MASTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Universitat Autònoma de Barcelona

Universitat Rovira i Virgili

Universitat de les Illes Balears

Universitat Oberta de Catalunya

Plan de implementación de la norma IOS/IEC 27001:2013

Juan Manuel Cárdenas Restrepo
Director: Antonio José Segovia Henares

Diciembre de 2014

ÍNDICE

Contenido

Tabla de contenido Imágenes

Tabla de contenido Tablas

Tabla de gráficas

1. SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL ENFOQUE Y SELECCIÓN DE LA EMPRESA

1.1 Introducción

Es importante saber que “la información es un activo que, como otros activos importantes de la empresa, es esencial para las operaciones de la organización, y en consecuencia necesita ser adecuadamente protegida”. ISO 27002:2005.

La información es presentada en las organizaciones en distintos medios como el papel, almacenada electrónicamente, trasmitid y otras, y tiene importantes propiedades que se deben mantener: disponibilidad, integridad y confidencialidad.

Es evidente que todas las organizaciones se enfrentan a diferentes tipos de amenazas (internas y externas) y vulnerabilidades como por ejemplo: espionaje, sabotaje, vandalismo, incendios, etc.; por todo ello aparece la necesidad de la seguridad de la información, área que nos permitirá protegerla adecuadamente para que nuestra organización pueda mantener su competitividad, rentabilidad y en general su existencia en la sociedad. Si la seguridad de la información fallara o no se aplicara correctamente podríamos tener distintos impactos en nuestra organización, como por ejemplo: pérdidas financieras, denuncias de las autoridades, pérdidas de clientes, pérdida de cuota de mercado, interrupción de las operaciones, daño en la imagen, etc. Por todas estas razones es importante el desarrollo de este proyecto que permitirá sentar las bases de apoyo al SGSI de la organización.

1.2 Objetivos

El objetivo es elaborar un plan de implementación de la ISO/IEC 27001 en la organización seleccionada. El proyecto establecerá las bases para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información) y por lo tanto deberá abordar las siguientes fases:

- Documentación normativa sobre las mejores prácticas en la seguridad de la información.
- Definición clara de la situación actual y de los objetivos del SGSI.
- Análisis de riesgos.
- Evaluación del nivel de cumplimiento de la ISO/IEC 27002 a una organización.
- Propuestas de proyectos para conseguir una gestión de la seguridad óptima.
- Esquema documental.

1.3 Descripción actual de la empresa

Para el proyecto seleccioné una de las empresas que más tienen que ver con el futuro de la seguridad de la información, en donde se encuentran empresas que se dedican o dedicarán a ofrecer productos y servicios de seguridad para otras empresas en la región, país y el mundo. Como empresa, cuenta con muchos aliados, pero debe fortalecerse en procesos de certificación y calidad en varias áreas con el fin de aumentar su capacidad de negociación y ofrecer confianza a los clientes nuevos y con los que cuenta actualmente.

La empresa cuenta con 315 mts cuadrados en dos pisos de un edificio que está actualmente en comodato con la alcaldía de la ciudad de Pereira, se delegaron dos personas para el apoyo a la realización de este proyecto, no cuentan con mucho tiempo dadas sus ocupaciones, ellas son la Coordinadora Administrativa y la Coordinadora de Buenas Prácticas.

Es una fundación sin ánimo de lucro que inició operaciones en marzo de 2005 con el propósito de crear y desarrollar empresas que provean al mercado productos y servicios innovadores en la industria de las Tecnologías de la Información y la economía del conocimiento.

Actualmente cuenta con más de 30 empresas dedicadas a la industria TI y servicios relacionados. Estas empresas generan actualmente empleo calificado para 125 personas, de las cuales 59 son emprendedores y los 66 restantes son colaboradores.

Hoy en día, al lado de otros en Colombia es el clúster de ciencia y tecnología informática más grande del país y uno de los más importantes líderes en apoyo a proyectos de emprendimiento con base tecnológica e investigación de paradigmas afines para aplicar al desarrollo de soluciones informáticas. Gracias al camino recorrido, la empresa recibió en el 2011 el reconocimiento internacional de la Young American Business Trust, en el 2012 fue reconocido como centro de excelencia de la organización de Estados Americanos y asimismo, obtuvo el premio nacional Gonzalo Vallejo del diario La Tarde, como la empresa más innovadora.

La empresa está trabajando en la elaboración de documentos conducentes a la certificación ISO 9001, esto es un punto de partida ya que ven el proyecto como un complemento y desde la Dirección se tiene conciencia sobre la importancia de la seguridad de la información para la empresa, directamente el Director ejecutivo de la empresa se encargó de abrir las puertas de la misma y asignar el personal de apoyo.

1.3.1 Ubicación

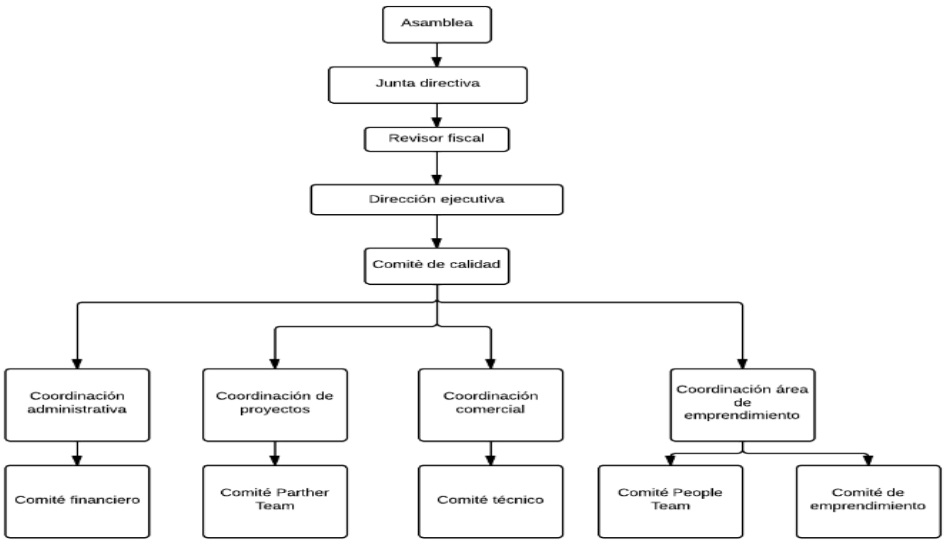
La empresa se encuentra ubicada en la ciudad de Pereira-Risaralda a la salida hacia la ciudad de Armenia-Quindío, a continuación se presenta la imagen satelital:

Imagen 1. Fotografía satelital empresa seleccionada.

Fuente: Google Maps.

1.4 Organigrama

Imagen 2. Organigrama de la empresa.



Fuente: Documento calidad empresa seleccionada.

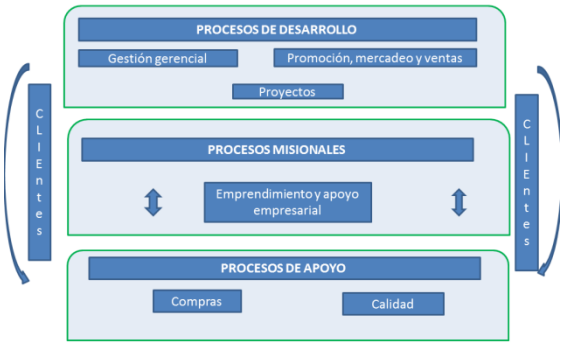
Se cuenta con los documentos que nombran las funciones y lineamientos de cada uno de los comité, perfiles de los empleados para las coordinaciones, estatutos de la empresa, reglamento interno, perfil de la dirección ejecutiva, no se cuenta con política de seguridad de la información y se evidencia que en los documentos falta ajustar con elementos de seguridad de la información.

1.4.1 Diagrama de red

La organización no cuenta con un diagrama de red, en su operación tienen una organización muy sencilla, todos los puntos están conectados a un switch que está conectado al servidor proxy que les brinda la salida a Internet, cuentan con un router inalámbrico que está conectado al switch en donde se permite la conexión inalámbrica para empleados y visitantes.

1.5 Red de procesos

Imagen 3. Red de procesos.



Fuente: Documento calidad empresa seleccionada.

1.6 Valores de la organización

Pasión: La búsqueda del conocimiento, la construcción de tecnología, el desarrollo de empresa y la generación de capital social es visceral. La ideología de la empresa se basa en un fuerte conjunto de emociones en torno al empuje y las ganas por lograr el objetivo tecnológico y de negocios del emprendedor.

Confianza: El combustible principal de los Negocios y las Redes Sociales es la Confianza. Esta acción es la que permite el desarrollo de actividades y relaciones humanas a gran velocidad. Para establecer relaciones de confianza se necesita una estructura fuerte de valores y principios, además de las competencias correctas para lograr los mejores desempeños, que generan cadenas de valor.

Trabajo duro: El proceso de construir una empresa demanda una alta inversión del Capital más grande que tiene un emprendedor; su tiempo. La fase inicial del proceso de emprendimiento es una etapa de alta cuota de sacrificio personal, cada hora que el emprendedor se distrae y no la invierta en su proyecto, la está restando a su oportunidad de éxito. En promedio un emprendedor debe trabajar en los primeros años de formación de su empresa un promedio de 12 horas diarias de lunes a domingo, del 1 de enero al 31 de diciembre, incluyendo días festivos. Esta es una de las características más diferenciadoras de los emprendedores contra el resto de la población laboral. El trabajo duro es una oportunidad de éxito, esto se debe patrocinar en los emprendedores en todo su sentido.

Sinergia: Este axioma es vital en la supervivencia y rápido desarrollo de su negocio para un emprendedor. El actuar conectado a redes de conocimiento, servicios y productos, les permite tomar ventajas competitivas sumando habilidades personales, tecnológicas y de negocios tanto a ellos como personas, como a sus proyectos. Un ambiente sinérgico acelera notoriamente la transferencia de experiencias (know how) y permite de una manera rápida e informal acompañamiento (coaching) por parte de la comunidad. Este modelo de pensamiento y acción también genera en sus entornos economías de escala.

Informalidad: En los mercados actuales de tecnología, altamente competidos, se requiere un dosis alta de innovación para poder salir y posicionarse en un nicho especifico. La innovación no es más que un acto de pensar diferente. Por eso es importante enfatizarla en los primeros años de la formación de los emprendedores, como una habilidad la informalidad de pensamiento y la informalidad de relacionarse con el entorno, convirtiéndolas en ventajas competitivas para resolver con mayor contenido de innovación, audacia y en menores tiempos los retos que plantea la formación de empresas altamente competitivas y productivas.

1.7 Activos de la organización

La empresa está situada actualmente en un predio que está en comodato con la Alcaldía de la ciudad de Pereira-Risaralda-Colombia, esto es que tiene a su cargo la administración del mismo, cuenta con 315 mts cuadrados en donde se sitúan las empresas de base tecnológica desarrolladoras de software, el espacio asignado para el área administrativa de la empresa es de 40 mts cuadrados aproximadamente. Los equipos de cómputo se sitúan todos en el primer piso al igual que el servidor y el rack. No se cuenta con cámaras de seguridad, se cuenta con un sistema de acceso por medio de clave en teclado que permite el acceso a la puerta principal en donde se encuentra el área administrativa. Se cuenta con llaves de los cajones en los puestos de trabajo que son asignadas a la persona que la ocupa en ese momento, la oficina de la dirección ejecutiva es la única que tiene puerta, el resto de las dependencias no tiene puertas, esto es política de la empresa para crear un ambiente de confianza en la comunidad.

1.7.1 Capital Humano

Director ejecutivo 1.

Coordinación Administrativa 1.

Coordinación Proyectos 1.

Coordinación Comercial 1.

Coordinación de Emprendimiento 1.

Coordinadora Calidad 1.

Revisor Fiscal 1.

Contador 1.

Auxiliares (buenas prácticas, emprendimiento, otros) 5.

1.7.2 Técnica

Planta eléctrica 1

Rack de Comunicaciones 1

Armarios de documentos 2

1.7.3 Hardware

Portátil dirección 1

Portátiles equipo de trabajo 9

Equipos de escritorio 3

Servidor proxy 1

Impresoras laser monocromática 2

Switch de 24 puertos 2

Router inalámbrico 1

1.7.4 Licencias

Todos los equipos de cómputo vienen equipados con el mismo software, cuentan con sistema operativo Windows de fábrica, Microsoft Office 2010, en algunos cuentan con licencias libres de algunos programas.

1.7.5 Información

La empresa cuenta con información que no ha valorado como activos, los contratos de toda índole están en armarios donde se almacenan, no se tiene un lugar de almacenamiento de bases de datos que son realizadas o adquiridas de terceros, los documentos como lineamientos, políticas y manuales de función son almacenados en su gran mayoría de forma digital, pero no se cuenta con un repositorio que permita hacer control de versiones o garantizar su seguridad. De la información

no se realizan copias de seguridad, puede suceder que en algún momento si un equipo se daña y es de alguna de las coordinaciones no puedan recuperar esta información.

1.8 Definición de los objetivos: Análisis diferencial ISO/IEC 27001 – 27002 y plan director de seguridad.

El alcance serán los sistemas de información que dan soporte a los procesos de desarrollo en donde se encuentran la gestión gerencial, promoción, mercadeo y ventas, proyectos, los procesos misionales que son emprendimiento y apoyo empresarial y los procesos de apoyo que son compras y calidad según la aplicabilidad vigente. La organización es pequeña en su operación, son pocas las personas que trabajan directamente con la misma, son muchos los colaboradores que son indirectos a la misma, es por este motivo que se pretende hacer un trabajo a nivel general.

1.8.1 Objetivo

El objetivo principal del trabajo de fin de máster consiste en el análisis de madurez de la organización, que es de tamaño pequeño, para la implantación de la ISO/IEC 27001 y la elaboración del Plan Director de Seguridad.

La organización desea que sean aplicadas todas las fases del SGSI para no solo conocer el estado actual en Seguridad de la Información, si no que sirva como una carta de navegación para que puedan ajustar todos los elementos que se necesitan para poder acceder a mediano plazo a una certificación en la norma ISO / IEC 27001 versión 2013.

1.8.2 Plan director de seguridad

En el desarrollo de un plan director de seguridad es primordial que la alta dirección esté de acuerdo en que se realicen las actividades que conduzcan a una correcta implementación de un sistema de gestión de seguridad de la información, también es claro que los factores humanos, organizativos, técnicos y procedimentales asociados con los sistemas de información deben considerarse, tendremos en cuenta la norma 27001:2013 y otras normativas que sean necesarias y que se puedan aplicar en la empresa.

El objetivo principal del plan director de seguridad será identificar los proyectos que la organización debe realizar en corto, mediano, y largo plazo para que se garantice la gestión de la seguridad de la información.

Después de realizar un buen análisis diferencial con la norma 27001:2013 y 27002 de buenas prácticas contrastado con el análisis de riesgos se realizarán los planes necesarios que sean basados en la estrategia de la empresa, necesidades específicas y otros que indicarán las prioridades de los mismos. La empresa debe fortalecerse al interior en seguridad de la información para que pueda proyectar seguridad y de esa forma generar confianza en los clientes y de las empresas que se encuentran incubadas al interior.

Como uno de los objetivos a corto plazo la empresa busca crear las políticas de seguridad de la información y estas poder replicarlas a las empresas que así lo deseen con un plan que seguirá las mismas pautas del que se está llevando a cabo en el presente trabajo.

1.8.2 Análisis diferencial de la empresa

Tabla 1. Análisis detallado ISO 27002

5. Política de Seguridad		
5.1 Dirección de la gestión de seguridad de la información		
5.1.1	Políticas de la seguridad de la información	No cumple
5.1.2	Revisión de las políticas de la seguridad de la información	No cumple
6. Organización de la seguridad de la información		
6.1 Organización interna		
6.1.1	Funciones y responsabilidades de seguridad de información	No cumple
6.1.2	Segregación de funciones	No cumple
6.1.3	Contacto con las autoridades.	Cumple
6.1.4	Contacto con grupos de interés especiales	Cumple
6.1.5	Seguridad de la información en la gestión de proyectos	No cumple
6.2 Dispositivos móviles y Teletrabajo		
6.2.1	Política de dispositivos móviles	Cumple
6.2.2	Teletrabajo	No cumple
7. Seguridad de Recursos Humanos		
7.1 Antes del empleo		
7.1.1	Screening	Cumple
7.1.2	Términos y condiciones de empleo	Cumple
7.2 Durante el empleo		
7.2.1	Responsabilidades de gestión	Cumple
7.2.2	Conciencia de seguridad de la información, educación y entrenamiento	Cumple
7.2.3	Proceso disciplinario	No cumple
7.3 Terminación y cambio de empleo		
7.3.1	Terminación o cambio de las responsabilidades de empleo	No cumple
8. Gestión de Activos		
8.1 Responsabilidad de los activos		
8.1.1	Inventario de Activos	No cumple

8.1.2	Propiedad de los activos	No cumple
8.1.3	Uso aceptable de los activos	No cumple
8.1.4	Retorno de los activos	No cumple
8.2 Clasificación de la Información		
8.2.1	Clasificación de la Información	No cumple
8.2.2	Etiquetado de la Información	No cumple
8.2.3	Manejo de Activos	No cumple
8.3 Manejo de Medios		
8.3.1	Gestión de medios extraíbles	No cumple
8.3.2	Eliminación de medios	No cumple
8.3.3	Transferencia de medios físicos	No cumple
9. Control de Acceso		
9.1 Business requirements of access control		
9.1.1	Política de control de acceso.	No cumple
9.1.2	Acceso a las redes y servicios de red	No cumple
9.2 Gestión de acceso de usuario		
9.2.1	Registro de usuario y cancelación de registro	No cumple
9.2.2	Acceso aprovisionamiento del usuario	No cumple
9.2.3	Gestión de derechos de accesos privilegiados	No cumple
9.2.4	Gestión de la información de autenticación de secreto de los usuarios	No cumple
9.2.5	Revisión de los derechos de acceso de usuario	No cumple
9.2.6	La eliminación o el ajuste de los derechos de acceso	No cumple
9.3 Responsabilidades del usuario		
9.3.1	El uso de información secreta de autenticación	No cumple
9.4 Control del sistemas y acceso a las aplicaciones		
9.4.1	Restricción de acceso Información	No cumple
9.4.2	Procedimientos de inicio de sesión seguro	No cumple
9.4.3	Sistema de gestión de contraseña	No cumple
9.4.4	El uso de los programas de servicios públicos privilegiados	No cumple
9.4.5	Control de acceso al código fuente del programa	No cumple

10. Criptografía		
10.1 Controles criptográficos		
10.1.1	Política sobre el uso de controles criptográficos	No cumple
10.1.2	Gestión de claves	No cumple
11 Seguridad física y ambiental		
11.1 áreas seguras		
11.1.1	Perímetro de seguridad física	No cumple
11.1.2	Controles de entrada físicas	No cumple
11.1.3	Asegurar oficinas, habitaciones e instalaciones	No cumple
11.1.4	La protección contra amenazas externas y ambientales	No cumple
11.1.5	Trabajar en zonas seguras	No cumple
11.1.6	Zonas de entrega y carga	No cumple
11.2 Equipo		
11.2.1	Ubicación y protección del equipo	No cumple
11.2.2	Apoyo a los servicios públicos	No cumple
11.2.3	seguridad cableado	No cumple
11.2.4	Mantenimiento del equipo	No cumple
11.2.5	Eliminación de los activos	No cumple
11.2.6	Seguridad de equipo y activos fuera de las instalaciones	No cumple
11.2.7	Eliminación segura o la reutilización de los equipos	No cumple
11.2.8	Equipos de usuario desatendidos	No cumple
11.2.9	Escritorio limpio y política pantalla limpia	No cumple
12. Operaciones de seguridad		
12.1 Procedimientos y responsabilidades operacionales		
12.1.1	Procedimientos operativos documentados	No cumple
12.1.2	Gestión del cambio	No cumple
12.1.3	gestión de la capacidad	No cumple
12.1.4	Separación de desarrollo, pruebas y entornos operativos	No cumple
12.2 Protección contra el malware		
12.2.1	Controles contra el malware	No cumple
12.3 Copias de seguridad		
12.3.1	Copia de seguridad de la información	No cumple

12.4 Registro y seguimiento		
12.4.1	registro de eventos	No cumple
12.4.2	Protección de la información de registro	No cumple
12.4.3	Registros de administrador y operador	No cumple
12.4.4	sincronización de reloj	No cumple
12.5 El control de software operativo		
12.5.1	La instalación del software en los sistemas operativos	No cumple
12.6 Técnico de gestión de vulnerabilidades		
12.6.1	Gestión de vulnerabilidades técnicas	No cumple
12.6.2	Las restricciones a la instalación de software	No cumple
12.7 Sistemas de información consideraciones de auditoría		
12.7.1	Sistemas de información controles de auditoría	No cumple
13. Seguridad de las comunicaciones		
13.1 Gestión de la seguridad de red		
13.1.1	Controles de red	No cumple
13.1.2	Seguridad de los servicios de red	No cumple
13.1.3	Segregación en redes	No cumple
13.2 transferencia de información		
13.2.1	Las políticas y los procedimientos de transferencia de información	No cumple
13.2.2	acuerdos sobre la transferencia de información	No cumple
13.2.3	mensajería electrónica	No cumple
13.2.4	acuerdos de confidencialidad o de no divulgación	No cumple
14. Sistema de adquisición, desarrollo y mantenimiento		
14.1 Security requirements of information systems		
14.1.1	Información de análisis de requisitos de seguridad y la especificación	No cumple
14.1.2	Asegurar los servicios de aplicaciones en las redes públicas	No cumple
14.1.3	protección de las transacciones de servicios de aplicaciones	No cumple
14.2 Seguridad en los procesos de desarrollo y de apoyo		
14.2.1	política de desarrollo seguro	No cumple
14.2.2	Procedimientos de control de cambio de sistema	No cumple

14.2.3	Revisión técnica de aplicaciones después de la plataforma operativa	No cumple
14.2.4	restricciones a los cambios en los paquetes de software	No cumple
14.2.5	Principios de ingeniería de sistemas seguros	No cumple
14.2.6	Entorno de desarrollo seguro	No cumple
14.2.7	desarrollo outsourced	No cumple
14.2.8	Pruebas de seguridad Sistema	No cumple
14.2.9	Pruebas de aceptación del sistema	No cumple
14.3 datos de prueba		
14.3.1	Protección de los datos de prueba	No cumple
15. relaciones con los proveedores		
15.1 Seguridad de la información en las relaciones con proveedores		
15.1.1	política de seguridad de la información para relaciones con los proveedores	No cumple
15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	No cumple
15.1.3	Cadena de información y tecnología de comunicación de suministro	No cumple
15.2 Gestión de la prestación de servicios de proveedores		
15.2.1	seguimiento y la revisión de los servicios de proveedores	No cumple
15.2.2	Gestión de cambios en los servicios de proveedores	No cumple
16. Información de gestión de incidentes de seguridad		
16.1 Gestión de incidentes de seguridad de la información y mejoras		
16.1.1	Responsabilidades y procedimientos	No cumple
16.1.2	Presentación de informes de eventos de seguridad de información	No cumple
16.1.3	Informes debilidades de seguridad de información	No cumple
16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	No cumple
16.1.5	Respuesta a incidentes de seguridad de la información	No cumple
16.1.6	Aprendiendo de los	No cumple

	incidentes de seguridad de la información	
16.1.7	acopio de pruebas	No cumple
17. Los aspectos de seguridad de información de la gestión de la continuidad del negocio		
17.1 Información continuidad seguridad		
17.1.1	Planificación información continuidad seguridad	No cumple
17.1.2	implementación de la información continuidad seguridad	No cumple
17.1.3	Verificar, revisar y evaluar la información de seguridad de continuidad	No cumple
17.2 despidos		
17.2.1	Disponibilidad de instalaciones de procesamiento de información	No cumple
18. conformidad		
18.1 cumplimiento de los requisitos legales y contractuales		
18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	No cumple
18.1.2	derechos de propiedad Intectual	No cumple
18.1.3	Protección de los registros	No cumple
18.1.4	Privacidad y protección de datos personales	No cumple
18.1.5	Reglamento de los controles criptográficos	No cumple
18.2 Revisiones de seguridad de información		
18.2.1	Revisión independiente de seguridad de la información	No cumple
18.2.2	El cumplimiento de las políticas y estándares de seguridad	No cumple
18.2.3	Revisión de cumplimiento técnico	No cumple

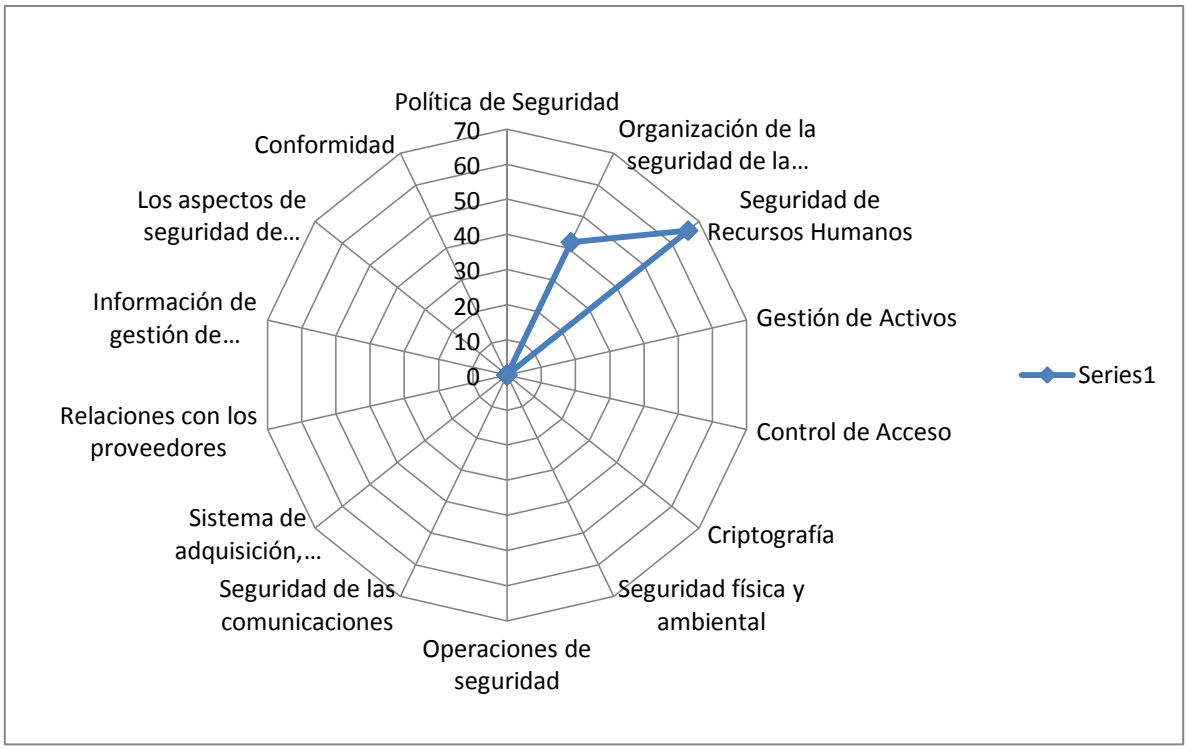
1.8.3 Resumen análisis diferencial

Tabla 2. Resumen análisis diferencial.

Dominio	Cumple %	No cumple %
Política de Seguridad	0%	100%
Organización de la seguridad de la información	42.9%	57.1%
Seguridad de Recursos Humanos	66.7%	33.3%
Gestión de Activos	0%	100%
Control de Acceso	0%	100%
Criptografía	0%	100%

Seguridad física y ambiental	0%	100%
Operaciones de seguridad	0%	100%
Seguridad de las comunicaciones	0%	100%
Sistema de adquisición, desarrollo y mantenimiento	0%	100%
Relaciones con los proveedores	0%	100%
Información de gestión de incidentes de seguridad	0%	100%
Los aspectos de seguridad de información de la gestión de la continuidad del negocio	0%	100%
Conformidad	0%	100%

Gráfica 1. Gráfica radar resumen análisis diferencial.



Fuente: elaboración propia.

La organización con respecto a las normas de referencia (ISO 27001 e ISO 27002) está muy débil, no conocen sobre el tema y no se han preocupado por implementar políticas, controles y otros elementos que le permitan estar más protegida en temas de seguridad de la información, es apenas en este acercamiento en donde la alta dirección se compromete con brindar el apoyo necesario y algunas de las personas que trabajan en la misma para que den información y ayuden a que se den los primeros pasos en temas de Sistemas de Gestión de Seguridad de la Información en la organización.

Los resultados de la gráfica anterior presenta resultados poco alentadores que motivan más a la misma organización a tomar la decisión de brindar más apoyo, no se cumple con más del 50% de los controles de buenas prácticas que nos ofrece ISO 27002:2013.

2. SISTEMA DE GESTIÓN DOCUMENTAL

2.1 Introducción

Todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo. Esto significa que en nuestro Sistema de Gestión de Seguridad de la Información tendremos que tener una serie de documentos, los cuales vienen establecidos en la propia norma ISO/IEC 27001.

2.2 Esquema Documental

2.2.1 Política de Seguridad

2.2.1.1Introducción

La información es uno de los bienes más valiosos de la organización si no el más valioso, la pérdida, deterioro, acceso no autorizado y uso no autorizado de la misma puede deteriorar procesos o toda la organización, es por esto que se debe garantizar a través de esta política de seguridad la integridad, confidencialidad y disponibilidad de la misma para minimizar los riesgos a los que se expone todos los días. La aplicación de la política y directrices de seguridad tienen un ámbito global y abarcan todos los sistemas de información, redes de comunicaciones, equipos informáticos, infraestructura informática y otros que estén a cargo de la organización.

Toda la organización es afectada por estas medidas de seguridad, el responsable de la seguridad debe poner en marcha y actualizar estas medidas y el resto de personas de la organización deben cumplirlas después de entenderlas a través de los procesos de capacitación, también comprenderán las consecuencias que acarrea no hacerlo, es importante que los visitantes, clientes y otros que no sean personal interno de la empresa cumplan con las mismas para evitar cualquier incidente de seguridad de la información en la organización.

La información contenida en este documento y en todos los que implique estándares, normas y otros sobre la seguridad de la información es de carácter confidencial con permiso de acceso a solo el personal autorizado.

2.2.1.2 Funciones y obligaciones del personal de la organización

Se presentan a continuación las funciones y obligaciones para el personal con acceso a los sistemas de información de esta organización, estas funciones y obligaciones tienen como objeto:

Garantizar la confidencialidad de la información.

Proteger los sistemas de información y las redes de comunicación propiedad de la organización o bajo su responsabilidad, contra el acceso o uso no autorizado, alteración indebida, destrucción, mal uso o robo.

Proteger la información perteneciente o proporcionada a la organización, contra revelaciones no autorizadas o accidentales, alteración, destrucción o mal uso.

Para todo el personal sin importar el cargo se deben cumplir estas obligaciones, la organización define algunos ítems que deben efectuarse con el fin de garantizar que las obligaciones se cumplan, estos son: Control de acceso físico, uso de recursos, hardware, software, correo electrónico, incidencias, propiedad intelectual.

A continuación se presentan los ítems definidos por la organización para el cumplimiento de las obligaciones:

Control de acceso físico: El acceso a las instalaciones donde se encuentran los Sistemas de Información y los locales de tratamiento, se realizará previo paso por un sistema de control de acceso físico o con autorización del responsable de las instalaciones.

Uso de recursos: Los recursos informáticos ofrecidos por la organización (datos, software, comunicaciones, etc.) están disponibles exclusivamente para cumplir con las obligaciones laborales y con una finalidad corporativa. Por lo tanto, queda terminantemente prohibido cualquier uso distinto al indicado, ejemplos: Introducir en los sistemas de información o red corporativa contenidos ilegales, inmorales u ofensivos y en general, sin utilidad para los procesos de negocio de la organización. Introducir voluntariamente programas, virus, spyware o cualquier otro software malicioso que sean susceptibles de causar alteraciones en los recursos informáticos de la organización o de terceros. Desactivar o inutilizar los programas antivirus y de protección del equipo. Intentar eliminar, modificar, inutilizar los datos, programas o cualquier otra información propios de la organización o confiados a ella. Intentar descubrir o descifrar las claves de acceso o cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la organización.

Hardware: El usuario en ningún caso accederá físicamente al interior del equipo que tiene asignado para su trabajo o que pertenezca a la propiedad de la organización. En caso necesario se comunicará la incidencia, según protocolo habilitado, para que el departamento indicado (o en su defecto el encargado de su función) realice las tareas de reparación, instalación o mantenimiento. Los usuarios no manipularán los mecanismos de seguridad que la organización implemente en los dispositivos (equipos, portátiles, móviles, smartphones, etc.). No sacar equipos, dispositivos o soportes de las instalaciones sin la autorización necesaria, y en todo caso, con los controles y medidas que se hayan establecido para cada supuesto.

Software: Los usuarios deben utilizar únicamente las versiones de software facilitadas por la organización y seguir sus normas de utilización. El director de sistemas o el encargado de su función es el responsable de definir los programas de uso estandarizado en la organización y de realizar las instalaciones en los PCs.

Correo electrónico: El servicio de correo electrónico (o cuentas de correo) que la organización pone a disposición de los usuarios tiene un uso estrictamente profesional y destinado a cubrir las necesidades de su puesto. Queda terminantemente prohibido intentar leer, borrar, copiar o modificar mensajes de correo electrónico de otros usuarios. Los usuarios no deben enviar mensajes de correo electrónico de forma masiva con fines publicitarios o comerciales. En el caso que sea necesario, dada la función del usuario, este tipo de mensajes se gestionarán con la dirección de la organización y con el responsable de seguridad. La dirección de sistemas o el encargado de su función velará por el uso correcto del correo electrónico con el fin de prevenir actividades que puedan afectar a la seguridad de los sistemas de información y de los datos.

Incidencias: El personal de la organización, clientes y otros tienen como obligación comunicar cualquier incidencia que se produzca y esté relacionada con los sistemas de información o cualquier otro recurso informático de la entidad. La comunicación, gestión y resolución de las incidencias de seguridad se realizarán mediante el sistema de gestión de incidencias habilitado por la organización.

Propiedad Intelectual: Se prohíbe a todo el personal de la organización, uso de aplicaciones informáticas sin la correspondiente licencia. Los programas informáticos propiedad de la organización están protegidos por la propiedad intelectual y por lo tanto está prohibida su reproducción, modificación, cesión o comunicación sin autorización. uso, reproducción, modificación, cesión o comunicación de cualquier otro tipo de obra protegida por la propiedad intelectual sin debida autorización.

2.2.1.3 Actualización de las pautas o directrices de seguridad

Siempre que ocurran cambios en la legislación, tecnología, riesgos de seguridad la organización podrá realizar los cambios que considere pertinentes en estas pautas o directrices de seguridad, estos cambios siempre serán comunicados a todo el personal de la organización haciendo uso de los medios que se consideren más pertinentes para ello. Se realizarán procesos de sensibilización especial a aquellas personas que tienen acceso a los sistemas de información de la organización. Después de realizarse los procesos de comunicación, sensibilización y capacitación de ser el caso de las nuevas pautas, todo el personal será responsable de cumplirlas.

2.2.1.4 Política de usuarios y contraseñas

Todos los usuarios con acceso al sistema de información dispondrán de una autorización de acceso compuesta de usuario y contraseña.

El nombre de usuario y contraseña asignados a una persona se comunicarán de forma escrita en sobre cerrado previa firma de recibido, junto con una copia de las obligaciones del personal en materia de seguridad de la información. La primera vez que la persona inicie sesión en el sistema deberá modificar la contraseña proporcionada para que esta sólo sea conocida por él.

El almacenamiento de usuarios y contraseñas se realizará utilizando los mecanismos propios de los Sistemas Operativos y aplicaciones, podrán usarse técnicas de perfiles como directorio activo y LDAP utilizando cifrado.

La longitud mínima será igual o superior a 8 caracteres alfabéticos, numéricos y especiales con excepción de caracteres como %,",&,*, será obligatorio para todo el personal de la organización.

La vigencia máxima de las contraseñas será de 90 días.

2.2.1.5 Acceso físico a las instalaciones

Se debe tener control de acceso físico a las instalaciones para prevenir el acceso accidental, no autorizado de terceros a los datos, así como prevenir accidentes y daños sobre los sistemas de información de la organización. Los entornos a proteger serán los data center si existen, dependencias con ordenadores personales y/o servidores, armarios y otras ubicaciones similares destinadas al tratamiento y almacenamiento de datos personales.

Sólo el personal autorizado tendrá el acceso permitido a los locales, instalaciones o despachos donde se encuentren los sistemas de información con datos de carácter personal.

La seguridad de los data center y almacenamiento de datos de carácter personal serán responsabilidad del responsable del archivo y responsable de seguridad.

Los equipos, soportes y documentos que contengan datos personales no serán sacados de las dependencias sin autorización expresa del responsable del archivo tal y como indica la política general de la organización.

2.2.1.6 Monitorización

Con el fin de velar por el uso correcto de los distintos sistemas de información de la organización, así como garantizar la integridad, confidencialidad y disponibilidad de los datos de la organización, la organización a través de los mecanismos formales y técnicos que considere oportuno, podría comprobar, ya sea de forma periódica o cuando la situación técnica lo requiera, la correcta utilización de los recursos de la organización por todo el personal.

En el caso de apreciar un uso incorrecto de los recursos asignados al usuario (software, correo electrónico, hardware, etc.) se le comunicará la circunstancia y se le facilitará la formación necesaria para el uso correcto de los recursos.

Si se detecta mala fe en la utilización de los recursos informáticos, la organización podría ejercer las acciones legales que le amparen para la protección de sus derechos.

2.2.1.7 Responsabilidades

En todo momento el Responsable de Seguridad velará por el cumplimiento de las normas escritas en la Política de Seguridad y la legislación vigente, y si detectan el incumplimiento de las mismas, ya sea de forma deliberada o accidental, alertará a los causantes realizando un seguimiento hasta asegurarse de que desaparece el problema. En el caso de un incumplimiento deliberado, reincidente o de relevante gravedad se analizarán las circunstancias pudiendo incurrir en la imputación de una falta disciplinaria, leve, grave o muy grave dependiendo de los hechos acontecidos. En tal caso, se adoptarán las medidas previstas y se informará a las autoridades competentes.

2.2.1.8 Revisión de la política de seguridad

Control: Las políticas de seguridad de la información deben ser revisados a intervalos planificados o si se producen cambios significativos para asegurar su conveniencia, adecuación y eficacia.

Cada política debe tener un propietario que ha aprobado la responsabilidad de gestión para el desarrollo, revisión y evaluación de las políticas. La revisión debe incluir la evaluación de oportunidades de mejora de las políticas de la organización y el enfoque de la gestión de seguridad de la información en respuesta a cambios en el entorno de la organización, las circunstancias del negocio, las condiciones jurídicas o entorno técnico.

La revisión de las políticas de seguridad de la información debe tener los resultados de las revisiones por la dirección en cuenta.

La política será revisada por el responsable de seguridad, el equipo de seguridad y la dirección, esta revisión se realizará cada año sin pasar el mes de Septiembre, la aprobación debe darse por la dirección de la organización y luego ser comunicada a todos el personal implicado en el alcance del SGSI.

La sistemática será:

- Revisión y ajustes a la política de seguridad
- Aprobación por parte de la dirección de la organización.
- Reunión con todo el personal implicado exponiendo los ajustes realizados.
- Recibo de sugerencias y otros por parte del personal.
- Tenerlas en cuenta para la próxima revisión y si es del caso retroalimentar la que se está presentando para ser aprobada de nuevo.

2.2.2 Procedimiento de auditorías internas

El objetivo es establecer los lineamientos y el procedimiento a seguir para la planificación y realización de auditorías internas al SGSI de la organización, así como para informar sus resultados y mantener los registros de calidad que se deriven de su aplicación. También es importante conocer los requisitos profesionales académicos y técnicos el auditor interno, el plan de auditoría, el informe de auditoría y el programa de auditoría.

2.2.2.1 Requisitos profesionales académicos y técnicos auditor interno:

Junto con esta dirección, el auditor jefe tendrá la responsabilidad de determinar la composición del equipo en base a:

- Los objetivos de auditoría, el alcance, los criterios y la duración estimada de la auditoría.
- La competencia general del equipo auditor necesaria para conseguir los objetivos de la auditoría.
- Los requisitos necesarios de los organismos de acreditación/certificación, si es de aplicación.
- La necesidad de asegurar la independencia del equipo auditor de las actividades a ser auditadas, y evitar conflictos de intereses.
- La capacidad de los miembros del equipo auditor para interactuar eficazmente con el auditado y trabajar conjuntamente.

Desde el punto de vista de sus características, es recomendable que los auditores jefe tengan conocimientos y habilidades adicionales a las del resto de los auditores del equipo. Estas habilidades adicionales son las de liderazgo de la auditoría, para permitir al equipo auditor llevar a cabo la auditoría de manera eficiente y eficaz. Los conocimientos y habilidades en esta área deben contemplar:

- Planificación y gestión de recursos.
- Capacidad de comunicación con el cliente de la auditoría y el auditado, para representar y defender al equipo auditor.
- Capacidad de liderazgo de personas.
- Capacidad de previsión y resolución de conflictos.
- participado, como mínimo, en tres auditorías como miembro de un equipo auditor realizando labores de auditor jefe bajo la supervisión del auditor jefe.
- Conocimientos sobre los principios de auditoría, procedimientos y técnicas que le permitan asegurarse de que las auditorías se llevan a cabo de manera coherente y sistemática. En entornos de auditorías de certificación de SGSI, este conocimiento es recomendable que se acredite mediante formación específica en auditoría, y también mediante experiencia.
- Revisión de la documentación del SGSI.
- Revisión del análisis de riesgos de una organización.
- Haber auditado la implantación de un SGSI.
- Haber desarrollado los informes relativos a la auditoría en la que participó.

2.2.2.2 Plan de auditoría

Se ha definido unos ítems que deberá llevar el plan de auditoría, para eso siempre se deberá llenar la siguiente tabla:

Tabla 3. Plan de auditoría

ITEM	DESCRIPCIÓN
Establecimiento del alcance	Se establece por la creación de un proyecto

	interno de auditoría, en este se podrán nombrar los controles a auditar.
Documento de compromiso por parte de la dirección	Lo habitual será que todo el personal de la organización haya firmado un acuerdo de confidencialidad en los términos que les sean aplicables según las funciones laborales que fueran a desarrollar.
Plazos temporales	– Fechas de inicio y fin de los periodos de prueba. – Periodos del día para realizar las pruebas. – Periodicidad del plan de auditoría. Establecer la periodicidad convierte el plan en un programa de auditoría (puede estar ligado al contenido de algún elemento de SGSI).
Procedimientos de comunicación	Con los responsables de proyecto en el auditado, especialmente para la comunicación del descubrimiento de vulnerabilidades críticas o situaciones de fraude.
Inventariado de las políticas corporativas	Que afecten a la auditoría y que van a ser comprobadas por el proceso de auditoría.
Documentación de las pruebas que se van a realizar indicando	
Objetivo de la prueba	Se tratará de identificar qué requisito de las políticas de seguridad del auditado, o en caso de no existir, qué requisito de un catálogo de buenas prácticas se va a auditar. Es por esta razón por lo que en esta fase el equipo auditor deberá estudiar las políticas y catálogos de buenas prácticas que sean de aplicación en el alcance de la auditoría.
Modo en que se realizará la prueba	Descripción, al menos somera, del procedimiento y técnicas de auditoría que se aplicarán para comprobar el/los requisito/s auditado/s.
Herramientas o requisitos específicos necesarios para realizar la prueba	

El plan de auditoría deberá estar aprobado tanto por el jefe del equipo auditor como por parte de la entidad auditada.

2.2.2.3 Informe de auditoría

Los auditores deben realizar un informe lo más simple y directo posible y siempre facilitando la información relevante, así como los distintos hallazgos realizados. Al mismo tiempo, debe facilitar de manera sencilla la forma de resolver las deficiencias halladas.

El informe final de auditoría puede seguir cualquier esquema, pero el elegido debe incluir o tratar de un modo u otro los siguientes aspectos:

Tabla 4. Informe final auditorías

ITEM	DESCRIPCIÓN
Resumen ejecutivo	Cuando se desarrolla el informe, y una vez analizada la información recogida durante la auditoría, es recomendable comenzar por este

	punto, puesto que puede requerirse por parte de la dirección una primera versión de las conclusiones de auditoría. En muchas ocasiones, esta parte del informe es la única que será leída por algunos de sus destinatarios, por lo que deberá reflejar de manera resumida su contenido. Incluirá, por tanto, una introducción, una visión general de la metodología empleada, las principales conclusiones que se hayan obtenido y las recomendaciones más relevantes que el equipo auditor pueda dar. El lenguaje empleado será lo más directo y comprensible para un público amplio.
Metodología empleada	Se debe dar una breve explicación de la metodología que se ha empleado. Se hará referencia a los estándares empleados o bien si se emplean estándares propios deberán ser explicados, detallando los objetivos, las fases y las técnicas utilizadas para realizar la auditoría. El receptor del informe debe conocer con qué criterios y de qué modo se ha realizado el trabajo. En este apartado se detallarán las pruebas, las entrevistas, las herramientas empleadas, los plazos en los que se realizó cada prueba, etc.
Listado detallado de los hallazgos	A continuación se dará un completo detalle de las pruebas y hallazgos realizados. El modo en que se organice este apartado dependerá exclusivamente del alcance de la auditoría y del detalle al que se haya llegado. Por claridad es recomendable facilitar en hojas independientes hallazgos independientes. De cada hallazgo se podrá realizar una evaluación de su importancia o impacto que podría causar en la organización y de este modo clasificar su criticidad. La técnica empleada es la anteriormente mencionada en la fase de análisis de realizar una estimación del riesgo empleando alguna de las metodologías de análisis de riesgos existentes, aunque cuanto más sencilla y fácil de transmitir al auditado, mejor. Esta información se podrá incluir en el informe. Es de gran utilidad dar una clasificación de la importancia de los hallazgos puesto que será empleada por el destinatario del informe para realizar el seguimiento de la resolución o mejora.
Anexos	En los anexos se deberá recopilar la información que dé respaldo a los hallazgos descritos en el cuerpo del informe. Incorporan, por tanto, las salidas de las herramientas que se empleen, los resultados de los *checklist* realizados, las actas de las reuniones celebradas, etc. También incluirán los detalles de la resolución recomendada a los hallazgos cuando por su complejidad requieran una explicación más extensa.

2.2.2.4 Programa de auditoría

Las auditorías se realizarán una vez por año para el ciclo PDCA de la ISO 27001, todos los años se realizarán los planes de auditoría y se emitirán informes para esto, serán en el mes de Octubre.

En el período de tiempo de 3 años se realizarán las auditorías una por año para diferentes dominios de controles, para que al cabo de los tres años estén cubiertos todos los controles.

En el año 1, mes de Agosto se realizará la auditoría a los dominios:

- Política de seguridad
- Organización de la seguridad de la información.
- Seguridad en los recursos humanos
- Gestión de activos
- Control de acceso

En el año 2, mes de Agosto se realizará la auditoría a los dominios:

- Cifrado
- Seguridad física y ambiental
- Operaciones de seguridad
- Gestión de comunicaciones y operaciones.
- Adquisición, desarrollo y mantenimiento de Sistemas de Información

En el año 3, mes de Agosto se realizará la auditoría a los dominios:

- Relaciones con proveedores
- Gestión de incidentes
- Gestión de continuidad de negocio
- Cumplimiento /Conformidad

2.2.2.5 Descripción del procedimiento

En la siguiente tabla se detalla el procedimiento definiendo el número de la actividad, la actividad y el responsable.

Tabla 5. Detalle procedimiento auditorías internas.

No	ACTIVIDAD	RESPONSABLE
Elaboración, Aprobación y Difusión del Programa Anual de Auditorías		
1	Elabora el Programa Anual de Auditorías del SGSI, para un periodo determinado.	Director de la organización o el representante de la Dirección y Responsable de Seguridad de la Información.
2	Aprueba el Programa Anual de Auditorías del SGSI.	Junta directiva.
Elaboración del Plan de Auditorías Internas		
3	Coordina con los responsables de las áreas involucradas, la(s) fecha(s) y hora(s) de ejecución de la auditoría, a fin de asegurar su disponibilidad durante la auditoría interna.	Director de la organización o el representante de la Dirección y Responsable de Seguridad de la Información.
4	Selecciona a los auditores internos que conformarán el Equipo Auditor, de acuerdo a los perfiles propuestos de	Director de la organización o el representante de la Dirección y

	Puesto del Auditor Interno Así como, de ser necesario, selecciona a la(s) persona(s) que participará(n) como experto(s) técnico(s) y observador(es).	Responsable de Seguridad de la Información.
5	Nombra a un Auditor Interno como Auditor Líder para que dirija el proceso de auditoría interna; considerando la experiencia previa y procesos a ser auditados.	Director de la organización o el representante de la Dirección y Responsable de Seguridad de la Información.
6	Prepara el Plan de Auditoría Interna para el SGSI, se definen las fecha(s), hora(s), itinerarios de auditoría, auditados, criterios de la auditoría y auditores.	Auditor Líder
7	Comunica el Plan de Auditoría Interna al personal involucrado en los procesos a ser auditados.	Auditor Líder
Preparación de la Auditoría Interna		
8	Revisa la documentación pertinente de los procesos a auditar teniendo en consideración los resultados de auditorías previas y/o cláusulas de la norma ISO/IEC 27001:2013.	Auditor Líder
Apertura de Auditoría		
9	Realiza la Reunión de Apertura con el personal involucrado de acuerdo al Plan de Auditoría Interna establecido, confirmando los horarios, responsables y procesos a ser auditados; en caso de ser necesario, modifica el Plan de Auditoria.	Auditor Líder
Ejecución de la Auditoria		
10	Audita los procesos y/o áreas previstas haciendo uso de la norma ISO/IEC 27001:2013, y procede a recoger evidencias objetivas de las mismas a través de entrevistas, observación de actividades y revisión de registros, con la finalidad de verificar la implementación y efectividad del SGSI.	Equipo auditor
11	Informa al área auditada de los hallazgos encontrados durante el proceso de auditoría.	Equipo auditor
Registros de No Conformidades		
12	Redacta las no conformidades indicando en qué cláusula de la norma ISO/IEC 27001:2013 se está incumpliendo.	Equipo auditor
Elaboración del Informe de Auditoría Interna		
13	Elabora Informe de Auditoría Interna.	Auditor Líder
14	Presenta el Informe de Auditoría Interna a la junta directiva anexando las Solicitudes de Acción, de ser necesario.	Auditor Líder
Cierre de Auditoría		
15	Realiza la Reunión de Cierre de acuerdo al Plan de Auditoría Interna, acordando los plazos para levantar las no conformidades detectadas.	Auditor Líder
16	Gestiona el tratamiento de las no conformidades según lo establecido en el Procedimiento de Acciones Preventivas y Correctivas.	Director de la organización o el representante de la Dirección y Responsable de Seguridad de la Información.
17	Evalúa a cada auditor interno, después de la auditoría interna.	Director de la organización o el representante de la Dirección y Responsable de Seguridad de la Información.

2.2.3 Gestión de indicadores

Los indicadores son importantes porque sirven para medir la eficacia de los controles de seguridad implantados, a continuación se presenta la lista de indicadores.

Descripción del indicador. Explicación del objetivo de medida de dicho indicador.

Fórmula de cálculo. Descripción de la fórmula aplicada para obtener la medición. Es importante que los parámetros que intervienen sean concretos y no se presten a ambigüedad.

Frecuencia de medición. Cada cuánto se debe recoger la medición. Es posible establecer una frecuencia inicial durante un período de tiempo, y una frecuencia posterior mayor (por ejemplo, quincenal los tres primeros meses, y mensual a partir del cuarto mes). En cualquier caso, la frecuencia dependerá de la variabilidad en el tiempo de la medición.

Valor objetivo y valor umbral, es decir y respectivamente, cuál es el valor que sería correcto para la compañía y cuál es el valor por debajo del cual se debiera levantar una alarma.

Responsable de la medida. Sobre quién o, preferiblemente, sobre qué cargo recae la responsabilidad de proporcionar el resultado de la medida.

Tabla 6. Indicador número de revisiones de la política de seguridad por parte de la dirección

Descripción del indicador	Medida del número de revisiones de la política de seguridad por parte de la dirección
Fórmula de cálculo	Número de revisiones realizadas
Frecuencia de revisión	2 veces por año
Responsable de las mediciones	Responsable de seguridad
Valor umbral	<1
Valor objetivo	2

Tabla 7. Indicador número de auditorías internas realizadas

Descripción del indicador	Medida del número de auditorías internas realizadas
Fórmula de cálculo	Número de auditorías internas realizadas
Frecuencia de revisión	2 veces por año
Responsable de las mediciones	Responsable de seguridad
Valor umbral	<1
Valor objetivo	2

Tabla 8. Indicador número de auditorías externas realizadas

Descripción del indicador	Medida del número de auditorías externas realizadas
Fórmula de cálculo	Número de auditorías externas realizadas
Frecuencia de revisión	1 vez por año
Responsable de las mediciones	Responsable de seguridad
Valor umbral	<1

Valor objetivo	1

Tabla 9. Indicador mantenimientos realizados a la infraestructura física contra amenazas externas

Descripción del indicador	Medida de mantenimientos realizados a la infraestructura física contra amenazas externas
Fórmula de cálculo	Número de mantenimientos realizados
Frecuencia de revisión	1 vez por año
Responsable de las mediciones	Responsable de seguridad
Valor umbral	<1
Valor objetivo	1

Tabla 10. Indicador programas maliciosos detectados en los equipos y servidores

Descripción del indicador	Medida de programas maliciosos detectados en los equipos y servidores
Fórmula de cálculo	(Número programas encontrados / Número total de equipos) * 100
Frecuencia de revisión	2 veces al año
Responsable de las mediciones	Responsable de seguridad
Valor umbral	>30%
Valor objetivo	<20%

Tabla 11. Indicador acuerdos de intercambio de datos

Descripción del indicador	Medida de acuerdos de intercambio de datos
Fórmula de cálculo	Número de acuerdos de intercambio de datos
Frecuencia de revisión	1 vez al año
Responsable de las mediciones	Responsable de seguridad
Valor umbral	<1
Valor objetivo	1

Tabla 12. Indicador usuarios dados de baja

Descripción del indicador	Medida de usuarios dados de baja
Fórmula de cálculo	(Número de usuarios dados de baja/Número de usuarios despedidos)*100
Frecuencia de revisión	2 veces al año
Responsable de las mediciones	Responsable de seguridad
Valor umbral	<90%
Valor objetivo	99%

Tabla 13. Indicador incidentes de seguridad

Descripción del indicador	Medida de incidentes de seguridad
Fórmula de cálculo	Número de incidentes de seguridad ocurridos
Frecuencia de revisión	1 vez por mes
Responsable de las mediciones	Responsable de seguridad

Valor umbral	>2
Valor objetivo	0

Tabla 14. Indicador dispositivos perdidos

Descripción del indicador	Medida de dispositivos perdidos
Fórmula de cálculo	(Número de dispositivos perdidos/Número de dispositivos en inventario)*100
Frecuencia de revisión	1 vez al año
Responsable de las mediciones	Responsable de seguridad
Valor umbral	15%
Valor objetivo	5%

Tabla 15. Indicador Documentación de seguridad elaborada respecto a la esperada

Descripción del indicador	Medida Documentación de seguridad elaborada respecto a la esperada
Fórmula de cálculo	[(Número documentos seguridad / Número ideal de documentos seguridad) * 100
Frecuencia de revisión	1 vez por año
Responsable de las mediciones	Responsable de seguridad
Valor umbral	<70%
Valor objetivo	80%

Tabla 16. Indicador Equipos sin antivirus instalado

Descripción del indicador	Medida Equipos sin antivirus instalado
Fórmula de cálculo	(Número equipos sin antivirus / Número total equipos) *100
Frecuencia de revisión	2 veces al año
Responsable de las mediciones	Responsable de seguridad
Valor umbral	>20%
Valor objetivo	10%

Tabla 17. Indicador Copias de seguridad fallidas

Descripción del indicador	Medida Copias de seguridad fallidas
Fórmula de cálculo	(Número copias fallidas / Número total copias) *100
Frecuencia de revisión	1 vez por mes
Responsable de las mediciones	Responsable de seguridad
Valor umbral	>15%
Valor objetivo	5%

Tabla 18. Indicador Accesos no autorizados a la red de la organización

Descripción del indicador	Medida Accesos no autorizados a la red de la organización
Fórmula de cálculo	(Número accesos no autorizados a la red /

	Número total de accesos) *100
Frecuencia de revisión	1 vez por mes
Responsable de las mediciones	Responsable de seguridad
Valor umbral	<20%
Valor objetivo	10%

2.2.4 Procedimiento de revisión por dirección

En la toma de decisiones relacionada con la seguridad de la información, debe participar la dirección de la organización de forma activa y efectiva, así se garantiza que el SGSI pueda funcionar de forma correcta en la organización, también la dirección debe usar mecanismos que le permita hacer un seguimiento de los controles, procedimientos y otros que brinden la información para la correcta toma de estas decisiones.

La Dirección de la organización deberá participar en la toma de decisiones relacionada con la seguridad de la información y hacer un "seguimiento" de los procedimientos, controles, u otros mecanismos implementados para garantizar el buen funcionamiento del SGSI.

Este apartado tiene como objetivo describir cual será el procedimiento de revisión de la dirección como acción indispensable en el SGSI.

La Dirección realizará, con un periodo inferior a un año, controles para verificar el cumplimiento de todos los estándares, normas y procedimientos establecidos en el SGSI. El Responsable de Seguridad será el encargado de realizar esta revisión.

El análisis de la situación se realizará al menos sobre las siguientes áreas / controles:

- Comprobación del conocimiento de las normas de seguridad por parte de las personas que acceden a los sistemas de información de la organización.
- Control, revisión y evaluación de registros de: usuarios, incidencias de seguridad, inventario de activos, etc.
- Control de autorizaciones de delegación de funciones relacionadas con la seguridad.

El Responsable de Seguridad realizará un breve informe sobre la revisión realizada anualmente. En este se incluirán las incidencias y deficiencias detectadas y una relación de soluciones y propuestas de mejora.

La organización, además de mantener actualizado los documentos del SGSI, y realizará una revisión, teniendo presente los últimos informes de auditoría, las incidencias y las revisiones internas.

La Dirección se encargará de revisar el resultado de las auditorías internas anuales y hacer un seguimiento de las acciones correctivas (al menos semestralmente). Se actuará de la misma manera con las auditorías externas con una frecuencia de 3 años, haciendo un seguimiento de las acciones al menos de forma anual.

De forma puntual se solicitará (al menos una vez al año) un resumen de los indicadores de seguridad y se analizarán en el comité de seguridad.

2.2.5 Gestión de roles y responsabilidades

El Sistema de Gestión de Seguridad de la Información tiene que estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema. Este equipo de trabajo, conocido habitualmente como Comité de Seguridad, debe estar compuesto al menos por una persona de Dirección, para que de esta manera las decisiones que se tomen puedan estar respaldadas por alguien de la Dirección de la organización.

2.2.5.1 Comité de seguridad

Este comité lo integran diferentes personas responsables de la organización, es un equipo que puede tener diferentes disciplinas, este equipo lo sugiere la dirección de la organización junto con el responsable de la seguridad y es presentado y aprobado por la junta directiva de la organización, sus funciones son:

Asignar roles y funciones en materia de seguridad de información al personal de la organización.

Hacer cumplir las políticas emanadas por el comité de dirección.

Participar en la aprobación de políticas, normas y responsabilidades en materia de seguridad de información en la organización.

Validar el plan director de seguridad de información de la organización.

Vigilar que se esté cumpliendo con la legislación actual en materia de seguridad de la información.

Realizar campañas de capacitación en materia de seguridad de la información en la organización.

Aprobar y revisar periódicamente el SGSI.

Validar el mapa de riesgos y sus acciones.

Participar en la resolución de conflictos presentados por el personal en materia de seguridad de la información.

Las personas que participarán de la organización son:

Representante de la junta directiva

Representante de la dirección ejecutiva

Coordinadora operativa o su representante

Coordinadora Administrativa o su representante

Director del departamento de sistemas o su representante

Responsable de la seguridad de la información

Representante de los empleados

2.2.5.2 Funciones y obligaciones del personal

Todo el personal que tenga acceso a los sistemas de información está en la obligación de cumplir y respetar las normas, políticas definidas de forma general y específica, también deberán cumplir solo con las funciones que han sido brindadas en su contrato laboral con respecto a la seguridad de la información. Sin importar el cargo y funciones todos deberán cumplir con la confidencialidad de la información, documentación recibida o creada que pertenezca a la organización, no podrán revelar información de ningún tipo a externos sin previa autorización, no podrán incorporar ninguna información a los sistemas de información sin autorización, los datos no podrán ser usados con otra finalidad que las que se les dio la autorización, deberán comunicar cualquier incidencia que tengan en materia de seguridad de la información al responsable de la seguridad de la información de la organización.

2.2.5.3 Funciones y obligaciones del responsable de la seguridad de la información

El responsable seguridad de la información de la organización coordina y controla las medidas de seguridad de información aplicables en la organización, esta persona es propuesta por la dirección de la organización según el perfil definido y es aprobada por la junta directiva de la misma.

El responsable de seguridad de la información debe cumplir las siguientes funciones y obligaciones:

Asesorar la definición y validar la implantación de los requisitos sobre las medidas de seguridad de la información necesaria en la organización.

Actualizar normas y procedimientos de seguridad de la información que le puedan servir a la organización.

Confirmar la ejecución de los controles establecidos en los documentos de seguridad de la información.

Realizar informes sobre las revisiones de los sistemas de seguridad de la información realizados periódicamente.

Establecer y comprobar que se están aplicando los procedimientos de: copia de respaldo, recuperación de datos, notificación de incidencias, gestión de incidencias y otros procedimientos definidos en los documentos de seguridad de la información.

Verificar que se están realizando las auditorías de seguridad de la información en los tiempos definidos.

Aplicar las medidas correctivas que resulten del análisis de los informes de auditorías de seguridad de la información en la organización.

Analizar las incidencias de seguridad de la información y gestionar las medidas correctivas.

Preparar el plan de formación para poner en marcha las medidas de seguridad de la información en la organización.

2.2.6 Metodología de análisis de riesgos

Establece la sistemática que se seguirá para calcular el riesgo, incluye la identificación y valoración de los activos, amenazas y vulnerabilidades.

Para realizar la metodología de análisis de riesgos se tomarán algunos elementos como base de MAGERIT, se pretende conocer cuánto está en juego y como se protegerá.

Se pretende realizar unos pasos para determinar el riesgo que son:

Determinar los activos relevantes para la Organización, su interrelación y su valor, que costo supondría su degradación.

Determinar las amenazas a la que están expuestos estos activos.

Determinar salvaguardas dispuestas y efectividad ante el riesgo.

Estimar el impacto, cuando se hace efectiva una amenaza sobre el activo.

Estimar el riesgo, como el impacto ponderado con la tasa de ocurrencia de la amenaza.

El análisis se realizará mediante tablas, que permiten la identificación de la importancia relativa de

los diferentes activos sometidos a amenazas.

2.2.6.1 Recolección de datos

En esta fase se definirá el alcance y se analizarán los procesos de la organización.

2.2.6.2 Establecimiento de Parámetros

Se identificarán los parámetros que se utilizarán durante el análisis de riesgos, los parámetros son:

Valoración de los activos: El valor económico se asignará al objeto analizado, se tendrá en cuenta el valor de reposición, configuración y uso.

Se presenta en la siguiente tabla la valoración, rango y valor:

Tabla 19. Valoración análisis de riesgos de los activos de la organización.

Valoración	Rango	Valor

Muy alta	Valor > $50.000.000	$60.000.000
Alta	$30.000.000<Valor>$50.000.000	$35.000.000
Media	$20.000.000<Valor>$30.000.000	$25.000.000
Baja	$10.000.000<Valor>$20.000.000	$15.000.000
Muy baja	Valor<$10.000.000	$7.000.000

Impacto: Se entiende como impacto el tanto por ciento del activo que se pierde en caso de que un impacto suceda sobre él.

Tabla 20. Impacto sobre activos en el análisis de riesgos.

Impacto	Rango
Muy alto	100%
Alto	75%
Medio	50%
Bajo	25%
Muy bajo	5%

Efectividad de los controles de seguridad: indicará la efectividad de las medidas de protección de los riesgos, pueden reducir la vulnerabilidad o el impacto dependiendo del control.

Tabla 21. Efectividad de controles de seguridad según análisis de riesgos.

Variación Impacto / Vulnerabilidad	Valor
Muy alto	95%
Alto	75%
Medio	50%
Bajo	30%
Muy bajo	10%

2.2.6.3 Análisis de activos

Se identificarán los activos de la empresa que se requieren para llevar a cabo la actividad. La organización puede poseer distintos tipos de activos físicos, lógicos, infraestructura, intangibles y

se valorarán teniendo en cuenta los parámetros de valoración de activos.

2.2.6.4 Análisis de amenazas

Las amenazas son aquellas situaciones que pueden provocar un problema de seguridad, según MAGERIT se clasifican en estos grupos:

Accidentes: Situaciones no provocadas voluntariamente y que la mayor parte de las veces no puede evitarse. Por ejemplo: incendio, inundación, etc.

Errores: Situaciones provocadas involuntariamente provocadas por el desarrollo de las actividades cotidianas ya sea por desconocimiento y/o descuido. Por ejemplo: Errores de desarrollo, errores de actualización, etc.

Amenazas intencionales presenciales: Son provocadas por el propio personal de la organización de forma voluntaria y conociendo el daño que puede ocasionar. Por ejemplo: Accesos no autorizados, filtración de datos, etc.

Amenazas intencionales remotas: Son provocadas por terceras personas ajenas a la organización con el objetivo de dañarla. Ejemplos: Suplantación de origen, gusanos, DoS, etc.

2.2.6.5 Establecimiento de las vulnerabilidades

Las vulnerabilidades son aquellos huecos de seguridad que permiten explotar una amenaza haciendo daño a un activo. No es necesario en la metodología MAGERIT listar las vulnerabilidades pero sí tenerlas identificadas para poder estimar la frecuencia de la ocurrencia de una determinada amenaza sobre un activo.

2.2.6.6 Valoración de impactos

Las amenazas pueden dañar los activos de la organización, es necesario cuantificar el impacto de una amenaza sobre el activo. Por ejemplo: daño económico, pérdidas cualitativas, etc.

2.2.6.7 Análisis de riesgos intrínseco

Son aquellos a los que la organización está expuesta sin tener en consideración las medidas de seguridad que podamos implantar.

Fórmula para el cálculo: Riesgo = Valor del activo x Vulnerabilidad x Impacto

Tabla 22. Nivel aceptable de riesgos intrínsecos según análisis de riesgos.

Nivel aceptable	Valor
Alto	80%

Medio	50%
Bajo	20%

2.2.6.8 Influencia de salvaguardas

Se hará uso de dos tipos de salvaguardas, preventivas y correctivas, con estas se pretende luego de analizar los riesgos aplicar la mejor solución para minimizarlos.

Preventivas: Nueva vulnerabilidad = Vulnerabilidad x % disminución vulnerabilidad.
Correctivas: Nuevo impacto = Impacto x % disminución impacto.

2.2.6.9 Análisis de riesgos efectivos

Luego de aplicar salvaguardas se debe calcular el riesgo efectivo, este se calcula con la siguiente fórmula:

Valor efectivo × Nueva vulnerabilidad × Nuevo Impacto = Valor activo × (Vulnerabilidad × Porcentaje de disminución de vulnerabilidad) × (Impacto × Porcentaje de disminución de impacto) = Riesgo intrínseco × Porcentaje de disminución de vulnerabilidad × Porcentaje de disminución de impacto

2.2.6.10 Gestión de riesgos

Se tomarán las decisiones que permitan aplicar las medidas de seguridad, para esto se debe tener presente el riesgo aceptable y el costo de la aplicación de estas medidas de seguridad en la organización, se usaran para gestionarlos la estrategia de reducirlos, transferirlos o aceptarlos.

2.2.7 Declaración de aplicabilidad

Tabla 23. Dominios ISO 27002 declaración de aplicabilidad.

5. Política de Seguridad				
5.1 Dirección de la gestión de seguridad de la información			Objetivo: Proporcionar la dirección de gestión y apoyo a la seguridad de la información de acuerdo con los requerimientos del negocio y las leyes y reglamentos pertinentes.	
5.1.1	Políticas de la seguridad de la información	Aplica	Descripción: Un conjunto de políticas de seguridad de la información debe ser definido, aprobado por la administración, publicar y comunicar a	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.

			los empleados y colaboradores externos.	
5.1.2	Revisión de las políticas de la seguridad de la información	Aplica	Descripción: Las políticas de seguridad de la información deben ser revisados a intervalos planificados o si se producen cambios significativos para asegurar su conveniencia, adecuación y eficacia.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
6. Organización de la seguridad de la información				
6.1 Organización interna			Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la organización.	
6.1.1	Funciones y responsabilidades de seguridad de información	Aplica	Descripción: Todas las responsabilidades de seguridad de la información deben ser definidos y asignados.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
6.1.2	Segregación de funciones	Aplica	Descripción: Las funciones en conflicto y áreas de responsabilidad deben estar separados para reducir las oportunidades para la modificación o mal uso de los activos de la organización no autorizado o involuntario.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
6.1.3	Contacto con las autoridades.	Aplica	Descripción: Los contactos pertinentes con las autoridades pertinentes deben mantenerse.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
6.1.4	Contacto con grupos de interés especiales	Aplica	Descripción: Los contactos pertinentes con los grupos de interés u otros foros de seguridad especializada y las asociaciones profesionales deben mantenerse.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
6.1.5	Seguridad de la información en la gestión de proyectos	Aplica	Descripción: Seguridad de la información debería abordarse en la gestión de proyectos,	Justificación: la organización necesita aplicar el control para poder

			independientemente del tipo de proyecto.	acceder posteriormente a la certificación.
6.2 Dispositivos móviles y Teletrabajo			Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.	
6.2.1	Política de dispositivos móviles	Aplica	Descripción: Una política y el apoyo a las medidas de seguridad deben adoptarse para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
6.2.2	Teletrabajo	Aplica	Descripción: Una política y el apoyo a las medidas de seguridad se deben implementar para proteger la información visitada, procesada o almacenada en los sitios de trabajo a distancia.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
7. Seguridad de Recursos Humanos				
7.1 Antes del empleo			Objetivo: Asegurarse de que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.	
7.1.1	Screening	Aplica	Descripción: Controles de verificación de antecedentes de todos los candidatos a empleo deben llevarse a cabo de acuerdo con las leyes, regulaciones y ética y debe ser proporcional a los requerimientos del negocio, la clasificación de la información para acceder a ellos y los riesgos percibidos.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
7.1.2	Términos y condiciones de empleo	Aplica	Descripción: Los acuerdos contractuales con los empleados y contratistas deben indicar y	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la

			responsabilidades de sus de la organización para la seguridad de la información.	certificación.
7.2 Durante el empleo		Objetivo: Asegurarse de que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información.		
7.2.1	Responsabilidades de gestión	Aplica	Descripción: La administración debe exigir a todos los empleados y contratistas para aplicar seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
7.2.2	Conciencia de seguridad de la información, educación y entrenamiento	Aplica	Descripción: Todos los empleados de la organización y, en su caso, los contratistas deben recibir una educación adecuada conciencia y la formación y actualizaciones periódicas en las políticas y procedimientos de la organización, como relevantes para su función de trabajo.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
7.2.3	Proceso disciplinario	Aplica	Descripción: Debe haber un proceso disciplinario formal y comunicado en lugar de tomar medidas contra los empleados que hayan cometido una violación de la seguridad de la información.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
7.3 Terminación y cambio de empleo		Objetivo: Proteger los intereses de la organización, como parte del proceso de cambiar o terminar el empleo.		
7.3.1	Terminación o cambio de las	Aplica	Descripción: Las responsabilidades	Justificación: la organización

	responsabilidades de empleo		de seguridad de la Información y deberes que siguen vigentes después de la terminación o cambio de trabajo deberían ser definidos, comunicado al trabajador o contratista y forzada.	necesita aplicar el control para poder acceder posteriormente a la certificación.
8. Gestión de Activos				
8.1 Responsabilidad de los activos		Objetivo: Identificar activos de la organización y definir las responsabilidades de protección adecuados.		
8.1.1	Inventario de Activos	Aplica	Descripción: Los activos asociados a las instalaciones de procesamiento de información y la información deben ser identificados y un inventario de estos activos deben elaborarse y mantenerse.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
8.1.2	Propiedad de los activos	Aplica	Descripción: Los activos mantenidos en el inventario deben ser de propiedad.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
8.1.3	Uso aceptable de los activos	Aplica	Descripción: Normas para el uso aceptable de la información y de los activos asociados a las instalaciones de procesamiento de información y la información deben ser identificados, documentados e implementados.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
8.1.4	Retorno de los activos	Aplica	Descripción: Todos los empleados y los usuarios externos del partido deben devolver todos los activos de la organización en su poder a la terminación de su	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.

			empleo, contrato o acuerdo.	
8.2 Clasificación de la Información		Objetivo: Asegurar que la información recibe un nivel adecuado de protección de acuerdo con su importancia para la organización.		
8.2.1	Clasificación de la Información	Aplica	Descripción: La información debe ser clasificada en términos de requisitos legales, el valor, la criticidad y sensibilidad a la divulgación o modificación no autorizada.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
8.2.2	Etiquetado de la Información	Aplica	Descripción: Un conjunto apropiado de los procedimientos para el etiquetado información debe ser desarrollado e implementado de acuerdo con el esquema de clasificación de la información adoptado por la organización.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
8.2.3	Manejo de Activos	Aplica	Descripción: Procedimientos para la manipulación de los activos deben ser desarrollados e implementados de acuerdo con el esquema de clasificación de la información adoptado por la organización.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
8.3 Manejo de Medios		Objetivo: Evitar la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios de comunicación.		
8.3.1	Gestión de medios extraíbles	Aplica	Descripción: Deberían aplicarse procedimientos para la gestión de medios extraíbles de acuerdo con el esquema de clasificación adoptado por la	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.

			organización.	
8.3.2	Eliminación de medios	Aplica	Descripción: Los medios deben ser eliminados de forma segura cuando ya no es necesario, utilizando los procedimientos formales.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
8.3.3	Transferencia de medios físicos	Aplica	Descripción: Los medios que contienen información deben estar protegidos contra el acceso no autorizado, mal uso o la corrupción durante el transporte.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
9. Control de Acceso				
9.1 Business requirements of access control		Objetivo: Limitar el acceso a las instalaciones de procesamiento de la información y de la información.		
9.1.1	Política de control de acceso.	Aplica	Descripción: Una política de control de acceso debe ser establecido, documentado y revisado en base a los requisitos de seguridad de negocios y de información.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
9.1.2	Acceso a las redes y servicios de red	Aplica	Descripción: Los usuarios sólo deben contar con acceso a los servicios de red y de la red que han sido autorizados específicamente para su uso.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
9.2 Gestión de acceso de usuario		Objetivo: Garantizar el acceso del usuario autorizado y evitar el acceso no autorizado a sistemas y servicios.		
9.2.1	Registro de usuario y cancelación de registro	Aplica	Descripción: Un proceso formal de registro de usuario y la cancelación del registro debe ser implementado para permitir la asignación de derechos de acceso.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.

9.2.2	Acceso aprovisionamiento del usuario	Aplica	Descripción: Un proceso de provisión de acceso de usuarios formal debe ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuario a todos los sistemas y servicios.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
9.2.3	Gestión de derechos de accesos privilegiados	Aplica	Descripción: La asignación y utilización de los derechos de acceso privilegiados deben ser restringidas y controladas.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
9.2.4	Gestión de la información de autenticación de secreto de los usuarios	Aplica	Descripción: La asignación de la información secreta de autenticación debe ser controlada a través de un proceso de gestión formal.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
9.2.5	Revisión de los derechos de acceso de usuario	Aplica	Descripción: Los propietarios de activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
9.2.6	La eliminación o el ajuste de los derechos de acceso	Aplica	Descripción: Los derechos de acceso de todos los empleados y usuarios de partidos externos a las instalaciones de procesamiento de información y la información deben ser retirados a la terminación de su empleo, contrato o convenio, o ajustarse a cambio.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
9.3 Responsabilidades del usuario		Objetivo: Hacer que los usuarios sean responsables de salvaguardar su información de autenticación.		
9.3.1	El uso de	Aplica	Descripción: Los	Justificación: la

	información secreta de autenticación		usuarios deben ser obligados a seguir las prácticas de la organización en el uso de información secreta de autenticación.	organización necesita aplicar el control para poder acceder posteriormente a la certificación.
9.4 Control del sistemas y acceso a las aplicaciones		Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.		
9.4.1	Restricción de acceso Información	Aplica	Descripción: El acceso a las funciones de información y sistema de aplicación debe limitarse de acuerdo con la política de control de acceso.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
9.4.2	Procedimientos de inicio de sesión seguro	Aplica	Descripción: Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de conexión segura.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
9.4.3	Sistema de gestión de contraseña	Aplica	Descripción: Sistemas de gestión de contraseña deben ser interactivos y deben asegurarse de contraseñas de calidad.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
9.4.4	El uso de los programas de servicios públicos privilegiados	Aplica	Descripción: El uso de programas de utilidades que podrían ser capaces de anular sistemas y aplicaciones controles debe ser restringido y estrechamente controlado.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
9.4.5	Control de acceso al código fuente del programa	Aplica	Descripción: El acceso al código fuente del programa debe ser restringido.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la

				certificación.
10. Criptografía				
10.1 Controles criptográficos		Objetivo: Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y / o integridad de la información.		
10.1.1	Política sobre el uso de controles criptográficos	Aplica	Descripción: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollado e implementado.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
10.1.2	Gestión de claves	Aplica	Descripción: Una política sobre el uso, la protección y la duración de las claves de cifrado debe ser desarrollado e implementado a través de todo su ciclo de vida.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
11 Seguridad física y ambiental				
11.1 áreas seguras		Objetivo: Evitar autorizado física de acceso, daños e interferencia a la información y procesamiento de información sobre las instalaciones de la organización.		
11.1.1	Perímetro de seguridad física	Aplica	Descripción: Perímetros de seguridad deben ser definidas y utilizan para proteger áreas que contienen información y procesamiento de la información, ya sea instalaciones sensibles o críticos.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
11.1.2	Controles de entrada físicas	Aplica	Descripción: Áreas seguras deben ser protegidos por los controles de entrada adecuados para garantizar que se permite el acceso sólo el personal autorizado.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
11.1.3	Asegurar oficinas, habitaciones e instalaciones	Aplica	Descripción: La seguridad física para oficinas, salas	Justificación: la organización necesita aplicar el

			e instalaciones deben ser diseñadas y aplicadas.	control para poder acceder posteriormente a la certificación.
11.1.4	La protección contra amenazas externas y ambientales	Aplica	Descripción: La protección física contra los desastres naturales, ataques maliciosos o accidentes debe ser diseñada y aplicada.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
11.1.5	Trabajar en zonas seguras	Aplica	Descripción: Procedimientos para trabajar en zonas seguras deberían diseñarse y aplicarse.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
11.1.6	Zonas de entrega y carga	Aplica	Descripción: Los puntos de acceso como las zonas de entrega y de carga y otros puntos en los que personas no autorizadas puedan entrar en los locales deberán ser controlados y, si es posible, aislada de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
11.2 Equipo		Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.		
11.2.1	Ubicación y protección del equipo	Aplica	Descripción: El equipo debe estar ubicado y protegido para reducir los riesgos de las amenazas ambientales y los riesgos y las oportunidades de acceso no autorizado.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
11.2.2	Apoyo a los servicios públicos	Aplica	Descripción: El equipo debe ser protegido de fallas de energía y otros trastornos causados por fallas	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la

			en el apoyo a los servicios públicos.	certificación.
11.2.3	seguridad cableado	Aplica	Descripción: Energía y telecomunicaciones cableado que transporta datos o apoyar los servicios de información debe ser protegida de intercepción, interferencia o daño.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
11.2.4	Mantenimiento del equipo	Aplica	Descripción: El equipo debe mantenerse correctamente para asegurar su disponibilidad e integridad continua.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
11.2.5	Eliminación de los activos	Aplica	Descripción: Equipos, información o software no deben tomarse fuera de las instalaciones sin autorización previa.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
11.2.6	Seguridad de equipo y activos fuera de las instalaciones	Aplica	Descripción: Seguridad debe ser aplicado a los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
11.2.7	Eliminación segura o la reutilización de los equipos	Aplica	Descripción: Todos los artículos de equipos que contengan soportes de almacenamiento deben ser verificados para asegurar que los datos sensibles y software con licencia ha sido eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
11.2.8	Equipos de	Aplica	Descripción: Los	Justificación: la

	usuario desatendidos		usuarios deben asegurarse de que el equipo desatendido tiene la protección adecuada.	organización necesita aplicar el control para poder acceder posteriormente a la certificación.
11.2.9	Escritorio limpio y política pantalla limpia	Aplica	Descripción: Una política de escritorio limpio de papeles y soportes de almacenamiento extraíbles y una política clara pantalla para las instalaciones de procesamiento de la información debe ser adoptada.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
12. Operaciones de seguridad				
12.1 Procedimientos y responsabilidades operacionales		Objetivo: Asegurar operaciones correctas y seguras de instalaciones de procesamiento de información.		
12.1.1	Procedimientos operativos documentados	Aplica	Descripción: Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que los necesitan.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
12.1.2	Gestión del cambio	Aplica	Descripción: Cambios en la organización, procesos de negocio, instalaciones de procesamiento de información y sistemas que afectan a la seguridad de información deben ser controlados.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
12.1.3	gestión de la capacidad	Aplica	Descripción: El uso de los recursos debe ser monitoreado, se ajusta y proyecciones de las futuras necesidades de capacidad para garantizar el rendimiento del sistema requerido.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
12.1.4	Separación de	Aplica	Descripción:	Justificación: la

	desarrollo, pruebas y entornos operativos		Desarrollo, pruebas y entornos operativos deben ser separados para reducir los riesgos de acceso o cambios no autorizados al entorno operativo.	organización necesita aplicar el control para poder acceder posteriormente a la certificación.
12.2 Protección contra el malware		Objetivo: Asegurar que las instalaciones de procesamiento de información y la información están protegidos contra el malware.		
12.2.1	Controles contra el malware	Aplica	Descripción: Detección, prevención y recuperación de controles para proteger contra el malware debe ser implementado, en combinación con el conocimiento del usuario apropiado.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
12.3 Copias de seguridad		Objetivo: Evitar la pérdida de datos.		
12.3.1	Copia de seguridad de la información	Aplica	Descripción: Las copias de seguridad de la información, software y sistemas de imágenes deben ser tomadas y analizadas regularmente de acuerdo con una política de copia de seguridad convenido.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
12.4 Registro y seguimiento		Objetivo: Registrar eventos y generar evidencia.		
12.4.1	registro de eventos	Aplica	Descripción: Los registros de eventos registran las actividades del usuario, excepciones, errores y eventos de seguridad de la información se deben producir, mantenidos y revisados con regularidad.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
12.4.2	Protección de la información de registro	Aplica	Descripción: Registro de instalaciones y registrar la información debe	Justificación: la organización necesita aplicar el control para poder acceder

			ser protegida contra la manipulación y acceso no autorizado.	posteriormente a la certificación.
12.4.3	Registros de administrador y operador	Aplica	Descripción: Administrador del sistema y las actividades del operador del sistema deben ser registrados y sus troncos protegidos y regularmente revisados.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
12.4.4	sincronización de reloj	Aplica	Descripción: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o dominio de seguridad deben estar sincronizados a una sola fuente de tiempo de referencia.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
12.5 El control de software operativo		Objetivo: Garantizar la integridad de los sistemas operativos.		
12.5.1	La instalación del software en los sistemas operativos	Aplica	Descripción: Deberían aplicarse procedimientos para controlar la instalación del software en los sistemas operativos.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
12.6 Técnico de gestión de vulnerabilidades		Objetivo: Prevenir la explotación de vulnerabilidades técnicas.		
12.6.1	Gestión de vulnerabilidades técnicas	Aplica	Descripción: Información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilicen deben ser obtenidos de manera oportuna, la exposición de la organización a tales vulnerabilidades evaluado y tomado las medidas	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.

			adecuadas para hacer frente a los riesgos asociados.	
12.6.2	Las restricciones a la instalación de software	Aplica	Descripción: Las normas que rigen la instalación de software los usuarios deben establecerse e implementarse.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
12.7 Sistemas de información consideraciones de auditoría		Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.		
12.7.1	Sistemas de información controles de auditoría	Aplica	Descripción: Requisitos y actividades de verificación de los sistemas operativos de auditoría deben ser cuidadosamente planificadas y acordadas para reducir al mínimo las interrupciones de los procesos de negocio.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
13. Seguridad de las comunicaciones				
13.1 Gestión de la seguridad de red		Objetivo: Garantizar la protección de la información en las redes y sus instalaciones de apoyo de procesamiento de información.		
13.1.1	Controles de red	Aplica	Descripción: Las redes deben ser gestionados y controlados para proteger la información en los sistemas y aplicaciones.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
13.1.2	Seguridad de los servicios de red	Aplica	Descripción: Los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de la red deben ser identificados e incluidos en los acuerdos de servicios de red, si estos servicios son prestados en la empresa o subcontratados.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.

13.1.3	Segregación en redes	Aplica	Descripción: Grupos de servicios de información, los usuarios y los sistemas de información deben ser segregados en las redes.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
13.2 transferencia de información		Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
13.2.1	Las políticas y los procedimientos de transferencia de información	Aplica	Descripción: Formales de transferencia de políticas, procedimientos y controles deben estar en su lugar para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
13.2.2	acuerdos sobre la transferencia de información	Aplica	Descripción: Los acuerdos deben abordar la transferencia segura de información comercial entre la organización y las partes externas.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
13.2.3	mensajería electrónica	Aplica	Descripción: Información involucrado en la mensajería electrónica debe ser protegido de manera apropiada.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
13.2.4	acuerdos de confidencialidad o de no divulgación	Aplica	Descripción: Requisitos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, revisados y documentados con regularidad.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.

14. Sistema de adquisición, desarrollo y mantenimiento				
14.1 Security requirements of information systems		Objetivo: Asegurarse de que la seguridad informática es una parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.		
14.1.1	Información de análisis de requisitos de seguridad y la especificación	Aplica	Descripción: Los requisitos relacionados con la seguridad de la información deben ser incluidos en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
14.1.2	Asegurar los servicios de aplicaciones en las redes públicas	Aplica	Descripción: Información involucrados en los servicios de aplicaciones que pasan a través de redes públicas debe protegerse de la actividad fraudulenta, disputa contractual y la divulgación no autorizada y modificación.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
14.1.3	protección de las transacciones de servicios de aplicaciones	Aplica	Descripción: Información involucrado en las transacciones de servicios de aplicación debe ser protegido para prevenir la transmisión incompleta, errónea enrutamiento, alteración mensaje no autorizado, revelación no autorizada, la duplicación de mensajes no autorizado o la repetición.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.:
14.2 Seguridad en los procesos de desarrollo y		Objetivo: Garantizar la seguridad de la		

de apoyo			información que se diseña e implementa dentro del ciclo de vida de desarrollo de sistemas de información.	
14.2.1	política de desarrollo seguro	Aplica	Descripción: Reglas para el desarrollo de software y sistemas deben establecerse y aplicarse a la evolución de la organización.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
14.2.2	Procedimientos de control de cambio de sistema	Aplica	Descripción: Los cambios en los sistemas dentro del ciclo de vida de desarrollo deben ser controlados por el uso de procedimientos formales de control de cambio.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
14.2.3	Revisión técnica de aplicaciones después de la plataforma operativa	Aplica	Descripción: Cuando se cambian las plataformas que operan, aplicaciones críticas de negocio deben ser revisados y probados para asegurar que no hay impacto adverso en las operaciones de la organización o de seguridad.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
14.2.4	restricciones a los cambios en los paquetes de software	Aplica	Descripción: Las modificaciones a los paquetes de software deben ser desalentados, otros, las modificaciones necesarias y todos los cambios deben ser estrictamente controlados.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
14.2.5	Principios de ingeniería de sistemas seguros	Aplica	Descripción: Principios para sistemas seguros de ingeniería deben establecerse, documentarse, mantenerse y aplicarse a cualquier esfuerzos	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.

			de implementación de sistemas de información.	
14.2.6	Entorno de desarrollo seguro	Aplica	Descripción: Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguras para los esfuerzos de desarrollo e integración de sistemas que cubren todo el ciclo de vida de desarrollo del sistema.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
14.2.7	desarrollo outsourced	Aplica	Descripción: La organización debe supervisar y controlar la actividad de desarrollo del sistema tercerizado.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
14.2.8	Pruebas de seguridad Sistema	Aplica	Descripción: Pruebas de la funcionalidad de seguridad debe llevarse a cabo durante el desarrollo.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
14.2.9	Pruebas de aceptación del sistema	Aplica	Descripción: Programas de pruebas de aceptación y criterios relacionados deben establecerse para los nuevos sistemas de información, actualizaciones y nuevas versiones.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
14.3 datos de prueba			Objetivo: Garantizar la protección de los datos utilizados para las pruebas.	
14.3.1	Protección de los datos de prueba	Aplica	Descripción: Los datos de prueba deben seleccionarse cuidadosamente, protegidos y controlados.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.:
15. relaciones con los proveedores				
15.1 Seguridad de la información en las			Objetivo: Garantizar la protección de los activos	

relaciones con proveedores			de la organización que sea accesible por los proveedores.	
15.1.1	política de seguridad de la información para relaciones con los proveedores	Aplica	Descripción: Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben arreglarse con el proveedor y documentados.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	Aplica	Descripción: Todos los requisitos de seguridad de la información pertinentes deben ser establecidos y acordados con cada proveedor que pueden acceder, procesar, almacenar, comunicar, o proporcionar TI componentes de la infraestructura de información de la organización.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
15.1.3	Cadena de información y tecnología de comunicación de suministro	Aplica	Descripción: Los acuerdos con los proveedores deberían incluir requisitos para hacer frente a los riesgos de seguridad de información asociados a los servicios de información y tecnología de las comunicaciones y de la cadena de suministro de productos.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
15.2 Gestión de la prestación de servicios de proveedores			Objetivo: Mantener un nivel acordado de seguridad de la información y la prestación de servicios en línea con los acuerdos con proveedores.	
15.2.1	seguimiento y la revisión de los	Aplica	Descripción: Las organizaciones	Justificación: la organización

	servicios de proveedores		deben controlar regularmente, revisión y auditoría de proveedores la prestación de servicios.	necesita aplicar el control para poder acceder posteriormente a la certificación.
15.2.2	Gestión de cambios en los servicios de proveedores	Aplica	Descripción: Los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, se deben manejar, teniendo en cuenta la criticidad de la información empresarial, los sistemas y los procesos involucrados y re-evaluación de los riesgos.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
16. Información de gestión de incidentes de seguridad				
16.1 Gestión de incidentes de seguridad de la información y mejoras		Objetivo: Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluidos los de comunicación en los eventos de seguridad y debilidades.		
16.1.1	Responsabilidades y procedimientos	Aplica	Descripción: Responsabilidades y procedimientos de gestión deben ser establecidos para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
16.1.2	Presentación de informes de eventos de seguridad de información	Aplica	Descripción: Los eventos de seguridad de la información deben ser reportados a través de canales de gestión adecuadas tan	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.

			pronto como sea posible.	
16.1.3	Informes debilidades de seguridad de información	Aplica	Descripción: Los empleados y contratistas que utilizan los sistemas y servicios de información de la organización deberían estar obligados a observar y reportar cualquier debilidad de seguridad de información observados o sospechados en los sistemas o servicios.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Aplica	Descripción: Los eventos de seguridad de la información deben ser evaluados y que se deben decidir si han de ser clasificados como incidentes de seguridad de la información.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
16.1.5	Respuesta a incidentes de seguridad de la información	Aplica	Descripción: Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
16.1.6	Aprendiendo de los incidentes de seguridad de la información	Aplica	Descripción: Los conocimientos adquiridos desde el análisis y la resolución de los incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de futuros incidentes.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
16.1.7	acopio de pruebas		Descripción: La organización debe definir y aplicar procedimientos	Justificación: la organización necesita aplicar el control para poder

			para la identificación, recolección, adquisición y conservación de la información, que puede servir como prueba.	acceder posteriormente a la certificación.
17. Los aspectos de seguridad de información de la gestión de la continuidad del negocio				
17.1 Información continuidad seguridad		Objetivo: Información continuidad de seguridad debe estar integrada en los sistemas de gestión de continuidad de negocio de la organización.		
17.1.1	Planificación información continuidad seguridad	Aplica	Descripción: La organización debe determinar sus necesidades de seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
17.1.2	implementación de la información continuidad seguridad	Aplica	Descripción: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles que garanticen el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
17.1.3	Verificar, revisar y evaluar la información de seguridad de continuidad	Aplica	Descripción: La organización debe verificar la información controles de continuidad de seguridad establecido y aplicado a intervalos regulares con el fin de asegurarse de que	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.

			son válidos y eficaces en situaciones adversas.	
17.2 despidos			Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.	
17.2.1	Disponibilidad de instalaciones de procesamiento de información	Aplica	Descripción: Instalaciones de procesamiento de la información deben ser implementados con redundancia suficiente para satisfacer los requisitos de disponibilidad.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
18. conformidad				
18.1 cumplimiento de los requisitos legales y contractuales			Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales en materia de seguridad de la información y de las exigencias de seguridad.	
18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	Aplica	Descripción: Todo legal legislativo pertinente, los requisitos reglamentarios, contractuales y el enfoque de la organización para cumplir con estos requisitos deben ser identificados de manera explícita, documentados y actualizados a la fecha de cada sistema de información y la organización.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
18.1.2	derechos de propiedad Intectual	Aplica	Descripción: Procedimientos apropiados deben ser implementadas para garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.

			de productos de software privativo.	
18.1.3	Protección de los registros	Aplica	Descripción: Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y la liberación no autorizada, de conformidad con los requisitos legislatory, reglamentarios, contractuales y comerciales.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
18.1.4	Privacidad y protección de datos personales	Aplica	Descripción: Privacidad y protección de la información de identificación personal que se debe garantizar a lo dispuesto en la legislación y la regulación en su caso pertinente.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
18.1.5	Reglamento de los controles criptográficos	Aplica	Descripción: Controles criptográficos deben ser utilizados en el cumplimiento de todos los acuerdos pertinentes, la legislación y los reglamentos.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
18.2 Revisiones de seguridad de información		Objetivo: Garantizar la seguridad de la información que se implementa y opera de acuerdo con las políticas y procedimientos de la organización.		
18.2.1	Revisión independiente de seguridad de la información	Aplica	Descripción: El enfoque de la organización para la gestión de seguridad de la información y su aplicación (es decir, los objetivos de control, controles, políticas, procesos y procedimientos de seguridad de la información) debe	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.

			ser revisado de forma independiente a intervalos planificados o cuando se producen cambios significativos.	
18.2.2	El cumplimiento de las políticas y estándares de seguridad	Aplica	Descripción: Los gerentes deben comprobar periódicamente el cumplimiento de los procedimientos de procesamiento y la información dentro de su área de responsabilidad con las políticas de seguridad, las normas y otros requisitos de seguridad.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.
18.2.3	Revisión de cumplimiento técnico	Aplica	Descripción: Los sistemas de información deben ser revisados regularmente por el cumplimiento de las políticas y normas de seguridad de la información de la organización.	Justificación: la organización necesita aplicar el control para poder acceder posteriormente a la certificación.

3. ANÁLISIS DE RIESGOS

3.1 Introducción

Es muy importante para las organizaciones tener un conocimiento claro de sus activos, las dependencias existentes entre ellos con su respectiva valoración todo con el fin de protegerlos de una forma más efectiva. Con el fin de cumplir lo anterior en este punto de análisis de riesgo de realizará:

- Inventario de activos
- Valoración de los activos
- Dimensiones de seguridad
- Resumen de valoración

- Análisis de amenazas
- Impacto Potencial
- Nivel de riesgo aceptable y riesgo residual
- Resultados

3.2 Inventario de activos

Se agruparán los activos por grupos en una tabla que como estructura tiene el grupo al que pertenece el activo y el activo en sí.

Tabla 24. Inventario de activos.

Ámbito	Activo	Cantidad
Capital Humano	Director ejecutivo Coordinación Administrativa Coordinación Proyectos Coordinación Comercial Coordinación de Emprendimiento Coordinadora Calidad Revisor Fiscal Contador Auxiliares (buenas prácticas, emprendimiento, otros)	1 1 1 1 1 1 1 1 5
Técnico	Planta eléctrica Rack de Comunicaciones Armarios de documentos	1 1 2
Hardware	Portátil dirección Portátiles equipo de trabajo Equipos de escritorio Servidor proxy Impresoras laser monocromática Switch de 24 puertos Router inalámbrico	1 9 3 1 2 2 1
Licencias	Todos los equipos de cómputo vienen equipados con el mismo software, cuentan con sistema operativo Windows de fábrica, Microsoft Office 2010, en algunos cuentan con licencias libres de algunos programas.	
Información	La empresa cuenta con información que no ha valorado como activos, los contratos de toda índole están en armarios donde se almacenan, no se tiene un lugar de almacenamiento de bases de datos que son realizadas o adquiridas de terceros, los documentos como lineamientos, políticas y manuales de función son almacenados en su gran mayoría de forma digital, pero no se cuenta con un repositorio que	

	permita hacer control de versiones o garantizar su seguridad. De la información no se realizan copias de seguridad, puede suceder que en algún momento si un equipo se daña y es de alguna de las coordinaciones no puedan recuperar esta información.	

3.3 Valoración de los activos

Se realizará una valoración cuantitativa de los activos, la clasificación se hará según las siguientes categorías:

- Muy alto
- Alto
- Medio
- Bajo
- Muy bajo

Tabla 25. Valoración de los activos

Activo	Cantidad	Valor
Director ejecutivo	1	Muy alto
Coordinación Administrativa	1	Muy alto
Coordinación Proyectos	1	Muy alto
Coordinación Comercial	1	Muy alto
Coordinación de Emprendimiento Coordinadora	1	Muy alto
Calidad	1	Muy alto
Revisor Fiscal	1	Muy alto
Contador	1	Muy alto
Auxiliares (buenas prácticas, emprendimiento, otros)	5	Alto
Planta eléctrica	1	Alto
Rack de Comunicaciones	1	Alto
Armarios de documentos	2	Medio
Portátil dirección	1	Medio
Portátiles equipo de trabajo	9	Alto
Equipos de escritorio	3	Medio
Servidor proxy	1	Alto
Impresoras laser monocromática	2	Bajo
Switch de 24 puertos	2	Medio
Router inalámbrico	1	Medio
Todos los equipos de cómputo vienen equipados con el mismo software, cuentan con sistema operativo Windows de fábrica, Microsoft Office 2010, en algunos cuentan con licencias libres de		Medio

algunos programas.		
La empresa cuenta con información que no ha valorado como activos, los contratos de toda índole están en armarios donde se almacenan, no se tiene un lugar de almacenamiento de bases de datos que son realizadas o adquiridas de terceros, los documentos como lineamientos, políticas y manuales de función son almacenados en su gran mayoría de forma digital, pero no se cuenta con un repositorio que permita hacer control de versiones o garantizar su seguridad. De la información no se realizan copias de seguridad, puede suceder que en algún momento si un equipo se daña y es de alguna de las coordinaciones no puedan recuperar esta información.		Muy alto

3.4 Dimensiones de seguridad

Desde el punto de vista de la seguridad, junto a la valoración en sí de los activos debe indicarse cuál es el aspecto de la seguridad más crítico. Esto será de ayuda en el momento de pensar en posibles salvaguardas, ya que estas se enfocarán en los aspectos que más nos interesen.

Las dimensiones de seguridad utilizadas para identificación del impacto son:

Tabla 26. Dimensiones de seguridad utilizadas.

A	Autenticidad
C	Confidencialidad
I	Integridad
D	Disponibilidad
T	Trazabilidad

Una vez explicadas las cinco dimensiones se ha de tener presente la escala en la que se realizarán las valoraciones. En este caso utilizaremos una escala de valoración de diez valores siguiendo los siguientes criterios:

Tabla 27. Valoración dimensiones de seguridad.

VALOR	CRITERIO
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

3.5 Resumen de valoración

Las columnas A,C,I,D y T representan la importancia del activo en relación a las dimensión de Seguridad.

Ámbito	Activo	Valor	Aspectos Críticos				
			A	C	I	D	T
Capital Humano	Director ejecutivo	Muy alto	4	7	4	4	4
	Coordinación Administrativa	Muy alto	4	7	4	5	4
	Coordinación Proyectos	Muy alto	4	7	6	5	4
	Coordinación Comercial	Muy alto	4	7	4	4	4
	Coordinación de Emprendimiento	Muy alto	4	7	4	4	4
	Coordinadora Calidad	Muy alto	4	7	4	4	4
	Revisor Fiscal	Muy alto	4	7	4	5	4
	Contador	Muy alto	4	7	4	5	4
	Auxiliares (buenas prácticas, emprendimiento, otros)	Alto	4	7	4	4	4
Técnico	Planta eléctrica	Alto	3	3	6	7	5
	Rack de Comunicaciones	Alto	3	3	6	7	5
	Armarios de documentos	Medio	3	7	5	7	5
Hardware	Portátil dirección	Medio	4	4	4	4	4
	Portátiles equipo de trabajo	Alto	4	5	4	4	4
	Equipos de escritorio	Medio	4	4	4	4	4
	Servidor proxy	Alto	4	4	5	6	4
	Impresoras laser	Bajo	3	3	3	3	3
	Switch de 24 puertos	Medio	3	3	3	5	3
	Router inalámbrico	Medio	3	3	3	5	3
Licencias	Todos los equipos de cómputo vienen equipados con el mismo software, cuentan con sistema operativo Windows de fábrica, Microsoft Office 2010, en algunos cuentan con licencias libres de algunos programas.	Medio	6	6	6	6	6
Información	La empresa cuenta con información que no ha valorado como activos, los	Muy Alto	8	8	8	8	8

	contratos de toda índole están en armarios donde se almacenan, no se tiene un lugar de almacenamiento de bases de datos que son realizadas o adquiridas de terceros, los documentos como lineamientos, políticas y manuales de función son almacenados en su gran mayoría de forma digital, pero no se cuenta con un repositorio que permita hacer control de versiones o garantizar su seguridad. De la información no se realizan copias de seguridad, puede suceder que en algún momento si un equipo se daña y es de alguna de las coordinaciones no puedan recuperar esta información.						

3.6 Análisis de amenazas

Los activos están expuestos a amenazas y estas pueden afectar a los distintos aspectos de la seguridad. Se analizan qué amenazas pueden afectar a qué activos. Una vez estudiado, estimar cuán vulnerable es el activo a la materialización de la amenaza así como la frecuencia estimada de la misma.

Usamos la metodología MAGERIT (en concreto Libro 2 “Catálogo de Elementos” (Punto 5)). Las amenazas están clasificadas en los siguientes grandes bloques:

- Desastres naturales
- De origen industrial
- Errores y fallos no intencionados
- Ataques intencionados

La información recopilada da lugar a una tabla resumen para un activo determinado. En definitiva, para cada tipo de activo se analizará la frecuencia con que puede producirse la amenaza, así como su impacto en las distintas dimensiones de la seguridad del activo.

La frecuencia o probabilidad de ocurrencia de los eventos se encuentra definida así:

Tabla 28. Frecuencia de ocurrencia de eventos.

Descripción	Abreviatura	Valor
Extremadamente frecuente	EF	1 (Una vez al día)
Muy frecuente	MF	0.071233 (Quincenal)
Frecuente	F	0,016438 (Bimestral)
Poco frecuente	PF	0,005479 (Semestral)
Muy poco frecuente	MPF	0,002739 (Anual)
Despreciable	D	0

Los tipos de activos se presentarán con abreviatura para realizar un análisis más completo, las abreviaturas son las siguientes:

Tabla 29. Abreviaturas tipos de activos

Capital Humano	CH
Técnico	T
Hardware	H
Licencias	L
Información	I

A continuación se presentan los cuatro grandes bloques con sus amenazas, indicando en qué tipo de activo afecta para el posterior análisis de la frecuencia.

Tabla 30. Bloques de amenazas y activos.

Grupo	Ref	Amenaza	Activos afectados				
			CH	T	H	L	I
Desastres naturales	DN1	Fuego		x	x		
	DN2	Daños por agua		x	x		
	DN3	Otros desastres naturales		x	x		
De origen industrial	OI1	Fuego		x	x		
	OI2	Daños por agua		x	x		
	OI3	Contaminación mecánica		x	x		
	OI4	Contaminación electromagnética		x	x	x	x
	OI5	Avería de origen físico o lógico		x	x		
	OI6	Corte del suministro eléctrico			x		x
	OI7	Condiciones inadecuadas de temperatura o humedad		x	x		
	OI8	Fallo de servicio de comunicaciones		x	x		
	OI9	Interrupción de otros servicios y suministros esenciales		x	x	x	
	OI10	Degradación de los soportes de almacenamiento de la información					x
	OI11	Emanaciones electromagnéticas		x	x	x	
Errores y fallos	EF1	Errores de los usuarios			x		x

no intencionados	EF2	Errores del administrador			x		x
	EF3	Errores de monitorización (log)					
	EF4	Errores de configuración					
	EF5	Deficiencias en la organización	x				
	EF6	Difusión de software dañino			x		x
	EF7	Errores de [re-]encaminamiento					x
	EF8	Errores de secuencia					x
	EF9	Escapes de información	x				x
	EF10	Alteración accidental de la información					x
	EF11	Destrucción de información					x
	EF12	Fugas de información	x				x
	EF13	Vulnerabilidades de los programas (software			x	x	x
	EF14	Errores de mantenimiento / actualización de programas (software)			x	x	x
	EF15	Errores de mantenimiento / actualización de equipos (hardware)		x	x		x
	EF16	Caída del sistema por agotamiento de recursos		x	x		
	EF17	Pérdida de equipos		x	x		
	EF18	Indisponibilidad del personal	x				x
Ataques intencionados	AI1	Manipulación de los registros de actividad (log)					x
	AI2	Manipulación de la configuración					
	AI3	Suplantación de la identidad del usuario					x
	AI4	Abuso de privilegios de acceso					x
	AI5	Uso no previsto			x		x
	AI6	Difusión de software dañino			x		
	AI7	[Re-]encaminamiento de mensajes			x		
	AI8 AI9	Alteración de secuencia Acceso no autorizado					X x
	AI10	Análisis de tráfico					x
	AI11	Repudio					x
	AI12	Interceptación de información (escucha)					x
	AI13	Modificación deliberada de la información					x
	AI14	Destrucción de información					x
	AI15	Divulgación de información					x
	AI16	Manipulación de programas				x	x
	AI17	Manipulación de los equipos			x		
	AI18	Denegación de servicio			x		x
	AI19	Robo		x	x	x	x
	AI20	Ataque destructivo		x	x		
	AI21	Ocupación enemiga		x	x		
	AI22	Indisponibilidad del personal	x				
	AI23	Extorsión	x				
	AI24	Ingeniería social	x				

Tabla 31. Activos, amenazas y frecuencias.

Tipo Activo	Amenaza	Frecuencia	A	C	I	D	T
Capital humano	EF5	PF				50%	
	EF9	PF		90%			
	EF12	PF		90%			
	EF18	PF				50%	50%
	AI22	PF				50%	50%
	AI23	MPF			80%		
	AI24	MPF		90%			
Técnico	DN1	MPF			80%	80%	
	DN2	MPF			80%	80%	
	DN3	MPF			80%	80%	
	OI1	PF				80%	
	OI2	PF				80%	
	OI3	PF				80%	
	OI4	PF				80%	
	OI5	PF				80%	
	OI7	PF				80%	
	OI8	PF				80%	
	OI9	PF				80%	
	OI11	PF				80%	
	EF15	PF			60%	60%	
	EF16	PF			60%	60%	
	EF17	PF			60%	60%	
	AI19	PF		90%			
	AI20	MPF			80%	80%	
	AI21	MPF			80%	80%	
Hardware	DN1	MPF			80%	80%	
	DN2	MPF			80%	80%	
	DN3	MPF			80%	80%	
	OI1	PF				80%	
	OI2	PF				80%	
	OI3	PF				80%	
	OI4	PF				80%	
	OI5	PF				80%	
	OI6	PF				80%	
	OI7	PF				80%	
	OI8	PF				80%	
	OI9	PF				80%	
	OI11	PF			60%	60%	
	EF1	PF			60%	60%	
	EF2	PF			60%	60%	
	EF6	PF					
	EF13	MPF				80%	
	EF14	PF				80%	
	EF15	PF				80%	
	EF16	PF				80%	

	EF17	PF				80%	
	AI5	PF				80%	
	AI6	PF				80%	
	AI7	PF				80%	
	AI17	PF				80%	
	AI18	PF				80%	
	AI19	PF		90%			
	AI20	PF			80%	80%	
	AI21	MPF			80%	80%	
Licencias	OI4	PF				70%	
	OI9	PF				70%	
	OI11	PF				70%	
	EF13	PF				70%	
	EF14	PF				70%	
	AI16	PF				70%	
	AI19	PF				70%	
Información	OI4	PF		90%			
	OI6	PF		90%			
	OI10	PF		90%			
	EF1	PF		90%			
	EF2	PF		90%			
	EF6	PF		90%			
	EF7	PF		90%			
	EF8	PF		90%			
	EF9	PF		90%			
	EF10	PF		90%			
	EF11	PF		90%			
	EF12	PF		90%			
	EF13	PF		90%			
	EF14	PF		90%			
	EF15	PF		90%			
	EF18	PF		90%			
	AI1	PF		90%			
	AI3	PF		90%			
	AI4	PF		90%			
	AI5	PF		90%			
	AI3	PF		90%			
	AI8 AI9	PF PF		90% 90%			
	AI10	PF		90%			
	AI11	PF		90%			
	AI12	PF		90%			
	AI13	PF		90%			
	AI14	PF		90%			
	AI15	PF		90%			
	AI16	PF		90%			
	AI18	PF		90%			
	AI19	PF		90%			

3.7 Nivel de riesgo aceptable

El nivel aceptable del riesgo se ha establecido manualmente y analizando concienzudamente cada activo. Se establecen tres niveles de riesgo (Bajo=75%, Medio=50%, Alto=25%) que se aplicarán sobre el riesgo intrínseco anual del activo, a partir de este resultado se establecerán las medidas necesarias para gestionar el riesgo.

Tabla 32. Niveles de riesgo aceptables activos.

Ámbito	Activo	Nivel de riesgo aceptable
Capital Humano	Director ejecutivo Coordinación Administrativa Coordinación Proyectos Coordinación Comercial Coordinación de Emprendimiento Coordinadora Calidad Revisor Fiscal Contador Auxiliares (buenas prácticas, emprendimiento, otros)	Medio Medio Medio Medio Medio Medio Medio Medio Medio
Técnico	Planta eléctrica Rack de Comunicaciones Armarios de documentos	Medio Medio Alto
Hardware	Portátil dirección Portátiles equipo de trabajo Equipos de escritorio Servidor proxy Impresoras laser monocromática Switch de 24 puertos Router inalámbrico	Medio Medio Alto Medio Alto Medio Medio
Licencias	Todos los equipos de cómputo vienen equipados con el mismo software, cuentan con sistema operativo Windows de fábrica, Microsoft Office 2010, en algunos cuentan con licencias libres de algunos programas.	Medio
Información	La empresa cuenta con información que no ha valorado como activos, los contratos de toda índole están en armarios donde se almacenan, no se tiene un lugar de almacenamiento de bases de datos que son realizadas o adquiridas de terceros, los documentos como lineamientos, políticas y manuales de función son	Bajo

	almacenados en su gran mayoría de forma digital, pero no se cuenta con un repositorio que permita hacer control de versiones o garantizar su seguridad. De la información no se realizan copias de seguridad, puede suceder que en algún momento si un equipo se daña y es de alguna de las coordinaciones no puedan recuperar esta información.	

3.8 Conclusiones

La aplicación de la metodología del análisis de riesgos en nuestra organización nos proporciona importantes conclusiones que serán el punto de partida para el establecimiento de los proyectos de seguridad de la empresa.

El trabajo para reducir las amenazas y riesgos de seguridad deberán orientarse a proyectos que fortalezcan todas las áreas afectadas en la organización.

4. PROPUESTA DE PROYECTOS

4.1 Introducción

En esta fase se pretende proponer soluciones para mejorar el estado de la organización. Para ello, en este capítulo se realizará la propuesta de un programa de proyectos y se definirán cuales son las expectativas de mejora previstas si se llevan a cabo.

4.2 Propuestas

En todos los proyectos presentados se tendrán en cuenta los siguientes ítems:

- Nombre del proyecto
- Objetivos
- Requisitos

- Esfuerzo (duración, coste, dificultad)
- Implicaciones en la organización
- Impacto económico y estratégico en la empresa

4.2.1 Proyecto 1

Nombre del proyecto: Organización de la seguridad y su política de aplicación.

Objetivos: Desarrollar la organización de la seguridad y su política de aplicación. Establecer la base del SGSI basado en ISO/IEC 27001. Implicar a la Dirección y obtener su soporte.

Requisitos:

- Elaboración, aceptación y comunicación de la política seguridad.
- Definición de organigrama y responsabilidades de seguridad.
- Definición de procesos y elaboración de metodologías básicas de seguridad.
- Establecimiento de medidas para el aseguramiento de la seguridad de terceras partes.

Esfuerzo:

- Duración: 1 mes y 15 días.
- Coste: USD 4.000 consultoría externa especializada.
- Dificultad: Es baja, se debe comprometer la dirección para que así sea.

Implicaciones en la organización: Necesidad del establecimiento de la organización y política de seguridad.

Impacto Económico: Indirecto. Reducirá los riesgos de seguridad e impactos de las amenazas. Reducción de 5% en el impacto de amenazas que significa ahorro en dinero.

Impacto Estratégico: Concienciación de la empresa en la seguridad. Mejora y optimización de los procesos de seguridad.

4.2.2 Proyecto 2

Nombre del proyecto: Formación y concienciación de seguridad.

Objetivos: Establecer e implantar un plan de formación, capacitación y concienciación destinado a todos los empleados de la organización y a terceros (colaboradores, proveedores, etc.)

Requisitos:

- Plan trianual
- Incluirá las áreas de formación, capacitación y concienciación.
- Destinado a empleados y terceros (clientes, proveedores, etc)

Esfuerzo:

- Duración: 1 mes.
- Coste: USD15.000 destinado a formación /año.
- Dificultad: Baja. La máxima dificultad se concentra en la implicación de los trabajadores.

Implicaciones en la organización: Necesidad de desarrollo e implementación de planes de formación (actualmente no existen).

Impacto económico: Incremento de la productividad de los empleados.

Impacto estratégico: Incremento en la calidad y seguridad de los servicios ofrecidos.

4.2.3 Proyecto 3

Nombre del proyecto: Mejora de la gestión de incidencias y problemas.

Objetivos: Optimizar la gestión de incidencias y problemas. Definir y formalizar los procesos. Identificar indicadores de productividad. Incorporar mejoras o nuevas herramientas.

Requisitos:

- Optimización del proceso de gestión de incidencias y problemas.
- Definición del proceso y flujo de actividades.
- Adaptación de la herramienta de ticketing.
- Formación y training.
- Establecimiento del proceso de mejora continua.

Esfuerzo:

- Duración: 3 meses y 15 días.
- Coste: USD 5.000 consultoría externa.
- Dificultad: Media. Requiere la implicación y formación de los usuarios finales.

Implicaciones en la organización: Mejorar la eficacia y eficiencia de la gestión de incidencias / problemas.

Impacto económico: Reducción de incidencias. Mejora de productividad. Incremento productividad.

Impacto estratégico: Aumento de la satisfacción de los clientes.

4.2.4 Proyecto 4

Nombre del proyecto: Continuidad y recuperación del negocio.

Objetivos: Establecer un plan de continuidad y recuperación del negocio ante desastres.

Requisitos:

- Análisis de riesgos (amenazas)
- Plan de continuidad y recuperación

- Pruebas y simulación.
- Proceso de mejora continua.

Esfuerzo:

- Duración: 5 Meses
- Coste: USD 20.000 consultoría externa
- Dificultad: Alta. Requiere una importante implicación de la dirección y mandos intermedios.

Implicaciones en la organización: Proteger la continuidad de la empresa en el mercado en caso de desastre.
Impacto económico: Refuerzo del valor de la marca ante desastres. Reducción de las pérdidas económicas en caso de problemas. Reducción 35% pérdidas económicas en caso de desastre.
Impacto estratégico: Resistencia del negocio ante desastres. No desaparición de la empresa.

4.2.5 Proyecto 5

Nombre del proyecto: Aseguramiento de infraestructuras críticas.
Objetivos: Asegurar la continuidad de las infraestructuras críticas ante desastres naturales o incidentes.
Requisitos:

- Segmentación y redundancia de sistemas críticos.
- Actualización y modernización de sistemas.
- Simulación de amenazas y traning al equipo.

Esfuerzo:

- Duración: 8 meses.
- Coste: USD 80.000 Infraestructura.
- Dificultad: Media. Requiere modificaciones en la infraestructura y migración de sistemas.

Implicaciones en la organización: Resistencia ante incidentes de seguridad.
Impacto económico: Reducción de daños económicos en caso de incidente. Reducción de -20% daños ante desastre.
Impacto estratégico: Continuidad del negocio frente a desastres e incidentes.

4.3 Resultados

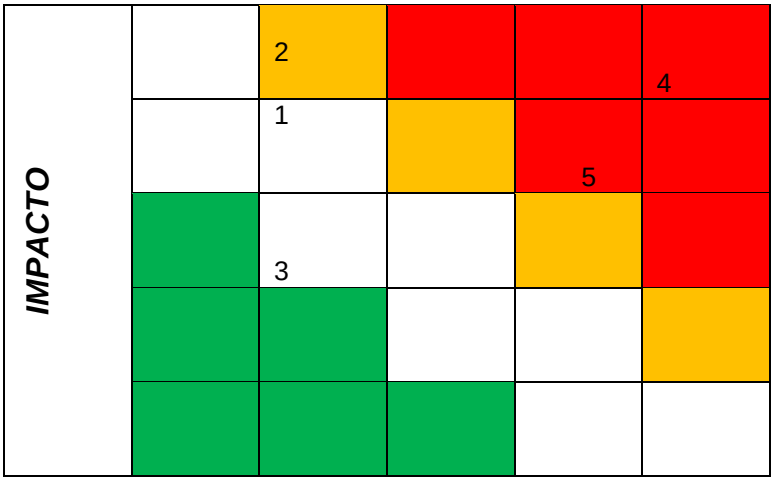
En este apartado se incluye una representación gráfica de los proyectos basándonos en dos de sus atributos: Impacto y Dificultad.

El gráfico nos muestra de una forma clara y sencilla como están posicionados los proyectos respecto a estos dos atributos. Su objetivo permite identificar fácilmente cuales son los prioritarios, es decir, requieren menos esfuerzo y tendrán mayor impacto positivo en la organización.

Tabla 33. Proyectos.

#	Proyecto
1	Organización de la seguridad y su política de aplicación.
2	Formación y concienciación de seguridad.
3	Mejora de la gestión de incidencias y problemas.
4	Continuidad y recuperación del negocio.
5	Aseguramiento de infraestructuras críticas

Imagen 4. Impacto y Esfuerzo.



ESFUERZO

Imagen 5. Escala Impacto y Esfuerzo.

Muy alto	
Alto	
Medio	
Bajo	

5. AUDITORÍA DE CUMPLIMIENTO

5.1 Introducción

Llegados a esta fase, conocemos los activos de la empresa y hemos evaluado las amenazas. Es el momento de hacer un alto en el camino y evaluar hasta que punto la empresa cumple con las buenas prácticas en materia de seguridad. La ISO/IEC 27002:2013 nos servirá como marco de control del estado de la seguridad.

5.2 Metodología

5.3 Evaluación de la madurez

El objetivo es evaluar la madurez de la seguridad en lo que respecta a los diferentes dominios de control y los 114 controles planteados por la ISO/IEC 27002:2013. De forma resumida, los dominios que deben analizarse son:

- Política de seguridad
- Organización de la seguridad de la información.
- Seguridad en los recursos humanos
- Gestión de activos
- Control de acceso
- Cifrado
- Seguridad física y ambiental
- Operaciones de seguridad
- Gestión de comunicaciones y operaciones.
- Adquisición, desarrollo y mantenimiento de Sistemas de Información
- Relaciones con proveedores
- Gestión de incidentes
- Gestión de continuidad de negocio
- Cumplimiento /Conformidad

El estudio debe realizar una revisión de los 114 controles planteados por la norma para cumplir con los diferentes objetivos de control – el número de los cuales se indica entre paréntesis para cada uno de los dominios-. Esta estimación la realizaremos según la siguiente tabla, que se basa en el Modelo de Madurez de la Capacidad (CMM):

Tabla 34. Modelo de Madurez de la Capacidad (CMM):

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	**L0**	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	**L1**	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas.

50%	**L2**	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	**L3**	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	**L4**	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	**L5**	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

(5) Política de seguridad

Objetivo: Proporcionar la dirección de gestión y apoyo a la seguridad de la información de acuerdo con los requerimientos del negocio y las leyes y reglamentos pertinentes.

Tabla 35. Evaluación de madurez de la capacidad Política de Seguridad.

Control		Evaluación
5. Política de Seguridad		10%
5.1 Dirección de la gestión de seguridad de la información		10%
5.1.1	Políticas de la seguridad de la información	10%
5.1.2	Revisión de las políticas de la seguridad de la información	10%

(6) Organización de la seguridad de la información.

Objetivo 6.1: Establecer un marco de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la organización.

Objetivo 6.2: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

Tabla 36. Evaluación de madurez de la capacidad Organización de la seguridad de la Información.

Control		Evaluación
6. Organización de la seguridad de la información		1%
6.1 Organización interna		2%
6.1.1	Funciones y responsabilidades de seguridad de información	10%
6.1.2	Segregación de funciones	0%
6.1.3	Contacto con las autoridades.	0%
6.1.4	Contacto con grupos de interés especiales	0%
6.1.5	Seguridad de la información en la gestión de proyectos	0%
6.2 Dispositivos móviles y Teletrabajo		0%
6.2.1	Política de dispositivos móviles	0%
6.2.2	Teletrabajo	0%

(7) Seguridad de Recursos Humanos

Objetivo 7.1: Asegurarse de que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.

Objetivo 7.2: Asegurarse de que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información.

Objetivo 7.3: Proteger los intereses de la organización, como parte del proceso de cambiar o terminar el empleo.

Tabla 37. Evaluación de madurez de la capacidad Seguridad de Recursos Humanos.

Control		Evaluación
7. Seguridad de Recursos Humanos		37%
7.1 Antes del empleo		30%
7.1.1	Screening	10%
7.1.2	Términos y condiciones de empleo	50%
7.2 Durante el empleo		30%
7.2.1	Responsabilidades de gestión	50%
7.2.2	Conciencia de seguridad de la información, educación y entrenamiento	10%
7.2.3	Proceso disciplinario	10%
7.3 Terminación y cambio de empleo		50%
7.3.1	Terminación o cambio de las responsabilidades de empleo	50%

(8) Gestión de Activos

Objetivo 8.1: Identificar activos de la organización y definir las responsabilidades de protección adecuados.

Objetivo 8.2: Asegurar que la información recibe un nivel adecuado de protección de acuerdo con su importancia para la organización.

Objetivo 8.3: Evitar la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios de comunicación.

Tabla 38. Evaluación de madurez de la capacidad Gestión de Activos.

Control		Evaluación
8. Gestión de Activos		5%
8.1 Responsabilidad de los activos		10%
8.1.1	Inventario de Activos	10%
8.1.2	Propiedad de los activos	10%
8.1.3	Uso aceptable de los activos	10%
8.1.4	Retorno de los activos	10%
8.2 Clasificación de la Información		3%
8.2.1	Clasificación de la Información	0%
8.2.2	Etiquetado de la Información	0%
8.2.3	Manejo de Activos	10%
8.3 Manejo de Medios		3%
8.3.1	Gestión de medios extraíbles	10%
8.3.2	Eliminación de medios	0%
8.3.3	Transferencia de medios	0%

	físicos	

(9) Control de Acceso

Objetivo 9.1: Limitar el acceso a las instalaciones de procesamiento de la información y de la información.

Objetivo 9.2: Garantizar el acceso del usuario autorizado y evitar el acceso no autorizado a sistemas y servicios.

Objetivo 9.3: Hacer que los usuarios sean responsables de salvaguardar su información de autenticación.

Objetivo 9.4: Prevenir el acceso no autorizado a los sistemas y aplicaciones.

Tabla 39. Evaluación de madurez de la capacidad Control de Acceso.

Control		Evaluación
9. Control de Acceso		18%
9.1 Business requirements of access control		50%
9.1.1	Política de control de acceso.	50%
9.1.2	Acceso a las redes y servicios de red	50%
9.2 Gestión de acceso de usuario		10%
9.2.1	Registro de usuario y cancelación de registro	10%
9.2.2	Acceso aprovisionamiento del usuario	10%
9.2.3	Gestión de derechos de accesos privilegiados	10%
9.2.4	Gestión de la información de autenticación de secreto de los usuarios	10%
9.2.5	Revisión de los derechos de acceso de usuario	10%
9.2.6	La eliminación o el ajuste de los derechos de acceso	10%
9.3 Responsabilidades del usuario		10%
9.3.1	El uso de información secreta de autenticación	10%
9.4 Control del sistemas y acceso a las aplicaciones		2%
9.4.1	Restricción de acceso Información	10%
9.4.2	Procedimientos de inicio de sesión seguro	10%
9.4.3	Sistema de gestión de contraseña	50%
9.4.4	El uso de los programas de servicios públicos privilegiados	10%

9.4.5	Control de acceso al código fuente del programa	10%

(10) Criptografía

Objetivo 10.1: Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y / o integridad de la información.

Tabla 40. Evaluación de madurez de la capacidad Criptografía.

Control		Evaluación
10. Criptografía		25%
10.1 Controles criptográficos		25%
10.1.1	Política sobre el uso de controles criptográficos	0%
10.1.2	Gestión de claves	50%

(11) Seguridad física y ambiental

Objetivo 11.1: Evitar autorizado física de acceso, daños e interferencia a la información y procesamiento de información sobre las instalaciones de la organización.

Objetivo 11.2: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

Tabla 41. Evaluación de madurez de la capacidad Seguridad física y ambiental.

Control		Evaluación
11 Seguridad física y ambiental		21.5%
11.1 áreas seguras		10%
11.1.1	Perímetro de seguridad física	10%
11.1.2	Controles de entrada físicas	10%
11.1.3	Asegurar oficinas, habitaciones e instalaciones	10%
11.1.4	La protección contra amenazas externas y ambientales	10%
11.1.5	Trabajar en zonas seguras	10%
11.1.6	Zonas de entrega y carga	10%
11.2 Equipo		33%
11.2.1	Ubicación y protección del equipo	50%
11.2.2	Apoyo a los servicios públicos	50%
11.2.3	seguridad cableado	50%
11.2.4	Mantenimiento del equipo	50%
11.2.5	Eliminación de los activos	50%
11.2.6	Seguridad de equipo y activos fuera de las	10%

	instalaciones	
11.2.7	Eliminación segura o la reutilización de los equipos	10%
11.2.8	Equipos de usuario desatendidos	10%
11.2.9	Escritorio limpio y política pantalla limpia	10%

(12) Operaciones de seguridad

Objetivo 12.1: Asegurar operaciones correctas y seguras de instalaciones de procesamiento de información.

Objetivo 12.2: Asegurar que las instalaciones de procesamiento de información y la información están protegidos contra el malware.

Objetivo 12.3: Evitar la pérdida de datos.

Objetivo 12.4: Registrar eventos y generar evidencia.

Objetivo 12.5: Garantizar la integridad de los sistemas operativos.

Objetivo 12.6: prevenir la explotación de vulnerabilidades técnicas.

Objetivo 12.7: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.

Tabla 42. Evaluación de madurez de la capacidad Operaciones de seguridad.

Control		Evaluación
12. Operaciones de seguridad		40%
12.1 Procedimientos y responsabilidades operacionales		17.5%
12.1.1	Procedimientos operativos documentados	50%
12.1.2	Gestión del cambio	10%
12.1.3	Gestión de la capacidad	10%
12.1.4	Separación de desarrollo, pruebas y entornos operativos	0%
12.2 Protección contra el malware		50%
12.2.1	Controles contra el malware	50%
12.3 Copias de seguridad		50%
12.3.1	Copia de seguridad de la información	50%
12.4 Registro y seguimiento		10%
12.4.1	registro de eventos	10%
12.4.2	Protección de la información de registro	10%
12.4.3	Registros de administrador y operador	10%
12.4.4	sincronización de reloj	10%
12.5 El control de software operativo		90%

12.5.1	La instalación del software en los sistemas operativos	90%
12.6 Técnico de gestión de vulnerabilidades		50%
12.6.1	Gestión de vulnerabilidades técnicas	10%
12.6.2	Las restricciones a la instalación de software	90%
12.7 Sistemas de información consideraciones de auditoría		10%
12.7.1	Sistemas de información controles de auditoría	10%

(13) Seguridad de las comunicaciones

Objetivo 13.1: Garantizar la protección de la información en las redes y sus instalaciones de apoyo de procesamiento de información.

Objetivo 13.2: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

Tabla 43. Evaluación de madurez de la capacidad Seguridad de las comunicaciones.

Control		Evaluación
13. Seguridad de las comunicaciones		30%
13.1 Gestión de la seguridad de red		50%
13.1.1	Controles de red	50%
13.1.2	Seguridad de los servicios de red	50%
13.1.3	Segregación en redes	50%
13.2 transferencia de información		10%
13.2.1	Las políticas y los procedimientos de transferencia de información	10%
13.2.2	acuerdos sobre la transferencia de información	10%
13.2.3	mensajería electrónica	10%
13.2.4	acuerdos de confidencialidad o de no divulgación	10%

(14) Sistema de adquisición, desarrollo y mantenimiento

Objetivo 14.1: Asegurarse de que la seguridad informática es una parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

Objetivo 14.2: Garantizar la seguridad de la información que se diseña e implementa dentro del ciclo de vida de desarrollo de sistemas de información.

Objetivo 14.3: Garantizar la protección de los datos utilizados para las pruebas.

Tabla 44. Evaluación de madurez de la capacidad Sistema de adquisición, desarrollo y mantenimiento.

Control		Evaluación
14. Sistema de adquisición, desarrollo y mantenimiento		4.6%
14.1 Security requirements of information systems		0%
14.1.1	Información de análisis de requisitos de seguridad y la especificación	0%
14.1.2	Asegurar los servicios de aplicaciones en las redes públicas	0%
14.1.3	protección de las transacciones de servicios de aplicaciones	0%
14.2 Seguridad en los procesos de desarrollo y de apoyo		3.4%
14.2.1	política de desarrollo seguro	10%
14.2.2	Procedimientos de control de cambio de sistema	0%
14.2.3	Revisión técnica de aplicaciones después de la plataforma operativa	0%
14.2.4	restricciones a los cambios en los paquetes de software	0%
14.2.5	Principios de ingeniería de sistemas seguros	0%
14.2.6	Entorno de desarrollo seguro	10%
14.2.7	desarrollo outsourced	0%
14.2.8	Pruebas de seguridad Sistema	10%
14.2.9	Pruebas de aceptación del sistema	10%
14.3 datos de prueba		10%
14.3.1	Protección de los datos de prueba	10%

(15) Relaciones con los proveedores

Objetivo 15.1: Garantizar la protección de los activos de la organización que sea accesible por los proveedores.

Objetivo 15.2: Mantener un nivel acordado de seguridad de la información y la prestación de servicios en línea con los acuerdos con proveedores.

Tabla 45. Evaluación de madurez de la capacidad Relación con los proveedores.

Control		Evaluación
15. Relaciones con los proveedores		0%
15.1 Seguridad de la información en las relaciones con proveedores		0%
15.1.1	Política de seguridad de la información para relaciones con los proveedores	0%
15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	0%
15.1.3	Cadena de información y tecnología de comunicación de suministro	0%
15.2 Gestión de la prestación de servicios de proveedores		0%
15.2.1	Seguimiento y la revisión de los servicios de proveedores	0%
15.2.2	Gestión de cambios en los servicios de proveedores	0%

(16) Información de gestión de incidentes de seguridad

Objetivo 16.1: Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluidos los de comunicación en los eventos de seguridad y debilidades.

Tabla 46. Evaluación de madurez de la capacidad Información de gestión de incidentes de la seguridad.

Control		Evaluación
16. Información de gestión de incidentes de seguridad		10%
16.1 Gestión de incidentes de seguridad de la información y mejoras		10%
16.1.1	Responsabilidades y procedimientos	10%
16.1.2	Presentación de informes de eventos de seguridad de información	10%
16.1.3	Informes debilidades de seguridad de información	10%
16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	10%
16.1.5	Respuesta a incidentes de seguridad de la información	10%
16.1.6	Aprendiendo de los incidentes de seguridad de la información	10%
16.1.7	acopio de pruebas	10%

(17) Los aspectos de seguridad de información de la gestión de la continuidad del negocio

Objetivo 17.1: Información continuidad de seguridad debe estar integrada en los sistemas de gestión de continuidad de negocio de la organización.

Objetivo 17.2: Asegurar la disponibilidad de instalaciones de procesamiento de información.

Tabla 47. Evaluación de madurez de la capacidad Los aspectos de seguridad de información de la gestión de la continuidad del negocio.

Control		Evaluación
17. Los aspectos de seguridad de información de la gestión de la continuidad del negocio		10%
17.1 Información continuidad seguridad		10%
17.1.1	Planificación información continuidad seguridad	10%
17.1.2	implementación de la información continuidad seguridad	10%
17.1.3	Verificar, revisar y evaluar la información de seguridad de continuidad	10%
17.2 despidos		10%
17.2.1	Disponibilidad de instalaciones de procesamiento de información	10%

(18) Conformidad

Objetivo 18.1: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales en materia de seguridad de la información y de las exigencias de seguridad.

Objetivo 18.2: Garantizar la seguridad de la información que se implementa y opera de acuerdo con las políticas y procedimientos de la organización.

Tabla 48. Evaluación de madurez de la capacidad Conformidad

Control		Evaluación
18. Conformidad		10%
18.1 cumplimiento de los requisitos legales y contractuales		10%
18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	10%
18.1.2	derechos de propiedad Intelectual	10%
18.1.3	Protección de los registros	10%
18.1.4	Privacidad y protección de datos personales	10%
18.1.5	Reglamento de los controles criptográficos	10%
18.2 Revisiones de seguridad de información		10%

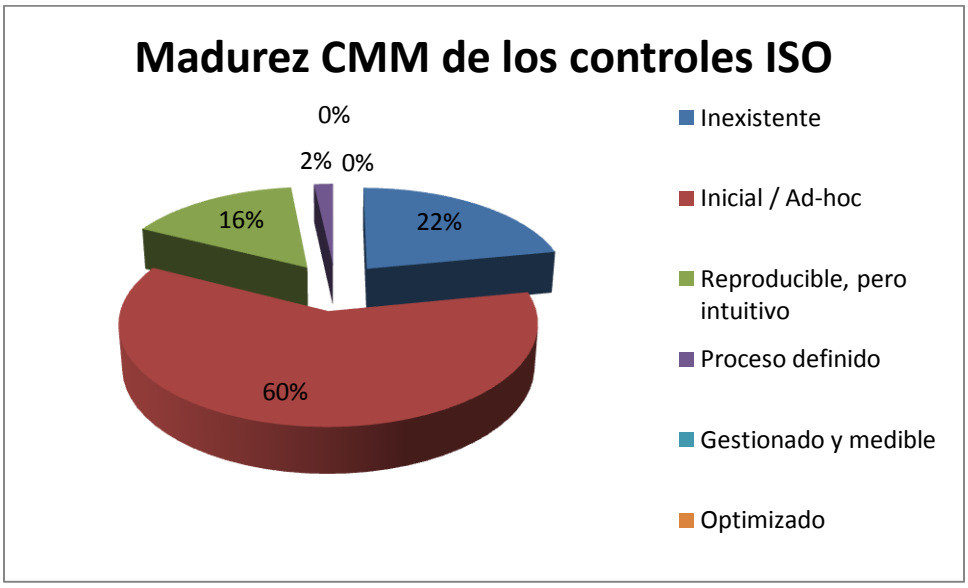
18.2.1	Revisión independiente de seguridad de la información	10%
18.2.2	El cumplimiento de las políticas y estándares de seguridad	10%
18.2.3	Revisión de cumplimiento técnico	10%

5.4 Presentación de resultados

Tabla 49. Resultados 114 controles - evaluación de madurez.

EFECTIVIDAD	CMM	SIGNIFICADO	NÚMERO DE CONTROLES
0%	**L0**	Inexistente	25
10%	**L1**	Inicial / Ad-hoc	69
50%	**L2**	Reproducible, pero intuitivo	18
90%	**L3**	Proceso definido	2
95%	**L4**	Gestionado y medible	0
100%	**L5**	Optimizado	0

Gráfica 2. Madurez CMM de los controles ISO.



Una visión más detallada es la que se presenta como 'diagrama de radar' que mostraría el nivel de cumplimiento por capítulo ISO. Anticipándonos a las medidas, será interesante comparar el estado actual con el estado deseado:

Gráfica 3. Madurez de los controles.

6. CONCLUSIONES

Objetivos conseguidos

La organización entiende de forma clara que debe comenzar a realizar todas las actividades que sean necesarias para establecer un SGSI y posteriormente poder aplicar a la certificación de la norma ISO/IEC 27001:2013.

La organización obtiene documentos muy importantes para continuar el camino que lo conduzca a una buena implementación de un SGSI.

Establecimiento de un plan de auditoría, informe de auditoría y programa de auditoría.

Creación de la política de seguridad.

La organización reconoce las debilidades que tiene en materia de seguridad de la información.

El aprendizaje obtenido sobre la norma ISO / IEC 27001 es muy importante para mi desarrollo profesional en esta área del conocimiento.

Las bases que fueron dadas a conocer permiten que todo el personal de la organización tenga conciencia de la importancia de realizar procesos con calidad y que sean documentados.

Objetivos no conseguidos

La creación de más documentos que apoyen la organización, el trabajo de la misma es muy lento para el levantamiento de la información, por ejemplo: diagrama de red.

El impacto potencial que apoye los proyectos en la gestión de riesgos, es difícil estimar sin mucha información, pero se logran proyectos que son los primeros con los que pueden comenzar a establecer planes presupuestales para ser ejecutados.

La sensibilización de toda la organización en el tema de SGSI, no fue posible reunirlos a todos durante las últimas fases del proyecto.

La evaluación de la madurez indica que puede haber un retroceso en los procesos, ya que comenzarán a desarrollar desde cero algunos de los documentos.

Ampliaciones del trabajo

Este trabajo puede servir como base para que la organización continúe en las tareas que deben ser realizadas con el fin de a mediano plazo acceder a la certificación ISO/IEC 27001:2013

7. BIBLIOGRAFÍA

Material de estudio asignatura Sistemas de Gestión de Seguridad de Información

Norma ISO/IEC 27001:2013

SGSI

http://www.iso27000.es/sgsi.html

Auditorías internas

http://www.revistadintel.es/Revista1/DocsNum22/Normas/Corletti.pdf

http://sociedaddelainformacion.wordpress.com/2006/11/12/auditoria-interna-de-un-sgsi-iso-27001/

Gestión de indicadores

http://sgsi-iso27001.blogspot.com/

Cuadro de mando indicadores

http://www.upo.es/cic/export/sites/webcic/SGS/CMI/DOC_CIC-51_SGS_CMI_2013.pdf

Gestión de roles y responsabilidades

http://www.ecopetrol.com.co/documentos/64203_Anexo_15._ECP-DTI-G-11_Roles_y_Responsabilidades_de_Seguridad_de_la_Informaci%C3%B3n_2010-v-1%5B1%5D.pdf

Políticas de seguridad

http://www.utp.edu.co/cms-utp/data/bin/UTP/web/uploads/media/calidad/documentos/politicas_sgsi.pdf

Modelo de política de seguridad

http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf

Pasos para implementar políticas y procedimientos

http://www.iso27001standard.com/es/blog/2011/03/08/siete-pasos-para-implementar-politicas-y-procedimientos/

MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VEPM7Pl5OSo

Libro I. Método – MAGERIT v3

http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf

Análisis de Riesgo Informático
http://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo_inform%C3%A1tico

Libro III – Guía de Técnicas – MAGERIT

file:///C:/Users/pc/Downloads/2012_Magerit_v3_libro3_gu%C3%ADa%20de%20t%C3%A9cnicas_es_NIPO_630-12-171-8.pdf