabilidad y seguridad.	Alto

A14.1.3	Protección de las transacciones de servicios de aplicaciones	Inexistente	La organización no cuenta con protección de las transacciones de servicios de aplicaciones.	A14.1.3.1	Determinar e identificar las transacciones y su nivel de seguridad que determine el fabricante para aplicar como normas en las políticas de seguridad.	Alto
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**					
A14.2.1	Política de desarrollo seguro	Inicial	La organización cuenta con una política de desarrollo seguro a criterio del personal del área de Sistemas.	A14.2.1.1	Documentar una política de desarrollo seguro, para implementarlo en el área de Sistemas de la organización.	Alto
A14.2.2	Procedimiento de control de cambios en sistemas	Inicial	La organización cuenta con un procedimiento de control de cambio en sistemas a criterio del personal del área de Sistemas.	A14.2.2.1	Documentar un procedimiento de control de cambio, para implementarlo en el área de Sistemas de la organización.	Alto
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Inicial	La organización cuenta con un procedimiento para revisión técnica de las aplicaciones a criterio del personal del área de Sistemas.	A14.2.3.1	Documentar un procedimiento para revisión técnica de aplicaciones, para implementarlo en el área de Sistemas de la organización.	Alto

A14.2.4	Restricciones a los cambios en los paquetes de software	Medio	La organización cuenta con restricciones a los cambios en los paquetes de software.	A14.2.4.1	Dar a conocer las restricciones a los cambios en los paquetes de software en conjunto con el área técnica de la organización.	Alto
A14.2.5	Principios de ingeniería de sistemas seguros	Inexistente	La organización no cuenta con principios de ingeniería de sistemas seguros.	A14.2.5.1	Implementar principios de ingeniería de sistemas seguros y aplicarlos en cada uno de los desarrollos.	Alto
A14.2.6	Entorno de desarrollo seguro	Inexistente	La organización no cuenta con un entorno de desarrollo seguro.	A14.2.6.1	Implementar un entorno de desarrollo seguro en el área de sistemas.	Alto
A14.2.7	Externalización del desarrollo de software	Inexistente	La organización no cuenta con externalización de desarrollo de software.	A14.2.7.1	Externalizar el desarrollo de software realizado a la interna de la organización.	Alto
A14.2.8	Pruebas funcionales de seguridad de sistemas	Inicial	La organización realiza pruebas funcionales de seguridad de sistemas a cargo del personal de Sistemas.	A14.2.8.1	Documentar el procedimiento a seguir en la realización de pruebas funcionales de seguridad.	Alto
A14.2.9	Pruebas de aceptación de sistemas	Inicial	La organización realiza pruebas de aceptación de	A14.2.9.1	Documentar las pruebas de aceptación de sistemas, para de esa forma	Alto

			sistemas a cargo del personal de Sistemas.		tener un respaldo del funcionamiento de los sistemas en cuestión.	
A14.3	**Datos de prueba**					
A14.3.1	Protección de los datos de prueba	Inicial	La organización protege los datos de prueba a cargo del personal de Sistemas.	A14.3.1.1	Implementar un procedimiento para mantener resguardado los datos de prueba.	Alto
A15	**Relación con proveedores**					
A15.1	**Seguridad en las relaciones con proveedores**					
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Inexistente	La organización no cuenta con una política de seguridad de la información en las relaciones con los proveedores	A15.1.1.1	Implementar una política de seguridad de la información en las relaciones con los proveedores.	Alto
A15.1.2	Requisitos de seguridad en contratos con terceros	Medio	La organización cuenta con requisitos de seguridad en contratos con terceros.	A15.1.2.1	Documentar los requisitos de seguridad en contratos con terceros.	Alto
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Inexistente	La organización no cuenta con una cadena de suministro	A15.1.3.1	Implementar una cadena de suministro de tecnología de	Alto

			de tecnología de la información y de las comunicaciones		la información y de las comunicaciones para así optimizar recursos de la organización.	
A15.2	Gestión de la provisión de servicios del proveedor					
A15.2.1	Control y revisión de la provisión de servicios del proveedor	Inicial	La organización cuenta con un control y revisión de la provisión de servicios del proveedor a criterio del departamento comercial.	A15.2.1.1	Documentar el control y revisión de la provisión de servicios del proveedor.	Alto
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Inicial	La organización cuenta con una gestión de cambios en la provisión del servicio del proveedor a criterio del departamento comercial.	A15.2.2.1	Documentar la gestión de cambios en la provisión del servicio del proveedor.	Alto
A16	**Gestión de incidentes de seguridad de la información**					
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**					
A16.1.1	Responsabilidades y procedimientos	Inexistente	La organización no cuenta con responsabilidades y procedimientos en gestión de incidentes.	A16.1.1.1	Crear un documento de responsabilidades y procedimientos en gestión de incidentes.	Alto

A16.1.2	Notificación de los eventos de seguridad de la información	Inicial	La organización cuenta con una notificación de los eventos de seguridad de la información.	A16.1.2.1	Documentar la notificación de los eventos de seguridad de la información para que la directiva esté al tanto.	Alto
A16.1.3	Notificación de puntos débiles de la seguridad	Inicial	La organización cuenta con la notificación de puntos débiles de la seguridad.	A16.1.3.1	Notificar al personal del área técnica sobre los puntos débiles de la seguridad para de esa manera poder documentarlos e implementar mejoras.	Alto
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Inexistente	La organización no cuenta con la evaluación y decisión sobre los eventos de seguridad de información.	A16.1.4.1	Implementar la evaluación y decisión sobre los eventos de seguridad de información.	Alto
A16.1.5	Respuesta a incidentes de seguridad de la información	Inicial	La organización cuenta con una respuesta a incidentes de seguridad de la información.	A16.1.5.1	Tener una respuesta efectiva a incidentes de seguridad de la información, documentándolo y notificando a la directiva.	Alto
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Inexistente	La organización no cuenta con un aprendizaje de los incidentes de seguridad de	A16.1.6.1	Implementar un ciclo de aprendizaje de los incidentes de seguridad de la información.	Alto

			la información.			
A16.1.7	Recopilación de evidencias	Inexistente	La organización no cuenta con recopilación de evidencias.	A16.1.7.1	Implementar una manera de recopilación de evidencias.	Alto
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**					
A17.1	**Continuidad de la seguridad de la información**					
A17.1.1	Planificación de la continuidad de la seguridad de la información	Inexistente	La organización no cuenta con una planificación de la continuidad de la seguridad de la información.	A17.1.1.1	Realizar una planificación periódica de la continuidad de la seguridad de la información.	Alto
A17.1.2	Implementar la continuidad de la seguridad de la información	Inexistente	La organización no implementa la continuidad de la seguridad de la información	A17.1.2.1	Implementar la continuidad de la seguridad de la información.	Alto
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Inexistente	La organización no cuenta con la verificación, revisión y evaluación de la continuidad de la seguridad de la información.	A17.1.3.1	Implementar la verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Alto
A17.2	**Redundancias**					

A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Inexistente	La organización no cuenta con la disponibilidad de los recursos de tratamiento de la información.	A17.2.1.1	Dar a conocer al personal del área técnica la disponibilidad de los recursos de tratamiento de la información.	Alto
A18	**Cumplimiento**					
A18.1	**Cumplimiento de los requisitos legales y contractuales**					
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Inicial	La organización cuenta con la identificación de la legislación aplicable y de los requisitos contractuales a cargo del departamento legal.	A18.1.1.1	Documentar la identificación de la legislación aplicable y de los requisitos contractuales.	Alto
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Inicial	La organización cuenta con los derechos de Propiedad Intelectual (DPI).	A18.1.2.1	Documentar los derechos de Propiedad Intelectual (DPI).	Alto
A18.1.3	Protección de los registros de la organización	Inicial	La organización cuenta con la protección de los registros de la organización.	A18.1.3.1	Resguardar de manera eficiente la protección de los registros de la organización.	Alto
A18.1.4	Protección y privacidad de la información de carácter personal	Inicial	La organización cuenta con la protección y privacidad de la información	A18.1.4.1	Documentar la protección y privacidad de la información de carácter personal.	Alto

			de carácter personal.			
A18.1.5	Regulación de los controles criptográficos	Inexistente	La organización no cuenta con la regulación de los controles criptográficos.	A18.1.5.1	Implementar la regulación de los controles criptográficos.	Alto
A18.2	**Revisiones de la seguridad de la información**					
A18.2.1	Revisión independiente de la seguridad de la información	Inexistente	La organización no cuenta con la revisión independiente de la seguridad de la información.	A18.2.1.1	Realizar una revisión independiente de la seguridad de la información.	Alto
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Inexistente	La organización no cuenta con el cumplimiento de las políticas y normas de seguridad.	A18.2.2.1	Constatar el cumplimiento de las políticas y normas de seguridad.	Alto
A18.2.3	Comprobación del cumplimiento técnico	Inexistente	La organización no cuenta con la comprobación del cumplimiento técnico.	A18.2.3.1	Realizar la comprobación de manera periódica del cumplimiento técnico.	Alto

Anexo 2: Evaluación de Riesgos

Amenazas	Vulnerabilidades	Impacto	Riesgo Inherente		
			Impacto	Probabilidad	Severidad
[N] Desastres naturales	No existe un DRP asociado a desastres naturales. El personal no está especializado ante un desastre natural. Las copias de seguridad no tienen una frecuencia a corto plazo. Los sistemas no cuentan con una ruta backup para las comunicaciones.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional.	CATASTRÓFICO	RARO	Alto
[I.4] Contaminación electromagnética	El sitio físico no cuenta con una aprobación ante la contaminación electromagnética. No se ha realizado inspección de los equipos cercanos.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales.	MODERADO	POCO PROBABLE	Moderado
[I.8] Fallo de servicios de comunicaciones	La cultura de aprendizaje a los usuarios no es muy efectiva. Las copias de seguridad no tienen una frecuencia a corto plazo. Los sistemas no cuentan con una ruta backup para las comunicaciones.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional. Demandas judicial, afectación Legal.	MODERADO	POCO PROBABLE	Moderado
[I.10] Degradación de los soportes de almacenamiento de la información	No hay un software que permita validar el correcto funcionamiento del hardware.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional.	MENOR	RARO	Bajo
[E.1] Errores de los usuarios	La cultura de aprendizaje a los usuarios no es muy efectiva. Las copias de seguridad no tienen una frecuencia a corto plazo. No se cuenta con un correcto control de roles de usuarios.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Afectación al clima laboral.	MODERADO	POSIBLE	Moderado
[E.4] Errores de configuración	El personal no tiene la suficiente especialización para la configuración de los sistemas e integración de los mismos. Las copias de seguridad no tienen una frecuencia a corto plazo. No hay una correcta gestión de cambio en los sistemas integradores.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional. Demandas judicial, afectación Legal.	CATASTRÓFICO	RARO	Alto
[E.14] Escapes de información	La cultura de aprendizaje a los usuarios no es muy efectiva. No existe una correcta manipulación de la información. Los sistemas no cuentan con un software para mitigar el uso de BYOD.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional. Demandas judicial, afectación Legal. Afectación al clima laboral.	MAYOR	POCO PROBABLE	Alto
[E.15] Alteración accidental de la información	Las copias de seguridad no tienen una frecuencia a corto plazo. La cultura de aprendizaje a los usuarios no es muy efectiva. No existe una correcta manipulación de la información. No hay una correcta gestión de cambio en los sistemas integradores.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional. Demandas judicial, afectación Legal. Afectación al clima laboral.	MODERADO	RARO	Moderado
[E.21] Errores de mantenimiento / actualización de programas (software)	No hay una correcta gestión de cambio en los sistemas integradores. No existe un protocolo en caso de fallo durante un mantenimiento en los programas. Las copias de seguridad no tienen una frecuenca a corto plazo. Los sistemas no cuentan con una ruta backup para las comunicaciones.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional. Demandas judicial, afectación Legal.	CATASTRÓFICO	POCO PROBABLE	Alto
[E.24] Caída del sistema por agotamiento de recursos	No hay un correcto uso de los canales de distribución de procesos. No hay una correcta asignación de recursos a los sistemas. No hay personal especializado para distribución y dimensionamiento de aplicativos.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional. Demandas judicial, afectación Legal. Afectación al clima laboral.	CATASTRÓFICO	POCO PROBABLE	Alto
[A.4] Manipulación de la configuración	No se cuenta con un correcto control de roles a los usuarios. No hay una correcta gestión de cambio en los sistemas integradores. Las copias de seguridad no tienen una frecuencia a corto plazo. No hay un software de registro de accesos.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional. Demandas judicial, afectación Legal.	CATASTRÓFICO	RARO	Alto
[A.11] Acceso no autorizado	No hay un software de registro de accesos. No se cuenta con un correcto control de roles a los usuarios. No hay una correcta gestión de cambio en los sistemas integradores. Las copias de seguridad no tienen una frecuencia a corto plazo. No existe una correcta manipulación de la información. Los sistemas no cuentan con un software para mitigar el uso de BYOD. La cultura de aprendizaje a los usuarios no es muy efectiva.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional. Demandas judicial, afectación Legal. Afectación al clima laboral.	CATASTRÓFICO	RARO	Alto
[A.6] Abuso de privilegios de acceso	No hay un software de registro de accesos. No se cuenta con un correcto control de roles a los usuarios. No hay una correcta gestión de cambio en los sistemas integradores. Las copias de seguridad no tienen una frecuencia a corto plazo. No existe un compromiso de confidencialidad especifico para cada sistema.	Pérdidas financieras. Interrupción de operaciones parciales y/o totales. Pérdida / Degradación de la Imagen institucional. Demandas judicial, afectación Legal. Afectación al clima laboral.	CATASTRÓFICO	RARO	Alto

Anexo 3: Riesgos y Controles

Nombre Activo	Riesgos	Objetivo de Control	Controles	Tipo de Control	Clasificación de Control	Frecuencia de Control	Fortaleza de Control	Controles a Implementar
Servidor CORE	Desastres naturales	Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional.	Identificar los posibles escenarios de desastres naturales posibles en la ubicación de la organización.	Manual	Preventivo	Anual	Alto	Definir las directrices necesarias para desarrollar un plan de contingencia de acuerdo a los riesgos existentes.
	Contaminación electromagnética	Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales.	Verificar si el servidor cuenta con conexiones a tierra. Identificar los componentes físicos del servidor y sus cargas electromagnéticas.	Automático	Preventivo Detectivo	Anual	Medio	Ingresar en el sistema operativo, identificar que las actividades realizadas en el servidor esten claramente identificadas en los logs de acceso. Evaluar que los accesos contengan permisos y esten aprobados previamente por un usuarios administrador para su acceso. Evaluar los permisos y privilegios de cada usuario en el sistema del directorio activo y que los mismos solo tengan acceso a los servicios otorgados por el ente regulador de cada área.
	Fallo de servicios de comunicaciones	Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional. Mitigar posibles demandas judiciales, afectación Legal.	Identificar si las comunicaciones cuentan con rutas alternas. Verificar si las comunicaciones cuentan con directrices pre establecidas para tolerancia a fallos.	Manual	Preventivo Detectivo	Mensual	Alto	Ingresar en los sistemas de comunicación del servidor y revisar los manuales y configuraciones pre establecidas para asegurar un canal de respaldo ante cualquier fallo del sistema principal. Implementar rutas de comunicación alternas a la principal en los sistemas verificando la disponibilidad del servicio.
	Degradación de los soportes de almacenamiento de la información	Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional.	Identificar los periodos de validéz de los soportes de almacenamiento y su vida útil.	Automático	Preventivo	Mensual	Medio	Ingresar en los sistemas de cada componente y verificar el periodo de validéz. Revisar los manuales de compra y mantenimiento de los componentes de almacenamiento identificando su vida útil.
	Errores de los usuarios	Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la afectación al clima laboral.	Identificar los roles asociados a cada usuario. Verificar si las políticas del servidor están anexadas a los usuarios activos.	Automático	Detectivo	Mensual	Alto	Ingresar en el directorio activo y validar los usuarios creados y asociados a la organización. Revisar el conjunto de políticas y directrices asociadas en el directorio activo validando que los usuarios estén atados a las normas y que cada uno de ellos contenga roles asociados. Ingresar en los parámetros de los usuarios verificando sus accesos y a los sistemas asociados que tengan permisos administrados.
	Errores de configuración	Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional. Mitigar posibles demandas judiciales, afectación Legal.	Identificar la integridad de los logs del servidor. Verificar la lista de control de acceso al servidor.	Manual	Detectivo	Mensual	Alto	Ingresar en el sistema principal e identificar que los logs estén siendo almacenados y que los mismos contengan información altamente importante como los controles de acceso al servidor. Ingresar en el sistema operativo y verificar que los controles de cambio estén previamente asociados a personal administrador del sistema.
	Escapes de información	Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional. Mitigar posibles demandas judiciales, afectación Legal. Mitigar la afectación al clima laboral.	Identificar que los registros de acceso a la información almacenada en el servidor esta monitorizada y registrada en los logs.	Automático	Preventivo Detectivo	Mensual	Medio	Ingresar en el sistema operativo del servidor, acceder a los logs del sistema y verificar las acciones realizadas por los usuarios y comparar que las descargas de los datos e información contengan un control de cambio o permisos asociados al mismo.
	Alteración accidental de la información	Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional. Mitigar posibles demandas judiciales, afectación Legal. Mitigar la afectación al clima laboral.	Identificar si los cambios en la información realizados en el servidor cuentan con respaldo en la lista de control de acceso y logs.	Automático	Preventivo Detectivo	Mensual	Alto	Ingresar en el sistema operativo, acceder a los logs del sistema y verificar que la información almacenada sea proporcional a la información registrada. Verificar mediante un usuario administrador que la información sea integra a la desplegada por el sistema.
	Errores de mantenimiento / actualización de programas (software)	Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional. Mitigar posibles demandas judiciales, afectación Legal.	Verificar que los programas de actualización y parches de seguridad han sido realizados en ambientes de pruebas. Identificar que las actualizaciones cuentan con un control de cambios aprobado por el comité.	Manual	Preventivo	Mensual	Medio	Ingresar en el sistema y acceder a los manuales de mantenimiento. Revisar que los mantenimientos previamente realizados consten con un control de cambios y aprobaciones de los entes de regualción. Verificar que los cambios y mantenimientos del sistema consten en los logs del sistema en conjunto a las actas de mantenimiento.
	Caída del sistema por agotamiento de recursos	Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional. Mitigar posibles demandas judiciales, afectación Legal. Mitigar la afectación al clima laboral.	Verificar que el servidor cuente con los recursos necesarios para un funcionamiento eficaz.	Automático	Preventivo Detectivo	Trimestral	Alto	Ingresar al sistema operativo, ingresar a las herramientas demonitoreo de recursos y verificar los recursos disponibles y compartidos que mantiene el servidor. Evaluar el correcto funcionamiento de los componentes y validar en conjunto con las actas de mantenimiento el soporte y validez de los mismos.
	Manipulación de la configuración	Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional. Mitigar posibles demandas judiciales, afectación Legal.	Identificar las listas de control de acceso al servidor. Verificar que los logs de configuración esten correctamente respaldados y contengan información periódica.	Manual	Preventivo	Mensual	Alto	Ingresar en el sistema operativo, ingresar a las herramientas de monitoreo de acceso y verificar que la lista de accesos estén previamente registradas en los logs de acceso. Verificar mediante un usuario administrador que los controles de cambio esten supervisados y comparar que las configuraciones sean integras acorde a las ultimas revisiones del sistema.
	Acceso no autorizado	Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional. Mitigar posibles demandas judiciales, afectación Legal. Mitigar la afectación al clima laboral.	Identificar que el acceso al servidor sea bajo normas y directrices previamente aprobadas y supervisadas.	Automático	Preventivo Detectivo	Mensual	Alto	Ingresar en el sistema operativo del servidor y revisar que los ogs de acceso estén funcionando correctamente. Revisar que los registros de acceso contengan usuarios y permisos aprobados. Evaluar que los accesos al servidor sean supervisados o con permisos de administrador.
	Abuso de privilegios de acceso	Mitigar las posibles pérdidas financieras. Mitigar las interrupciones de operaciones parciales y/o totales. Mitigar la Pérdida / Degradación de la Imagen institucional. Mitigar posibles demandas judiciales, afectación Legal. Mitigar la afectación al clima laboral.	Identificar que las actividades realizadas en el servidor cuenten con un registro en los logs de acceso. Identificar que las actividades realizadas sean realizadas por los administradores del servidor.	Automático	Preventivo Detectivo	Mensual	Alto	Ingresar en el sistema operativo, identificar que las actividades realizadas en el servidor esten claramente identificadas en los logs de acceso. Evaluar que los accesos contengan permisos y esten aprobados previamente por un usuarios administrador para su acceso. Evaluar los permisos y privilegios de cada usuario en el sistema del directorio activo y que los mismos solo tengan acceso a los servicios otorgados por el ente regulador de cada área.

Anexo 4: Plan de acción

Código	Acción	Responsable	Costo	Q1	Q2	Q3	Q4	Estado
PA1	Definir y acordar con todas las partes interesadas los objetivos del SGSI precautelando su eficacia durante la implementación.	Gerente Sistemas	Tiempo laboral	x				N/A
PA2	Analizar e identificar los factores internos y externos (obligaciones legales, regulatorias y contractuales), así como las tendencias en el entorno de negocio que pueden influir en el programa.	Gerente Sistemas	Tiempo laboral	x	x			N/A
PA3	Analizar los diversos requerimientos obtenidos, madurar cada requerimiento conforme a las obligaciones que competen al mismo.	Coordinador Sistemas	Tiempo laboral	x	x	x	x	N/A
PA4	Evaluar y determinar directrices para el cumplimiento del alcance propuesto.	Gerente Sistemas	Tiempo laboral	x				N/A
PA5	Validar y ejecutar el programa propuesto en la organización permitiendo de esta forma obtener un programa SGSI acorde a las necesidades de la empresa.	Gerente Sistemas	Tiempo laboral	x				N/A
PA6	Mantener una constante supervisión del programa SGSI para su mejora continua en base a las directrices establecidas.	Gerente Sistemas	Tiempo laboral	x	x	x	x	N/A
PA7	Establecer las directrices de comportamiento para proteger la información, sistemas e infraestructura corporativa.	Gerente Sistemas Gerente Soporte	Tiempo laboral	x				N/A

PA8	Establecer, acordar y comunicar los roles y responsabilidades relacionadas con I&T a todo el personal de la empresa, de acuerdo con las necesidades y objetivos de la empresa.	Ingeniero de sistemas	Tiempo laboral		x			N/A
PA9	Definir el alcance y los límites del sistema de gestión de seguridad de la información (SGSI) en términos de las características de la empresa, organización, ubicación, activos y tecnología.	Gerente Sistemas Gerente Soporte	Tiempo laboral	x				N/A
PA10	Definir el alcance adecuado de los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y/o la criticidad de los activos para el negocio.	Gerente Sistemas	Tiempo laboral	x				N/A
PA11	Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con objetivos estratégicos y la arquitectura empresarial. Asegurar que el plan identifique las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, responsabilidades y prioridades asociados para la gestión de los riesgos de seguridad de la información identificados.	Ingeniero de Seguridad de la información	Tiempo laboral		x	x		N/A
PA12	Definir el alcance y los límites del sistema de gestión de seguridad de la información (SGSI) en términos de las características de la	Ingeniero de sistemas	Tiempo laboral	x	x			N/A

	empresa, organización, ubicación, activos y tecnología.							
PA13	Llevar a cabo las actualizaciones y reformas programadas basadas en los directrices establecidas de mejora.	Ingeniero de sistemas Ingeniero de seguridad de la información	Tiempo laboral			x	x	N/A
PA14	Alinear los objetivos de la empresa basándose en la mejora continua y capacitación constante al personal para obtener trabajadores competentes a su cargo.	Personal externo	$200 / Día		x	x	x	N/A
PA15	Preparar un programa de comunicación que presente el plan de forma eficaz usando los medios de comunicación y tecnologías disponibles.	Ingeniero de seguridad de la información	Tiempo laboral	x				N/A
PA16	Mantener los principios para la comunicación con partes interesadas externas e internas, incluidos formatos y canales de comunicación, así como la aceptación y firma de informes de las partes interesadas.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A
PA17	Formular y evaluar un plan de gestión de documentación basándose en perfiles y roles dentro de la organización para control de activos de información mitigando su vulneración.	Ingeniero de seguridad de la información	Tiempo laboral	x	x			N/A
PA18	Determinar y alinear directrices basadas en el comité de revisión para la	Gerente Sistemas Gerente Soporte	Tiempo laboral	x				N/A

	aprobación de documentos.							
PA19	Determinar un plan de tratamiento de documentación, procurando su confidencialidad, integridad, confidencialidad y privacidad.	Gerente Sistemas Gerente Soporte	Tiempo laboral	x				N/A
PA20	Determinar normas y directrices para el proceso de gestión de riesgos y su tratamiento respectivo.	Gerente Sistemas Gerente Soporte	Tiempo laboral	x	x			N/A
PA21	Documentar los cambios, reevaluar y priorizar el portafolio para garantizar el alineamiento con el programa de SGSI resguardando la seguridad de la información.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A
PA22	Mantener, como parte de la arquitectura de la empresa, un inventario de los componentes de la solución establecida para gestionar los riesgos relacionados con la seguridad.	Ingeniero de seguridad de la información	Tiempo laboral	x	x			N/A
PA23	Implementar métricas y directrices para hacer un seguimiento de cómo se alcanzan los beneficios, cómo evolucionan a lo largo del ciclo de vida del programa.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A
PA24	Determinar y documentar un proceso de auditoria interna anula en base a las auditorías de otras áreas de la empresa.	Ingeniero de sistemas	Tiempo laboral	x	x			N/A

PA25	Revisar de forma regular los planes de continuidad para considerar el impacto del actual SGSI en base a nuevas amenazas y procesos que influyan en la organización.	Ingeniero de sistemas	Tiempo laboral	x			x	N/A
PA26	Establecer una plataforma para compartir buenas prácticas y captar información sobre los defectos y errores para permitir el aprendizaje a partir de ellos.	Ingeniero de sistemas	Tiempo laboral	x				N/A
PA27	Identificar los procesos críticos para el negocio basado en los motivadores de rendimiento y conformidad y el riesgo relacionado. Evaluar la capacidad e identificar los objetivos de mejora. Analizar las brechas de capacidad y control. Identificar opciones para mejorar o rediseñar el proceso.	Ingeniero de seguridad de la información	Tiempo laboral	x				N/A
PA28	Alinear la gestión de identidades y derechos de acceso con los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad-de-tener y necesidad-de-conocer.	Ingeniero de sistemas	Tiempo laboral	x				N/A
PA29	Determinar un periodo constante de revisión de políticas con la finalidad de conocer y prevenir vulnerabilidades y/o amenazas.	Ingeniero de sistemas Ingeniero de seguridad de la información	Tiempo laboral	x	x			N/A

PA30	Establecer, acordar y comunicar los roles y responsabilidades relacionadas con I&T a todo el personal de la empresa, de acuerdo con las necesidades y objetivos de la empresa	Gerente Sistemas	Tiempo laboral	x				N/A
PA31	Asignar roles para actividades sensibles para que haya una clara segregación de funciones.	Gerente Sistemas	Tiempo laboral	x				N/A
PA32	Establecer una comunicación formal con las autoridades de la empresa, documentando las comunicaciones con la finalidad de tener respaldos de las acciones tomadas en caso de necesitarlo.	Gerente Sistemas Gerente Soporte	Tiempo laboral	x	x	x	x	N/A
PA33	Mantener un contacto con grupos de interés manejando procedimientos previamente establecidos para de esa manera documentar de una mejor manera todo lo que se lleva a cabo en la empresa.	Coordinador de gestión comercial	Tiempo laboral	x	x	x	x	N/A
PA34	Mantener y hacer cumplir una estrategia estándar de gestión de proyectos, alineada con el entorno específico de la empresa y con las buenas prácticas, conforme a procesos definidos y al uso de la tecnología correcta, aplicando diversas políticas de seguridad de la información.	Coordinador de proyectos Gerente Soporte	Tiempo laboral	x	x	x	x	N/A

PA35	Mantener documentación formal en donde se indique los dispositivos móviles entregados a las diferentes personas de la organización, dejando en claro las condiciones para el uso del equipo en cuestión.	Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A
PA36	Tener documentados los accesos de cada persona de la organización y mantener un control remoto de las actividades de los miembros de la organización con la finalidad de dar un buen uso al tiempo y recursos.	Ingeniero de Soporte	Tiempo laboral	x	x	x	x	N/A
PA37	Incluir verificaciones de antecedentes en el proceso de contratación de TI para empleados, contratistas y terceros. El alcance y frecuencia de estas verificaciones debe depender de la sensibilidad y/o criticidad de la función.	Gerente Sistemas	Tiempo laboral	x	x	x	x	N/A
PA38	Proporciona directrices para la gestión de contratos (p. ej., términos y condiciones, supervisión de contratos).	Coordinador de personal	Tiempo laboral	x	x	x	x	N/A
PA39	Considerar y definir claramente los roles las responsabilidades de todas las partes involucradas	Coordinador de personal	Tiempo laboral	x	x	x	x	N/A
PA40	Realizar formación sobre concienciación de la seguridad de la información de forma regular a todo el personal de la empresa.	Coordinador de personal	Tiempo laboral	x	x	x	x	N/A
PA41	Implementar y comunicar un proceso disciplinario, dando a conocer a todos	Coordinador de personal	Tiempo laboral	x				N/A

	los empleados de la organización.							
PA42	Capacitar al personal de manera regular, sobre los pasos a seguir y responsabilidades que conlleva la finalización del empleo o cambios en el puesto de trabajo	Coordinador de personal	Tiempo laboral	x	x	x	x	N/A
PA43	Mantener un inventario de información (sistemas y datos) que incluyan una lista de Dueños, custodios y clasificaciones. Incluir sistemas que sean externalizados y aquellos cuya propiedad debería estar dentro de la empresa	Ingeniero de sistemas	Tiempo laboral	x	x	x	x	N/A
PA44	Revisar periódicamente el registro de propiedad de los activos para saber los movimientos que se producen con los mismos y así mantener el registro actualizado.	Ingeniero de Soporte	Tiempo laboral	x	x	x	x	N/A
PA45	Capacitar al personal de manera periódica con el fin de que los mismos sepan como manipular de manera adecuada los activos de la organización.	Ingeniero de seguridad de la información	Tiempo laboral	x			x	N/A
PA46	Dar a conocer todo el proceso que se debe seguir al momento de devolución de activos a cada uno de los miembros de la organización, de igual forma capacitar al área técnica para que sepan los pasos correctos a seguir en estos casos	Ingeniero de soporte	Tiempo laboral	x				N/A

PA47	Proporcionar las directrices para garantizar la clasificación adecuada y consistente de los elementos de información en toda la empresa	Ingeniero de soporte	Tiempo laboral	x	x			N/A
PA48	Proporcionar los accesos necesarios a las personas autorizadas para de esa manera garantizar que la información sea resguardada de manera adecuada y así evitar posible fuga de información.	Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A
PA49	Implementar un conjunto de directrices y normas basados en los sistemas de gestión para el uso adecuado de dispositivos extraíbles, permitiendo de esta manera mitigar la manipulación de la información.	Ingeniero de soporte	Tiempo laboral	x	x			N/A
PA50	Idear e implementar normas de eliminación de soportes aprobados por la directiva de seguridad.	Ingeniero de soporte	Tiempo laboral	x				N/A
PA51	Implementar un conjunto de normas que permitan tener un control estricto sobre los soportes físicos que mantiene cada miembro de la organización.	Ingeniero de soporte	Tiempo laboral	x				N/A
PA52	Implementar una política de control de acceso más moderno para de esa manera aumentar la seguridad de la organización.	Ingeniero de soporte	Tiempo laboral	x				N/A
PA53	Dar a conocer quienes son las personas autorizadas a acceder a las redes y los servicios de red para de	Ingeniero de soporte	Tiempo laboral	x				N/A

	esa manera garantizar un buen manejo de los recursos.							
PA54	Identificar el proceso de registro y baja de usuario automatizado, basando en métricas de uso del directorio activo de la organización.	Ingeniero de soporte	Tiempo laboral	x				N/A
PA55	Implementar un conjunto de normas para los aprovisionamientos temporales de acceso basándose en los roles otorgados al mismo.	Ingeniero de soporte	Tiempo laboral	x				N/A
PA56	Identificar y diseñar un proceso automatizado de gestión de privilegios basados en el rol de desempeño el mismo deberá ser aprobado por un comité técnico.	Ingeniero de Soporte	Tiempo laboral	x	x			N/A
PA57	Diseñar un proceso de gestión automática de autenticación de los usuarios, evitando de está manera el contacto directo de claves con el personal técnico.	Ingeniero de soporte	Tiempo laboral	x				N/A
PA58	Implementar una revisión periódica de los derechos de acceso de los usuarios.	Ingeniero de soporte	Tiempo laboral	x			x	N/A
PA59	Implementar un proceso formalizado de reasignación de derechos de acceso, notificando a los participes y a la directiva sobre los cambios.	Ingeniero de soporte	Tiempo laboral	x	x			N/A
PA60	Implementar un curso de concientización para toda la organización con la finalidad de mostrar de los peligros y riesgos existentes de compartir	Coordinador de personal	Tiempo laboral	x				N/A

	información secreta de autenticación con terceras personas.							
PA61	Implementar un mayor nivel de restricciones de acceso a la información para que la misma solo sea accedida por las personas autorizadas y con ello resguardar la información.	Ingeniero de Soporte	Tiempo laboral	x				N/A
PA62	Capacitar al personal para que los mismos apliquen procedimientos seguros de inicio de sesión, y sean responsables y conscientes que la información que se reguarda es el activo más importante que existe.	Ingeniero de Soporte	Tiempo laboral	x				N/A
PA63	Proponer una mejora sobre el sistema donde se alojan todas las contraseñas, para de esa manera tener una segunda opción de alojamiento y de esa forma aumentar el nivel de seguridad.	Coordinador Sistemas	Tiempo laboral	x				N/A
PA64	Implementar el uso de utilidades con privilegios del sistema y que los mismos sean aprobados por el comité.	Ingeniero de sistemas Ingeniero de soporte	Tiempo laboral	x				N/A
PA65	Implementar un conjunto de normas y directrices para el cambio, renovación y gestión de los controles criptográficos para que puedan ser aprobados y revisados por un comité.	Ingeniero de sistemas	Tiempo laboral	x	x			N/A
PA66	Implementar directrices de revisión y aprobación para la correcta gestión de claves de la organización.	Ingeniero de soporte	Tiempo laboral	x	x			N/A

PA67	Se deben implementar perímetros de seguridad física para precautelar la integridad física de todo el personal de la organización y saber como actuar de manera adecuada en caso de emergencia.	Coordinador de personal	Tiempo laboral	x				N/A
PA68	Se debe modernizar los controles físicos de entrada para de esa manera, tener mayor seguridad y proteger las oficinas de la organización de acceso no autorizado.	Coordinador de seguridad	Tiempo laboral	x				N/A
PA69	Se debe mejorar la seguridad de oficinas, despachos y recursos para que solo el personal autorizado de cada área pueda acceder a las oficinas según sea la necesidad.	Coordinador de seguridad	Tiempo laboral	x				N/A
PA70	Capacitar al personal para que de esa manera sepan como actuar de manera correcta ante las diferentes amenazas externas y ambientales que puedan presentarse.	Coordinador de personal	Tiempo laboral	x				N/A
PA71	Mejorar la distribución de espacios para que todo el personal de la organización se sienta a gusto en el lugar de trabajo y pueda desempeñar sus funciones de manera eficiente y eficaz.	Coordinador de personal	Tiempo laboral	x				N/A
PA72	Implementar un área de carga y descarga segura con la finalidad de tener un mejor manejo por parte de todo el personal de la organización.	Coordinador de seguridad	Tiempo laboral	x				N/A

PA73	Determinar e identificar el correcto uso de los equipos personales de la organización con el fin de evitar daños y mal funcionamiento de los dispositivos.	Ingeniero de soporte	Tiempo laboral	x	x			N/A
PA74	Determinar el uso del computador e identificar posibles escenarios de falla de los suministros basados en los cuidados que mantiene el miembro de la organización.	Ingeniero de soporte	Tiempo laboral	x	x			N/A
PA75	Identificar la seguridad del cableado de los hogares y proponer actividades de cambio y mejora para la seguridad de los empleados.	Ingeniero de soporte	Tiempo laboral		x	x		N/A
PA76	Identificar las mejoras potenciales basándose en métricas de productividad y de fallos registrados en los equipos.	Ingeniero de soporte	Tiempo laboral	x				N/A
PA77	Identificar basado en métricas posibles mejoras y alargar los años productivos de los materiales de la empresa.	Ingeniero de soporte	Tiempo laboral	x				N/A
PA78	Identificar e implementar un seguro para los equipos que se encuentren fuera de las instalaciones, previniendo cualquier tipo de afectación a la organización.	Ingeniero de soporte	Tiempo laboral	x				N/A
PA79	Determinar los tiempos de vida útil de los equipos de la organización para permitir una eliminación segura aprobada por la directiva y no de último momento.	Ingeniero de soporte	Tiempo laboral	x				N/A

PA80	Determinar los tiempos de uso de los equipos e implementar una regla para equipos desatendidos basados en métricas y aprobaciones de la directiva.	Ingeniero de soporte	Tiempo laboral	x				N/A
PA81	Determinar e implementar políticas de trabajo despejado y pantalla limpia en la organización basándose en el uso de Active Directory	Ingeniero de soporte	Tiempo laboral	x				N/A
PA82	Determinar todos los procedimientos operacionales a seguir en cada una de las áreas, y que sea de conocimiento de todos los miembros de la organización.	Coordinador de personal	Tiempo laboral	x	x	x	x	N/A
PA83	Identificar e implementar una serie de pasos a seguir en la gestión de cambios de las operaciones y que sea conocido por el personal técnico.	Ingeniero de soporte	Tiempo laboral	x				N/A
PA84	Identificar e implementar una serie de pasos a seguir en la gestión de capacidades de las operaciones y que sea conocido por el personal técnico.	Ingeniero de soporte	Tiempo laboral	x				N/A
PA85	Determinar las diferentes fases con las que cuentan los recursos para que las mismas sean claras y plenamente identificadas por parte del personal técnico de la organización.	Ingeniero de soporte	Tiempo laboral	x	x			N/A
PA86	Dar mantenimiento preventivo cada cierto tiempo en cada uno de los ordenadores, ejecutando análisis de malware para	Ingeniero de soporte	Tiempo laboral	x			x	N/A

	de esa manera evitar infecciones de las máquinas y prevenir desastres.							
PA87	Elaborar un cronograma bien establecido y generar un registro de las copias de seguridad de la información de cada uno de los miembros de la organización para poder acceder a la información cuando sea requerido.	Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A
PA88	Elaborar un registro de eventos documentado y aprobado por el comité, con la finalidad de saber los eventos que han sucedido por cada uno de los eventos de la organización.	Ingeniero de soporte	Tiempo laboral	X	X	X	X	N/A
PA89	Elaborar un registro de la protección de la información del registro documentado y aprobado por el comité, con la finalidad de saber los eventos que han sucedido por cada uno de los eventos de la organización.	Ingeniero de soporte	Tiempo laboral	X	X	X	X	N/A
PA90	Elaborar un registro de administración y operación documentado y aprobado por el comité, con la finalidad de saber los eventos que han sucedido por cada uno de los eventos de la organización.	Coordinador de gestión comercial	Tiempo laboral	x	x			N/A
PA91	Elaborar un registro de la sincronización del reloj aunque esto no es estrictamente necesario.	Ingeniero de soporte	Tiempo laboral	X				N/A

PA92	Se debe instalar software en explotación con la finalidad de poder simular ataques controlados y conocer sobre las vulnerabilidades existentes.	Ingeniero de sistemas	Tiempo laboral	x	x			N/A
PA93	Identificar y analizar la gestión de vulnerabilidades técnicas documentando los procesos y evaluar las acciones en el directivo.	Ingeniero de sistemas Ingeniero de soporte	Tiempo laboral	X	X			N/A
PA94	Determinar de mejores maneras los roles y uso de aplicaciones para la limitación de software y permitir basado en métricas la instalación de software de terceros a usuarios con roles administrativos.	Ingeniero de sistemas	Tiempo laboral	x	x			N/A
PA95	Contar con una auditoria de sistemas de información cada cierto tiempo y llevar un registro para su debido control.	Ingeniero de sistemas	Tiempo laboral	x	x			N/A
PA96	Documentar los controles de red, creando manuales de control permitiendo tener métricas de evaluación continua.	Ingeniero de soporte	Tiempo laboral	X	X			N/A
PA97	Determinar los responsables de la documentación de la seguridad en los servicios de red para tener una aprobación por parte de un comité e implementar una revisión continua de los mismos.	Ingeniero de soporte	Tiempo laboral	X	X			N/A
PA98	Identificar las áreas de red e implementar una nueva segregación permitiendo obtener un control de red	Ingeniero de soporte	Tiempo laboral	X	X			N/A

	mas transparente y escalable.							
PA99	Documentar las políticas y procedimientos de intercambio de información y que esté al alcance de todos los miembros de la organización.	Ingeniero de seguridad de la información	Tiempo laboral	X	X			N/A
PA100	Documentar los acuerdos de intercambio de información y que esté al alcance de todos los miembros de la organización.	Ingeniero de seguridad de la información	Tiempo laboral	X	X			N/A
PA101	Actualizar periódicamente el software de mensajería electrónica más aun ahora que es de uso primordial en la modalidad de teletrabajo.	Ingeniero de sistemas	Tiempo laboral	x	x			N/A
PA102	Capacitar a todo el personal de la organización acerca de las consecuencias en caso de romper los acuerdos de confidencialidad o no revelación.	Coordinador de personal	Tiempo laboral	x	x	x	x	N/A
PA103	Identificar los requisitos y especificaciones de la seguridad de la información basándose en normas orientadas a las buenas prácticas, documentado el proceso y verificando los mismos con un comité.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A
PA104	Determinar e identificar los servicios de aplicaciones que usen redes públicas para mejorar su operatividad y seguridad.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A

PA105	Determinar e identificar las transacciones y su nivel de seguridad que determine el fabricante para aplicar como normas en las políticas de seguridad.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A
PA106	Documentar una política de desarrollo seguro, para implementarlo en el área de Sistemas de la organización.	Gerente Sistemas	Tiempo laboral	x	x	x	x	N/A
PA107	Documentar un procedimiento de control de cambio, para implementarlo en el área de Sistemas de la organización.	Ingeniero de sistemas	Tiempo laboral	x	x			N/A
PA108	Documentar un procedimiento para revisión técnica de aplicaciones, para implementarlo en el área de Sistemas de la organización.	Ingeniero de sistemas	Tiempo laboral	x				N/A
PA109	Dar a conocer las restricciones a los cambios en los paquetes de software en conjunto con el área técnica de la organización.	Ingeniero de sistemas	Tiempo laboral	x				N/A
PA110	Implementar principios de ingeniería de sistemas seguros y aplicarlos en cada uno de los desarrollos.	Ingeniero de sistemas	Tiempo laboral	x				N/A
PA111	Implementar un entorno de desarrollo seguro en el área de sistemas.	Ingeniero de sistemas	Tiempo laboral	x				N/A
PA112	Externalizar el desarrollo de software realizado a la interna de la organización.	Ingeniero de sistemas	Tiempo laboral	x	x	x	x	N/A
PA113	Documentar el procedimiento a seguir en la realización de pruebas funcionales de seguridad.	Ingeniero de seguridad de la información	Tiempo laboral	x	x			N/A

PA114	Documentar las pruebas de aceptación de sistemas, para de esa forma tener un respaldo del funcionamiento de los sistemas en cuestión.	Ingeniero de sistemas	Tiempo laboral	x	x	x	x	N/A
PA115	Implementar un procedimiento para mantener resguardado los datos de prueba.	Ingeniero de sistemas	Tiempo laboral	x	x	x	x	N/A
PA116	Implementar una política de seguridad de la información en las relaciones con los proveedores.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A
PA117	Documentar los requisitos de seguridad en contratos con terceros.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A
PA118	Implementar una cadena de suministro de tecnología de la información y de las comunicaciones para así optimizar recursos de la organización.	Ingeniero de seguridad de la información	Tiempo laboral	x				N/A
PA119	Documentar el control y revisión de la provisión de servicios del proveedor.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A
PA120	Documentar la gestión de cambios en la provisión del servicio del proveedor.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A
PA121	Crear un documento de responsabilidades y procedimientos en gestión de incidentes.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A
PA122	Documentar la notificación de los eventos de seguridad de la información para que la directiva esté al tanto.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A

PA123	Notificar al personal del área técnica sobre los puntos débiles de la seguridad para de esa manera poder documentarlos e implementar mejoras.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A
PA124	Implementar la evaluación y decisión sobre los eventos de seguridad de información.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A
PA125	Tener una respuesta efectiva a incidentes de seguridad de la información, documentándolo y notificando a la directiva.	Ingeniero de seguridad de la información Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A
PA126	Implementar un ciclo de aprendizaje de los incidentes de seguridad de la información.	Ingeniero de seguridad de la información	Tiempo laboral	x	x			N/A
PA127	Implementar una manera de recopilación de evidencias.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A
PA128	Realizar una planificación periódica de la continuidad de la seguridad de la información.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A
PA129	Implementar la continuidad de la seguridad de la información.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A
PA130	Implementar la verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Ingeniero de seguridad de la información	Tiempo laboral	x	x	x	x	N/A

PA131	Dar a conocer al personal del área técnica la disponibilidad de los recursos de tratamiento de la información.	Ingeniero de seguridad de la información	Tiempo laboral	x				N/A
PA132	Documentar la identificación de la legislación aplicable y de los requisitos contractuales.	Ingeniero de seguridad de la información	Tiempo laboral	x				N/A
PA133	Documentar los derechos de Propiedad Intelectual (DPI).	Ingeniero de seguridad de la información	Tiempo laboral	x				N/A
PA134	Resguardar de manera eficiente la protección de los registros de la organización.	Ingeniero de seguridad de la información Ingeniero de soporte	Tiempo laboral	x				N/A
PA135	Documentar la protección y privacidad de la información de carácter personal.	Ingeniero de soporte	Tiempo laboral	x	x			N/A
PA136	Implementar la regulación de los controles criptográficos.	Ingeniero de sistemas	Tiempo laboral	x	x			N/A
PA137	Realizar una revisión independiente de la seguridad de la información.	Ingeniero de sistemas Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A
PA138	Constatar el cumplimiento de las políticas y normas de seguridad.	Ingeniero de seguridad de la información Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A
PA139	Realizar la comprobación de manera periódica del cumplimiento técnico.	Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A

PA140	Definir las directrices necesarias para desarrollar un plan de contingencia de acuerdo con los riesgos existentes.	Ingeniero de seguridad de la información	Tiempo laboral	x	x			N/A
PA141	Ingresar en el sistema operativo, identificar que las actividades realizadas en el servidor estén claramente identificadas en los logs de acceso. Evaluar que los accesos contengan permisos y estén aprobados previamente por un usuario administrador para su acceso. Evaluar los permisos y privilegios de cada usuario en el sistema del directorio activo y que los mismos solo tengan acceso a los servicios otorgados por el ente regulador de cada área.	Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A
PA142	Ingresar en los sistemas de comunicación del servidor y revisar los manuales y configuraciones preestablecidas para asegurar un canal de respaldo ante cualquier fallo del sistema principal. Implementar rutas de comunicación alternas a la principal en los sistemas verificando la disponibilidad del servicio.	Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A
PA143	Ingresar en los sistemas de cada componente y verificar el periodo de validez. Revisar los manuales de compra y mantenimiento de los componentes de	Ingeniero de sistemas Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A

	almacenamiento identificando su vida útil.							
PA144	Ingresar en el directorio activo y validar los usuarios creados y asociados a la organización. Revisar el conjunto de políticas y directrices asociadas en el directorio activo validando que los usuarios estén atados a las normas y que cada uno de ellos contenga roles asociados. Ingresar en los parámetros de los usuarios verificando sus accesos y a los sistemas asociados que tengan permisos administrados.	Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A
PA145	Ingresar en el sistema principal e identificar que los logs estén siendo almacenados y que los mismos contengan información altamente importante como los controles de acceso al servidor. Ingresar en el sistema operativo y verificar que los controles de cambio estén previamente asociados a personal administrador del sistema.	Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A
PA146	Ingresar en el sistema operativo del servidor, acceder a los logs del sistema y verificar las acciones realizadas por los usuarios y comparar que las descargas de los datos e información contengan un	Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A

	control de cambio o permisos asociados al mismo.							
PA147	Ingresar en el sistema operativo, acceder a los logs del sistema y verificar que la información almacenada sea proporcional a la información registrada. Verificar mediante un usuario administrador que la información sea integra a la desplegada por el sistema.	Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A
PA148	Ingresar en el sistema y acceder a los manuales de mantenimiento. Revisar que los mantenimientos previamente realizados consten con un control de cambios y aprobaciones de los entes de regulación. Verificar que los cambios y mantenimientos del sistema consten en los logs del sistema en conjunto a las actas de mantenimiento.	Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A
PA149	Ingresar al sistema operativo, ingresar a las herramientas de monitoreo de recursos y verificar los recursos disponibles y compartidos que mantiene el servidor. Evaluar el correcto funcionamiento de los componentes y validar en conjunto con las actas de mantenimiento el soporte y validez de estos.	Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A

PA150	Ingresar en el sistema operativo, ingresar a las herramientas de monitoreo de acceso y verificar que la lista de accesos esté previamente registrada en los logs de acceso. Verificar mediante un usuario administrador que los controles de cambio estén supervisados y comparar que las configuraciones sean integras acorde a las ultimas revisiones del sistema.	Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A
PA151	Ingresar en el sistema operativo del servidor y revisar que los logs de acceso estén funcionando correctamente. Revisar que los registros de acceso contengan usuarios y permisos aprobados. Evaluar que los accesos al servidor sean supervisados o con permisos de administrador.	Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A
PA152	Ingresar en el sistema operativo, identificar que las actividades realizadas en el servidor estén claramente identificadas en los logs de acceso. Evaluar que los accesos contengan permisos y estén aprobados previamente por un usuario administrador para su acceso. Evaluar los permisos y privilegios de cada usuario en el sistema del directorio activo y que los mismos solo tengan acceso a los servicios	Ingeniero de soporte	Tiempo laboral	x	x	x	x	N/A

	otorgados por el ente regulador de cada área.							

Anexo 5: Políticas de Alto Nivel

Nombre Activo	Riesgos	Objetivo	Código actividad	Política de Alto Nivel	Calificación
Servidor CORE	Desastres naturales	El objetivo es evitar los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.	A11.1.1.1	Definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica de la organización.	Alto
			A17.2.1.1	Dar a conocer al personal del área técnica la disponibilidad de los recursos de tratamiento de la información.	Alto
			A17.1.1.1	Realizar una planificación periódica de la continuidad de la seguridad de la información.	Medio
			A17.1.2.1	Implementar la continuidad de la seguridad de la información.	Medio
			A17.1.3.1	Implementar la verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Alto
			A12.6.1.1	Identificar y analizar la gestión de vulnerabilidades técnicas documentando los procesos y evaluar las acciones en el directivo.	Alto
			A12.3.1.1	Elaborar un cronograma bien establecido y generar un registro de las copias de seguridad de la información de cada uno de los miembros de la organización para poder acceder a la información cuando sea requerido.	Alto
			A11.2.6.1	Identificar e implementar un seguro para los equipos que se encuentren fuera de las instalaciones, previniendo cualquier tipo de afectación a la organización.	Bajo

	Contaminación electromagnética	El objetivo es evitar la pérdida, los daños, el robo o el compromiso de activos y la interrupción a las operaciones de la organización.	A11.2.1.1	Determinar e identificar el correcto uso de los equipos personales de la organización con el fin de evitar daños y mal funcionamiento de los dispositivos.	Alto
			A11.2.2.1	Determinar el uso del computador e identificar posibles escenarios de falla de los suministros basados en los cuidados que mantiene el miembro de la organización.	Medio
			A11.2.3.1	Identificar la seguridad del cableado de los hogares y proponer actividades de cambio y mejora para la seguridad de los empleados.	Bajo
			A11.2.4.1	Identificar las mejoras potenciales basandose en métricas de productividad y de fallos registrados en los equipos.	Alto
	Fallo de servicios de comunicaciones	El objetivo es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.	A11.2.6.1	Identificar e implementar un seguro para los equipos que se encuentren fuera de las instalaciones, previniendo cualquier tipo de afectación a la organización.	Medio
			A12.4.1.1	Elaborar un registro de eventos documentado y aprobado por el comité, con la finalidad de saber los eventos que han sucedido por cada uno de los eventos de la organización.	Alto
			A13.1.1.1	Documentar los controles de red, creando manuales de control permitiendo tener métricas de evaluación continua.	Alto
			A13.1.2.1	Determinar los responsables de la documentación de la seguridad en los servicios de red para tener una aprobación por parte de un comité e implementar una revisión continua de los mismos.	Alto
			A13.1.3.1	Identificar las áreas de red e implementar una nueva segregación permitiendo obtener un control de red mas transparente y escalable.	Alto

	Degradación de los soportes de almacenamiento de la información	El objetivo es evitar la divulgación, modificación, retirada o destrucción de activos no autorizada almacenada en soportes de almacenamiento.	A8.3.1.1	Implementar un conjunto de directrices y normas basados en los sistemas de gestión para el uso adecuado de dispositivos extraibles, permitiendo de esta manera mitigar la manipulación de la información.	Alto
			A8.3.2.1	Idear e implementar normas de eliminación de soportes aprobados por la directiva de seguridad.	Alto
			8.3.1	Mantener, como parte de la arquitectura de la empresa, un inventario de los componentes de la solución establecida para gestionar los riesgos relacionados con la seguridad.	Alto
	Errores de los usuarios	El objetivo es el de asegurarse de que los empleados y contratistas están en conocimiento y cumplen con sus responsabilidades en seguridad de la información.	A7.2.1.1	Considerar y definir claramente los roles las responsabilidades de todas las partes involucradas	Alto
			A7.2.2.1	Realizar formación sobre concienciación de la seguridad de la información de forma regular a todo el personal de la empresa.	Alto
			A7.2.3.1	Implementar y comunicar un proceso disciplinario, dando a conocer a todos los empleados de la organización.	Alto
			A9.3.1.1	Implementar un curso de concientización para toda la organización con la finalidad de mostrar de los peligros y riesgos existentes de compartir información secreta de autenticación con terceras personas.	Alto
			A9.4.1.1	Implementar un mayor nivel de restricciones de acceso a la información para que la misma solo sea accedida por las personas autorizadas y con ello resguardar la información.	Alto
			A9.4.2.1	Capacitar al personal para que los mismos apliquen procedimientos seguros de inicio de sesión,y sean responsables y conscientes que la información que se reguarda es el activo más importante que existe.	Alto
			A9.4.3.1	Proponer una mejora sobre el sistema donde se alojan todas las contraseñas, para de esa manera tener una segunda opción de alojamiento y de esa forma aumentar el nivel de seguridad.	Alto
			A9.4.4.1	Implementar el uso de utilidades con privilegios del sistema y que los mismos sean aprobados por el comité.	Alto

	Errores de configuración	El objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada.	A12.1.1.1	Determinar todos los procedimientos operacionales a seguir en cada una de las áreas, y que sea de conocimiento de todos los miembros de la organización.	Alto
			A12.1.2.1	Identificar e implementar una serie de pasos a seguir en la gestión de cambios de las operaciones y que sea conocido por el personal técnico.	Alto
			A12.1.3.1	Identificar e implementar una serie de pasos a seguir en la gestión de capacidades de las operaciones y que sea conocido por el personal técnico.	Alto
			A12.1.4.1	Determinar las diferentes fases con las que cuentan los recursos para que las mismas sean claras y plenamente identificadas por parte del personal técnico de la organización.	Alto
			A12.4.1.1	Elaborar un registro de eventos documentado y aprobado por el comité, con la finalidad de saber los eventos que han sucedido por cada uno de los eventos de la organización.	Medio
			A12.4.2.1	Elaborar un registro de la protección de la información del registro documentado y aprobado por el comité, con la finalidad de saber los eventos que han sucedido por cada uno de los eventos de la organización.	Alto
			A12.4.3.1	Elaborar un registro de administración y operación documentado y aprobado por el comité, con la finalidad de saber los eventos que han sucedido por cada uno de los eventos de la organización.	Medio
			A14.2.2.1	Documentar un procedimiento de control de cambio, para implementarlo en el área de Sistemas de la organización.	Alto
			A14.2.8.1	Documentar el procedimiento a seguir en la realización de pruebas funcionales de seguridad.	Alto

	Escapes de información	El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.	A16.1.1.1	Crear un documento de responsabilidades y procedimientos en gestión de incidentes.	Alto
			A16.1.2.1	Documentar la notificación de los eventos de seguridad de la información para que la directiva esté al tanto.	Alto
			A16.1.3.1	Notificar al personal del área técnica sobre los puntos débiles de la seguridad para de esa manera poder documentarlos e implementar mejoras.	Alto
			A16.1.4.1	Implementar la evaluación y decisión sobre los eventos de seguridad de información.	Alto
			A16.1.5.1	Tener una respuesta efectiva a incidentes de seguridad de la información, documentando y notificando a la directiva.	Alto
			A16.1.6.1	Implementar un ciclo de aprendizaje de los incidentes de seguridad de la información.	Alto
			A16.1.7.1	Implementar una manera de recopilación de evidencias.	Alto
	Alteración accidental de la información	El objetivo es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos.	A18.2.1.1	Realizar una revisión independiente de la seguridad de la información.	Alto
			A18.2.2.1	Constatar el cumplimiento de las políticas y normas de seguridad.	Alto
			A18.2.3.1	Realizar la comprobación de manera periódica del cumplimiento técnico.	Alto
			A12.1.2.1	Identificar e implementar una serie de pasos a seguir en la gestión de cambios de las operaciones y que sea conocido por el personal técnico.	Alto
			A9.4.1.1	Implementar un mayor nivel de restricciones de acceso a la información para que la misma solo sea accedida por las personas autorizadas y con ello resguardar la información.	Alto
			A8.2.3.1	Proporcionar los accesos necesarios a las personas autorizadas para de esa manera garantizar que la información sea resguardada de manera adecuada y asi evitar posible fuga de información.	Alto

	Errores de mantenimiento / actualización de programas (software)	El objetivo es mitigar cualquier tipo de vulneración durante el proceso de mantenimiento u actualziación de los servicios de la organización con el fin de que incurra errores o paro de las actividades.	8.1.1	Determinar normas y directrices para el proceso de gestión de riesgos y su tratamiento respectivo.	Alto
			8.2.1	Documentar los cambios, reevaluar y priorizar el portafolio para garantizar el alineamiento con el programa de SGSI resguardando la seguridad de la información.	Alto
			8.3.1	Mantener, como parte de la arquitectura de la empresa, un inventario de los componentes de la solución establecida para gestionar los riesgos relacionados con la seguridad.	Alto
			A8.2.3.1	Proporcionar los accesos necesarios a las personas autorizadas para de esa manera garantizar que la información sea resguardada de manera adecuada y asi evitar posible fuga de información.	Alto
			A9.2.3.1	Identificar y diseñar un proceso automatizado de gestión de privilegios basados en el rol de desempeño el mismo deberá ser aprobado por un comité técnico.	Alto
			A9.4.1.1	Implementar un mayor nivel de restricciones de acceso a la información para que la misma solo sea accedida por las personas autorizadas y con ello resguardar la información.	Alto
			A9.4.2.1	Capacitar al personal para que los mismos apliquen procedimientos seguros de inicio de sesión,y sean responsables y conscientes que la información que se reguarda es el activo más importante que existe.	Alto
			A9.4.3.1	Proponer una mejora sobre el sistema donde se alojan todas las contraseñas, para de esa manera tener una segunda opción de alojamiento y de esa forma aumentar el nivel de seguridad.	Alto
			A9.4.4.1	Implementar el uso de utilidades con privilegios del sistema y que los mismos sean aprobados por el comité.	Alto
			A11.2.4.1	Identificar las mejoras potenciales basandose en métricas de productividad y de fallos registrados en los equipos.	Alto

	Caída del sistema por agotamiento de recursos	El objetivo es garantizar la integridad de los sistemas operacionales para la organización.	A12.6.1.1	Identificar y analizar la gestión de vulnerabilidades técnicas documentando los procesos y evaluar las acciones en el directivo.	Alto
			A12.6.2.1	Determinar de mejor maneras los roles y uso de aplicaciones para la limitación de software y permitir basado en métricas la instalación de software de terceros a usuarios con roles administrativos.	Medio
			A12.1.2.1	Identificar e implementar una serie de pasos a seguir en la gestión de cambios de las operaciones y que sea conocido por el personal técnico.	Alto
			A11.2.4.1	Identificar las mejoras potenciales basandose en métricas de productividad y de fallos registrados en los equipos.	Alto
			A11.2.1.1	Determinar e identificar el correcto uso de los equipos personales de la organización con el fin de evitar daños y mal funcionamiento de los dispositivos.	Alto
			A11.2.2.1	Determinar el uso del computador e identificar posibles escenarios de falla de los suministros basados en los cuidados que mantiene el miembro de la organización.	Medio
	Manipulación de la configuración	El objetivo es el de asegurarse de que los empleados y contratistas están en conocimiento y cumplen con sus responsabilidades en seguridad de la información.	A12.3.1.1	Elaborar un cronograma bien establecido y generar un registro de las copias de seguridad de la información de cada uno de los miembros de la organización para poder acceder a la información cuando sea requerido.	Alto
			A12.4.1.1	Elaborar un registro de eventos documentado y aprobado por el comité, con la finalidad de saber los eventos que han sucedido por cada uno de los eventos de la organización.	Alto
			A12.4.2.1	Elaborar un registro de la protección de la información del registro documentado y aprobado por el comité, con la finalidad de saber los eventos que han sucedido por cada uno de los eventos de la organización.	Alto
			A12.4.3.1	Elaborar un registro de administración y operación documentado y aprobado por el comité, con la finalidad de saber los eventos que han sucedido por cada uno de los eventos de la organización.	Alto
			A7.2.1.1	Considerar y definir claramente los roles las responsabilidades de todas las partes involucradas	Alto
			A7.2.2.1	Realizar formación sobre concienciación de la seguridad de la información de forma regular a todo el personal de la empresa.	Alto
			A7.2.3.1	Implementar y comunicar un proceso disciplinario, dando a conocer a todos los empleados de la organización.	Medio

	Acceso no autorizado	El objetivo es el de garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.	A9.2.1.1	Identificar el proceso de registro y baja de usuario automatizado, basando en métricas de uso del directorio activo de la organización.	Alto
			A9.2.2.1	Implementar un conjunto de normas para los provisionamientos temporales de acceso basandose en los roles otorgados al mismo.	Alto
			A9.2.3.1	Identificar y diseñar un proceso automatizado de gestión de privilegios basados en el rol de desempeño el mismo deberá ser aprobado por un comité técnico.	Alto
			A9.2.4.1	Diseñar un proceso de gestión automática de autenticación de los usuarios, evitando de está manera el contacto directo de claves con el personal técnico.	Alto
			A9.2.5.1	Implementar una revisión periódica de los derechos de acceso de los usuarios.	Alto
			A9.2.6.1	Implementar un proceso formalizado de reasignación de derechos de acceso, notificando a los participes y a la directiva sobre los cambios.	Alto
			A9.3.1.1	Implementar un curso de concientización para toda la organización con la finalidad de mostrar de los peligros y riesgos existentes de compartir información secreta de autenticación con terceras personas.	Alto
			A9.4.1.1	Implementar un mayor nivel de restricciones de acceso a la información para que la misma solo sea accedida por las personas autorizadas y con ello resguardar la información.	Alto
			A9.4.2.1	Capacitar al personal para que los mismos apliquen procedimientos seguros de inicio de sesión,y sean responsables y conscientes que la información que se reguarda es el activo más importante que existe.	Alto
			A9.4.3.1	Proponer una mejora sobre el sistema donde se alojan todas las contraseñas, para de esa manera tener una segunda opción de alojamiento y de esa forma aumentar el nivel de seguridad.	Alto
			A9.4.4.1	Implementar el uso de utilidades con privilegios del sistema y que los mismos sean aprobados por el comité.	Alto
	Abuso de privilegios de acceso	El objetivo es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.	A9.2.4.1	Diseñar un proceso de gestión automática de autenticación de los usuarios, evitando de está manera el contacto directo de claves con el personal técnico.	Alto
			A9.2.5.1	Implementar una revisión periódica de los derechos de acceso de los usuarios.	Alto
			A9.2.6.1	Implementar un proceso formalizado de reasignación de derechos de acceso, notificando a los participes y a la directiva sobre los cambios.	Alto
			A9.1.1.1	Implementar una política de control de acceso más moderno para de esa manera aumentar la seguridad de la organización.	Alto
			A7.2.1.1	Considerar y definir claramente los roles las responsabilidades de todas las partes involucradas	Alto
			A7.2.2.1	Realizar formación sobre concienciación de la seguridad de la información de forma regular a todo el personal de la empresa.	Medio
			A7.2.3.1	Implementar y comunicar un proceso disciplinario, dando a conocer a todos los empleados de la organización.	Alto