PLAN DE IMPLEMENTACIÓN DE LA ISO/IEC 27001:2005

Master Interuniversitario en Seguridad de las TIC MISTIC

Este documento presenta de manera práctica la construcción de un plan de implementación de la norma ISO/IEC 27001:2005, lo cual es un aspecto clave para cualquier organización que desee alinear los objetivos del negocio orientado a un Sistema de Gestión de la Seguridad de la Información (SGSI) que permitan alcanzar el nivel adecuado de seguridad.

HELDIS LIZARAZO HERNÁNDEZ
TUTOR: ANTONIO JOSÉ SEGOVIA HENARES

Tabla de Contenido

1. SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL.

1.1 INTRODUCCIÓN AL PROYECTO.

La información es el activo más importante de cada organización y por ello aparece la necesidad de la seguridad de la información, que nos permite proteger esta con el fin de mantener minimizados los riesgos en los que se puede verse afectada la organización.

Es muy común encontrar organizaciones que no tienen ningún criterio definido para la gestión de la seguridad de la información, la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI) es la manera más eficaz de poder coordinar y gestionar todos los requerimientos necesarios que conduzcan a la obtención de los objetivos de las organizaciones.

La gestión de la seguridad conlleva a tratar los posibles efectos que tendrían los activos si se enfrentan a un riesgo por esta razón debe ser un proceso de mejora continua y de constante adaptación a los cambios en la organización en cuanto a procesos de negocio y a la tecnología implicada.

La mejor forma de lograr el objetivo es a través de las normas internacionales ISO/IEC 27001:2005 que proporciona un marco de gestión de la seguridad de la información aplicable a cualquier organización. En las organizaciones grandes, medianas o pequeñas, públicas o privadas necesitan establecer medidas que aseguran sus activos más importantes que es la información para hacerlas más competitivas.

1.2 ENFOQUE Y SELECCIÓN DE LA EMPRESA.

1.2.1 Descripción Actual de la Entidad.

La organización, como parte integrante de las autoridades de la República y, como cuerpo armado permanente de naturaleza civil a cargo de la Nación, está instituida para proteger a todas las personas residentes en Colombia, en su vida, honra,

bienes, creencias y demás derechos y libertades para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares. Así mismo, para el mantenimiento de las condiciones necesarias para el ejercicio de los derechos y libertades públicas y para asegurar que los habitantes de Colombia convivan en paz.

Esta entidad se encuentra distribuida en todo el territorio nacional, por ser de gran envergadura se realizara el análisis a una de sus sedes. La sede donde se realiza el estudio ocupa una área de 3250 M2 áreas, encontramos distintas instalaciones donde funcionan varios departamentos pero por sus funciones sensibles no son nombradas. El Departamento de Informática está encargado de brindar los servicios telemáticos a todo los departamentos en ella se encuentra el centro de procesamientos de datos (CPD), y los servicios que se ofrecen a todas las unidades están alojados en el CPD.

La entidad tiene conocimientos sobre las buenas prácticas de la gestión de la información, porque de la dirección general se han emitido oficios que tienen que ver con el tema sin embargo las personas que se encuentran en la sede donde se realizara el estudio no tienen capacitaciones que permita contar con personal idóneo para la implantación de las buenas prácticas como son COBIT e ITIL.

1.2.3 Activos de Información

La entidad cuenta con el departamento de telemática su visión está sustentada en soluciones tecnológicas efectivas y de vanguardia aplicadas al 100% del servicio. Su despliegue se realiza con personal profesional y técnico en el área de las Tecnologías de la Información y las Telecomunicaciones a través de los Grupos de Telemática.

En la sede de telemática donde se realiza el estudio se cuenta con un equipo de trabajo de 50 personas que prestan soporte a nivel tecnológico, la infraestructura tecnológica consta de una granja de 35 servidores, 2 cabinas de almacenamiento, CPD nivel 2, 45 cámaras de vigilancia, 1500 PC, 5 Firewalls, 6 Router, 3 Switch Core C3, 30 switch de borde.

1.3 OBJETIVOS DEL PLAN DIRECTOR.

El principal objetivo es la realización de un análisis y diagnóstico de la seguridad de los sistemas de información de la SGSI basados en los estándares de la ISO 27001 y utilizando la metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT, que permitan analizar para poder proponer las políticas pertinentes para la solución a la protección de la información y llegar al objetivo de definir un plan director de seguridad.

La entidad está comprometida para asumir las responsabilidades dentro del plan del tal manera que se satisfaga todos los requerimientos para poder cubrir todas sus necesidades. Para poder obtener este objetivo es necesario:

- Proporcionar apoyo a todas las iniciativas de seguridad.
- Identificar cuáles son los objetivos de la seguridad para poder integrar los procesos relevantes dentro de la organización con el fin de identificar los procesos más críticos dentro de la organización.
- Iniciar un programa de sensibilización para mantener informado acerca de la seguridad de información.

1.3.1 Plan Director.

El Plan Director de Seguridad tiene por misión el establecimiento de políticas y controles en el contexto de la organización a corto, mediano y largo plazo que permitan garantizar una adecuada gestión de la seguridad de la información. Este se logra a través de un conjunto de documentos y herramientas que demuestran y ayudan a realizar la gestión de la seguridad como son la ISO 27001 y la metodología para el análisis y gestión de riesgos de los sistemas de información MAGERIT.

El Plan Director de Seguridad se elabora después del análisis de diferencial (GAP) de la norma ISO/IEC 27001:2005, se tendrá en cuenta aspectos como recurso humano, administrativo, técnicos y procedimentales asociados a los sistemas de información.

1.4 ANÁLISIS DIFERENCIAL DE LA EMPRESA.

	POLÍTICA DE SEGURIDAD		
5.1	Política de seguridad de la información		
5.1.1	Documento de política de seguridad de la información	Existe un documento de política pero fue creado hace mas de 8 años , los cuales han surgido muchos cambios en los sistemas y no cubre las necesidad actual.	3, DEFINIDA
5.1.2	Revisión de la política de seguridad de la información	Desde su aprobación no se han hecho mas revisiones.	1, INICIAL
	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN		
6.1	Organización interna.		
6.1.1	Compromiso de la Dirección con la seguridad de la información.	A nivel de Dirección General hay un comité pero en las sedes solo se cuenta con un funcionario y un grupo que lo apoya pero no se hace seguimiento al cumplimiento de las políticas	2, REPETIBLE
6.1.2	Coordinación de la seguridad de la información	existe un plan para las actividades desarrolladas pero no se le da cumplimiento	2, REPETIBLE
6.1.3	Asignación de responsabilidades relativas a la seg. de la información	Existen los procedimientos de asignación de responsabilidades. Aunque en algunos casos se obvia este punto.	3, DEFINIDA
6.1.4	Proceso de autorización de recursos para el tratamiento de la información	existe un proceso de autorización para los nuevos recursos	3, DEFINIDA
6.1.5	Acuerdos de confidencialidad	Existen los acuerdos de confidencialidad, pero no se tiene un control riguroso.	3, DEFINIDA
6.1.6	Contacto con las autoridades	Existen de procedimientos ante una eventualidad en las instalaciones, sin embargo en cuanto a la seguridad de la información no se han establecidos los procedimientos necesarios.	3, DEFINIDA
6.1.7	Contacto con grupos de especial interés	No existe relaciones con proveedores en materia de seguridad solo se hacen capacitaciones.	0, INEXISTENTE
6.1.8	Revisión independiente de la seguridad de la información.	Se hacen revisiones dos veces al año de MECI que incluye revisión en materia de seguridad. Pero los hallazgos muchas veces no se toman acciones correctivas.	3, DEFINIDA
6.2	Terceros		
6.2.1	Identificación de los riesgos derivados del acceso de terceros	no se identifican los riesgos , los proveedores siempre son seleccionado por procesos de contratación así que el mejor oferente gana el contrato,	0, INEXISTENTE
6.2.2	Tratamiento de la seguridad en la relación con los clientes	se establecen controles	3, DEFINIDA
6.2.3	Tratamiento de la seguridad en contratos con terceros	Cuando se realiza un contrato por prestación de servicios se incluye unas cláusulas de seguridad, pero no se es riguroso con este tema.	3, DEFINIDA
	GESTIÓN DE ACTIVOS		
7.1	Responsabilidad sobre activos		
7.1.1	Inventarios de activos	se realiza inventarios de equipos pero no se lleva el control de los equipos que se han dado de baja así que esta información no es actualizada, solo se lleva inventarios de los activos de información de algunos servidores.	3, DEFINIDA

7.1.2	Propiedad de los activos	Se le asigna a un propietario, ya que los activos entran al almacén y antes de salir lleva la placa de inventarios y se le asigna a un usuario.	3, DEFINIDA
7.1.3	Uso aceptable de los activos	No existe una guía de uso aceptable de recursos.	2, REPETIBLE
7.2	Clasificación de la información		
7.2.1	Directrices de clasificación	La información es clasificada de acuerdo al nivel de criticidad, pero no se tiene un seguimiento rigurosos de la directriz	3, DEFINIDA
7.2.2	Etiquetado y manipulado de la información	Existe el documento donde se clasifica la información se etiqueta el tipo de información y la manipulación que se debe tener, si la información es de carácter secreto y ultrasecreto se tiene control el resto de información se es más laxo en la manipulación.	3, DEFINIDA
	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS		
8.1	Antes del empleo		
8.1.1	Funciones y responsabilidades	Existe un manual de funciones para todo el personal que se encuentra a nomina, pero en los casos de personal por prestación de servicios no se tiene establecidos un documento donde se describan las responsabilidades respecto a la seguridad.	3, DEFINIDA
8.1.2	Investigación de antecedentes	Se realiza estudios de seguridad de personas y se le pide el certificado de antecedentes antes de las contrataciones.	3, DEFINIDA
8.1.3	Términos y condiciones de contratación	Se firma una clausula legal,	4, ADMINISTRADA
8.2	Durante el empleo		
8.2.1	Responsabilidades del cese o cambio	No existe una guía de uso aceptable de recursos.	1, INICIAL
8.2.2	Concienciación, formación y capacitación en seg. De la información	Si existe capacitaciones pero no son frecuentes	2, REPETIBLE
8.2.3	Proceso disciplinario.	No existe un procedimiento acerca de qué hacer con respecto a las violaciones de seguridad que realicen los empleados.	1, INICIAL
8.3	Cese del empleo o cambio de puesto de trabajo		
8.3.1	Responsabilidades del cese o cambio	No existe un procedimiento documentado con respecto al cese o cambio de puesto de personal.	0, INEXISTENTE
8.3.2	Devolución de activos	No existe un procedimiento de devolución de activos.	0, INEXISTENTE
8.3.3	Retirada de los derechos de acceso	Existe un procedimiento documentado respecto a la supresión de derechos de accesos.	3, DEFINIDA
	SEGURIDAD FÍSICA Y DEL ENTORNO		
9.1	Áreas seguras		
9.1.1	Perímetro de seguridad física	Existe controles para el acceso al complejo los visitantes deben tener una autorización de alguien que labore internamente para tener acceso, se realiza el trámite de un formato donde se especifique los datos de la persona que entra. Una vez autorizada la persona quien facilito su acceso debe acompañarlo al lugar donde se desplace	4, ADMINISTRADA
9.1.2	Controles físicos de entrada	existen controles en ciertos departamentos para el acceso en otros no.	3, DEFINIDA

9.1.3	Seguridad de oficinas, despachos e instalaciones	El CPD es fácil su acceso por tener el sistema biométrico dañado sin embargo para entrar a ese lugar hay que haber pasado por otra puerta que tiene sistema biométrico.	3, DEFINIDA
9.1.4	Protección contra las amenazas externas y de origen ambiental	El CPD no tiene sistemas de detección y extinción de incendios, en cada oficina existe extintores.	0, INEXISTENTE
9.1.5	Trabajo en áreas seguras	Si existen áreas en las cuales se especifican en una directiva el trabajo en esas áreas.	3, DEFINIDA
9.1.6	Áreas de acceso público y de carga y descarga	Las áreas de acceso al público siempre están un encargado para el acompañamiento en el lugar.	4, ADMINISTRADA
9.2	Seguridad de los equipos		
9.2.1	Emplazamiento y protección de equipos	existe procedimientos para la protección de equipos	3, DEFINIDA
9.2.2	Instalaciones de suministro	Lo único con que cuenta una planta eléctrica es el CPD, ante fallas el resto del complejo queda sin servicios.	0, INEXISTENTE
9.2.3	Seguridad de cableado	Existe control en algunos centros donde solo es accedido por personal autorizados en otros el control es mínimo.	1, INICIAL
9.2.4	Mantenimiento de los equipos	los equipos se monitorean constantemente, pero si fallan no se tiene un plan de contingencia.	2, REPETIBLE
9.2.5	Seguridad de los equipos fuera de las instalaciones	se tiene el mismo control de los equipos que están dentro de las instalaciones.	3, DEFINIDA
9.2.6	Reutilización o retirada segura de equipos	no se tiene buenas prácticas de retiradas de equipos.	0, INEXISTENTE
9.2.7	Retirada de materiales propiedad de la empresa	Existen controles pero no son lo más adecuados.	2, REPETIBLE
	GESTIÓN DE COMUNICACIONES Y OPERACIONES		
10.1	Responsabilidades y procedimientos de operación		
10.1.1	Documentación de los procedimientos de operación	existe procedimientos de las operaciones pero no todo los procedimientos están suficientemente documentados.	2, REPETIBLE
10.1.2	Gestión de cambios	existe el proceso de control de cambios pero no todos los formatos aplican a las situaciones.	2, REPETIBLE
10.1.3	Segregación de tareas	se segregan funciones y tareas.	3, DEFINIDA
10.1.4	Separación de los recursos de desarrollo, prueba y operación	no existe política al respecto.	0, INEXISTENTE
10.2	Gestión de la provisión de servicios por terceros		
10.2.1	Provisión de servicios	se tiene control sobre los acuerdos pero no existe una política de revisión	1, INICIAL
10.2.2	Supervisión y revisión de los servicios prestados por terceros	se revisan los niveles de servicios de terceros pero no existe una política para la gestión de servicios.	1, INICIAL
10.2.3	Gestión del cambio en los servicios prestados por terceros	se gestionan los cambios pero no se tiene una política para la gestión de cambios.	2, REPETIBLE
10.3	Planificación y aceptación del sistema		
10.3.1	Gestión de capacidades	se realiza proyecciones anuales de las necesidades futuras	3, DEFINIDA
10.3.2	Aceptación del sistema	no existe las pruebas antes de entra en ejecución.	0, INEXISTENTE

10.4		Protección contra el código malicioso y descargable		
	10.4.1	Controles contra el código malicioso	se tiene una consola de antivirus.	2, REPETIBLE
	10.4.2	Controles contra el código descargado en el cliente	se tienen barreras perimetrales.	2, REPETIBLE
10.5		Copias de seguridad		
	10.5.1	Copias de seguridad de la información	se hacen copias de seguridad pero no se cuenta con las herramientas para hacerlas , actualmente las copias se hacen locales. No existe un procedimiento de copias de seguridad.	1, INICIAL
10.6		Gestión de la seguridad de las redes		
	10.6.1	Controles de red	se tienen implementados control de acceso	3, DEFINIDA
	10.6.2	Seguridad de los servicios de red	se tienen identificados las características de seguridad	3, DEFINIDA
10.7		Manipulación de los soportes		
	10.7.1	Gestión de soportes extraíbles	el uso de soportes extraíbles no está autorizado sin embargo no hay un control para este procedimientos	0, INEXISTENTE
	10.7.2	Retirada de soportes	no existe una política de retirada de soportes.	0, INEXISTENTE
	10.7.3	Procedimientos de manipulación de la información	existen controles pero no un procedimiento	3, DEFINIDA
	10.7.4	Seguridad de la documentación del sistema	se tiene un control pero no es el mas optimo	3, DEFINIDA
10.8		Intercambio de información		
	10.8.1	Políticas y procedimientos de intercambio de información	no existe una política, ni procedimiento para el intercambio de información.	0, INEXISTENTE
	10.8.2	Acuerdos de intercambio	no existe acuerdos de intercambios	0, INEXISTENTE
	10.8.3	Soportes físicos en transito	si existe pero no se utiliza el procedimiento para todos los casos.	3, DEFINIDA
	10.8.4	Mensajería electrónica	se tiene protección dela información contenida en los correos	2, REPETIBLE
	10.8.5	Sistemas de información empresariales	la conexiones se gestiona correctamente.	3, DEFINIDA
10.9		Servicios de comercio electrónicos		
	10.9.1	Comercio electrónico	no aplica	
	10.9.2	Transacciones en línea	no aplica	
	10.9.3	Información públicamente disponibles	la información pública está protegida de modificaciones	3, DEFINIDA
10.10		Supervisión		
	10.10.1	Registros de auditoría	se registran los eventos pero no existe una política	2, REPETIBLE
	10.10.2	Supervisión del uso del sistema	se supervisa el uso de los sistemas pero no existe una política	2, REPETIBLE
	10.10.3	Protección de la información de los registros	se protegen la información de los registros	3, DEFINIDA
	10.10.4	Registros de administración y operación	no existe un procedimiento de revisión.	1, INICIAL
	10.10.5	Registros de fallos	se tiene u software que permita monitorizar las conexiones de red	3, DEFINIDA
	10.10.6	Sincronización del reloj	se tiene sincronizados los reloj	3, DEFINIDA
		CONTROL DE ACCESO		
11.1		Requisitos de negocio para el control de acceso		
	11.1.1	Política de control de acceso	si hay política de control de acceso pero no se cumple dicha política.	3, DEFINIDA

11.2	Gestión de acceso de usuario		
11.2.1	Registro de usuario	se tiene un procedimiento pero no se revisa con frecuencia	3, DEFINIDA
11.2.2	Gestión de privilegios	Se gestionan los privilegios pero no tiene un procedimiento de gestión de privilegios.	3, DEFINIDA
11.2.3	Gestión de contraseñas de usuario	Se gestionan las contraseñas y se establece tiempo de caducidad.	3, DEFINIDA
11.2.4	Revisión de los derechos de acceso de usuario	No existe ningún procedimiento de revisión de derechos de accesos de usuario.	0, INEXISTENTE
11.3	Responsabilidades de usuario		
11.3.1	Uso de contraseñas	existen una guía de recomendaciones para elegir contraseñas	3, DEFINIDA
11.3.2	Equipo de usuarios desatendido	existe la política	3, DEFINIDA
11.3.3	Política de puestos de trabajo despejado y pantalla limpia	existe la política	3, DEFINIDA
11.4	Control de acceso a la red		
11.4.1	Política de uso de los servicios en red	existe política	3, DEFINIDA
11.4.2	Autenticación de usuario para conexiones externas	existe política	3, DEFINIDA
11.4.3	Identificación de los equipos en las redes	Hay creadas VLAN que nos permite identificar los equipos en la red, pero no se tienen el parte total de los inventarios.	2, REPETIBLE
11.4.4	Protección de los puertos de diagnóstico y configuración remotos	existen medidas de protección	3, DEFINIDA
11.4.5	Segregación de las redes	las redes están segregadas	3, DEFINIDA
11.4.6	Control de la conexión a la red	existe controles de conexión a la red	3, DEFINIDA
11.4.7	Control de encaminamiento (routing) de red	existe controles de encaminamiento de red	3, DEFINIDA
11.5	Control de acceso al sistema operativo		
11.5.1	Procedimientos seguros de inicio de sesión	existe mecanismos de inicio de sesión	3, DEFINIDA
11.5.2	Identificación y autenticación de usuario	existe mecanismos de identificación y autenticación de usuario	3, DEFINIDA
11.5.3	Sistemas de gestión de contraseñas	existe el sistema de gestión de contraseñas	3, DEFINIDA
11.5.4	Uso de los recursos del sistema	Las aplicaciones innecesarias son eliminadas del sistema	3, DEFINIDA
11.5.5	Desconexión automática de sesión	no existe	0, INEXISTENTE
11.5.6	Limitación del tiempo de conexión	no existe	0, INEXISTENTE
11.6	Control de acceso a las aplicaciones y a la información		
11.6.1	Restricción del acceso a la información	existe políticas en las restricciones de acceso de la información	3, DEFINIDA
11.6.2	Aislamiento de sistemas sensibles	si existe aislamiento de los sistemas sensibles	3, DEFINIDA
11.7	Ordenadores portátiles y teletrabajo		
11.7.1	Ordenadores portátiles y comunicaciones móviles	no existe políticas para dispositivos móviles	0, INEXISTENTE
11.7.2	Teletrabajo	no aplica	
	ADQUISICIÓN DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN		
12.1	Requisitos de seguridad de los sistemas de información		
12.1.1	Análisis y especificación de los requisitos de seguridad	se asumen las debilidades pero no se realiza evaluación de riesgos	2, REPETIBLE
12.2	Tratamiento correcto de las aplicaciones		
12.2.1	Validación de los datos de entrada	si existen los controles que protegen las aplicaciones	3, DEFINIDA

12.2.2	Control del procesamiento interno	si existe	3, DEFINIDA
12.2.3	Integridad de los mensajes	si existe	3, DEFINIDA
12.2.4	Validación de los datos de salida	no se validan los datos de salidas	0, INEXISTENTE
12.3	Controles criptográficos		
12.3.1	Política de uso de los controles criptográficos	existe solo para la información ultrasecreta	3, DEFINIDA
12.3.2	Gestión de claves	no existe	0, INEXISTENTE
12.4	Seguridad de los archivos del sistema		
12.4.1	Control de software en explotación	no existe controles	0, INEXISTENTE
12.4.2	Protección de los datos de prueba del sistema	no existe protección de los datos de pruebas	0, INEXISTENTE
12.4.3	Control de acceso al código fuente de los programas	no existe un control al código fuente	0, INEXISTENTE
12.5	Seguridad en los procesos de desarrollo y soporte		
12.5.1	Procedimientos de control de cambios	si existe los procedimientos pero no se cumple	3, DEFINIDA
12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	si existe el procedimientos pero no se cumple	3, DEFINIDA
12.5.3	Restricciones a los cambios en los paquetes de software	no se realizan cambios en los paquetes de software	3, DEFINIDA
12.5.4	Fugas de información	existe controles pero no son suficientes	3, DEFINIDA
12.5.5	Externalización del desarrollo de software	se realizan contratos para el desarrollo de algunos software	3, DEFINIDA
12.6	Gestión de las vulnerabilidades técnica		
12.6.1	Control de las vulnerabilidades técnicas	no se tienen suficientes controles de vulnerabilidades	2, REPETIBLE
	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN		
13.1	Notificación de eventos y puntos débiles de seguridad de la información		
13.1.1	Notificación de los eventos de seguridad de la información	no existe documentación de sistema de gestión de incidencias	0, INEXISTENTE
13.1.2	Notificación de puntos débiles de seguridad	no se hacen notificaciones de los puntos débiles	0, INEXISTENTE
13.2	Gestión de incidentes y mejoras de seguridad de la información		
13.2.1	Responsabilidades y procedimientos	no se tiene un esquema de procedimientos de incidencias	0, INEXISTENTE
13.2.2	Aprendizaje de los incidentes de seguridad de la información	no se tienen los mecanismos de aprendizaje sobre los incidentes de seguridad	0, INEXISTENTE
13.2.3	Recopilación de evidencias	no se sigue un procedimientos de las incidencias detectadas	0, INEXISTENTE
	GESTION DE LA CONTINUIDAD DEL NEGOCIO		
14.1	Aspectos de seguridad de la información en el proceso de la gestión de la continuidad del negocio		
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	no se tiene una gestión de continuidad	0, INEXISTENTE
14.1.2	Continuidad del negocio y evaluación de riesgos	no se tienen un plan de continuidad ni evaluación de riesgos	0, INEXISTENTE
14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información	idem	1, INICIAL
14.1.4	Marco de referencia para la planificación de la cont. Del negocio	idem	1, INICIAL

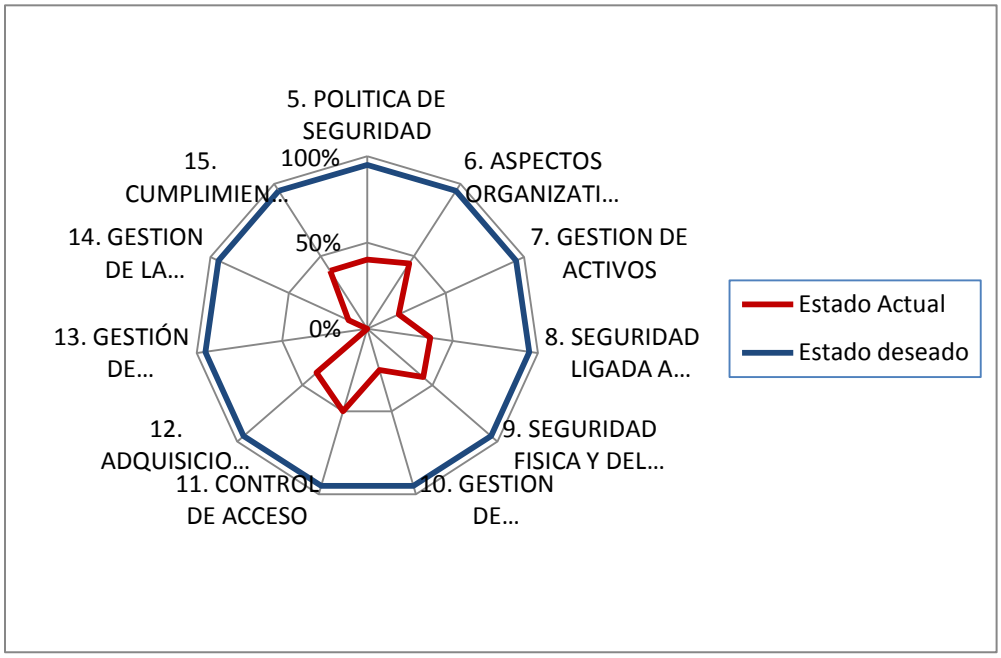
14.1.5	Pruebas, mantenimiento y revaluación de planes de continuidad	idem	1, INICIAL
	CUMPLIMIENTO		
15.1	Cumplimiento de los requisitos legales		
15.1.1	Identificación de la legislación aplicable	no se cumple al 100% las legislaciones vigentes	3, DEFINIDA
15.1.2	Derechos de propiedad intelectual	aún falta para cumplir totalmente con los derechos de propiedad intelectual	2, REPETIBLE
15.1.3	Protección de los documentos de la organización	se le da un tratamiento especial a los documentos una vez van a ser archivados	3, DEFINIDA
15.1.4	Protección de datos y privacidad de la información de carácter personal	aún falta para el tratamiento de la información de carácter personal	2, REPETIBLE
15.1.5	Prevención del uso indebido de recursos de tratamiento de la información	aun no se ha trabajado en este tema	0, INEXISTENTE
15.1.6	Regulación de los controles criptográficos	alguna documentación cumple con los controles criptográficos	3, DEFINIDA
15.2	Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico		
15.2.1	Cumplimiento de las políticas y normas de seguridad	se le hace un seguimiento informal pero se evidencia el no cumplimiento de las políticas	2, REPETIBLE
15.2.2	Comprobación del cumplimiento técnico	se realizan auditorias de MECI el cual se generan informes con las novedades detectadas para mejora	3, DEFINIDA
15.3	Consideraciones sobre las auditorias de los sistemas de información		
15.3.1	Controles de auditoria de los sistemas de información	en las auditorias se hace el levantamiento de novedades pero no se le hace seguimiento	2, REPETIBLE
15.3.2	Protección de las herramientas de auditoria de los Sist. información	no existen herramientas de auditoria	0, INEXISTENTE

1.4.1 Resumen Análisis Diferencial.

DOMINIO	Cumple	No Cumple
5. POLÍTICA DE SEGURIDAD	**40%**	**95%**
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**45%**	**55%**
7. GESTIÓN DE ACTIVOS	**20%**	**80%**
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**37%**	**63%**
9. SEGURIDAD FÍSICA Y DEL ENTORNO	**43%**	**57%**
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES	**25%**	**75%**
11. CONTROL DE ACCESO	**50%**	**50%**
12. ADQUISICIÓN DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	**39%**	**61%**
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	**0%**	**100%**
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**12%**	**88%**
15. CUMPLIMIENTO	**40%**	**60%**

1.5 RESULTADOS

Luego de realizado el análisis, se determinó que la entidad la cual está siendo objeto de estudio solo alcanza un 32% en el cumplimiento de los objetivo y por lo que la entidad espera al menos un cumplimiento del 95%, es evidente que se hace necesario emprender acciones para mejorar los porcentajes de cumplimiento y alcanzar el objetivo deseado. A continuación se muestra la representación gráfica del grado de madurez ISO 27001 e ISO 27002 de la entidad.



2. SISTEMA DE GESTIÓN DOCUMENTAL.

2.1 INTRODUCCIÓN.

Todos los sistemas de gestión deben tener como línea base un sistema de gestión documental que permita indicar el cumplimiento normativo, para esto se proporciona la documentación correspondiente para implementar un SGSI según la norma ISO/IEC 27001:2005.

2.2 ESQUEMA DOCUMENTAL.

2.2.1. Política de Seguridad.

Incluida en el anexo “A” de este documento.

2.2.2. Procedimientos de Auditorías Internas.

Incluida en el anexo “B” de este documento.

2.2.3 Gestión de Indicadores.

Todo proceso de implementación del Sistema de Gestión de Seguridad de la Información involucra realizar un seguimiento para evaluar el grado de cumplimiento, por esta razón es necesario establecer algunos indicadores para cuantificar el avance de las actividades para alcanzar los objetivos planteados.

Este trabajo propone un conjunto de indicadores que a continuación se describe.

CONTROL DE SEGURIDAD	INDICADOR	META	FRECUENCIA
Documento de la Política de Seguridad de la información	Núm. revisión de la política de seguridad por parte de la dirección	100%	Anual
Acuerdos de confidencialidad	Num. de acuerdos de confidencialidad	100%	Trimestral
Activos críticos	Num. de activos		

identificados	críticos identificados	100%	Mensual
Investigaciones de antecedentes	Num. de investigaciones de antecedentes	100%	Trimestral - Anual
Mantenimiento de los equipos	Num. de mantenimiento de equipos	100%	Mensual
Controles contra software malicioso	Num. De controles de Software malicioso	100%	Mensual
Gestión de privilegios	Num. De permisos otorgados a los usuarios.	100%	Mensual
Fuga de Información	Num. De incidentes de seguridad.	100%	Mensual
Recopilación de evidencias	Num. De revisiones de evidencias	100%	Mensual
Realizar auditorías y controles	Numero de auditorías realizadas	100%	Trimestral

.

2.2.4 Procedimiento Revisión por Dirección.

La revisión por la dirección es el auténtico feedback del sistema de gestión de seguridad de la información para lograr la mejora continua, es imprescindible que la Dirección proporcione los medios para poder llevar a cabo cualquier cambio en la cultura de seguridad, por esta razón el apoyo de la Dirección es fundamental para la toma de decisiones en temas relacionados en seguridad de la información y además realizar un seguimiento de todos los procedimientos y controles que deban hacerse para garantizar el buen funcionamiento de los Sistemas de Gestión de la Seguridad de la Información SGSI.

A continuación se describe las entradas de la revisión por la dirección

- Resultados de auditorías y revisiones del SGSI.
- Retroalimentación de las partes interesadas.
- Técnicas, productos o procedimientos, para mejorar el desempeño y efectividad del SGSI.
- Estados de acciones preventivas y correctivas.

- Vulnerabilidades o amenazas no tratadas adecuadamente en la evaluación de riesgo previa.
- Resultados de mediciones realizadas.
- Acciones de seguimiento de las revisiones gerenciales previas.
- Cualquier cambio que pudiera afectar el SGSI.
- Recomendaciones para la mejora.

Salidas de la revisión por la dirección el cual debe incluir.

- Mejoramiento de la eficacia del SGSI.
- Actualización de la evaluación del riesgo y el plan de tratamiento del riesgo.
- Modificación de procedimientos y controles que afectan la seguridad de la información, para responder a eventos internos o externos que pudieran tener impacto sobre el SGSI. incluyendo cambios en:

    1) Requerimientos comerciales.
    2) Requerimientos de seguridad.
    3)Procesos comerciales que afectan los requerimientos comerciales existentes.
    4) Requerimientos reguladores o legales.
    5) Obligaciones contractuales.
    6) Niveles de riesgo y/o criterio de aceptación del riesgo

- Necesidades de recursos.
- Mejoramiento de la medición de efectividad de los controles.

La dirección realizara controles con un periodo inferior, a un año controles para verificar el cumplimiento de todos los estándares, normas y procedimientos establecidos en el SGSI. Además si se han detectado incidencias es necesario realizar una revisión del documento para ajustarlo a las necesidades actuales de la entidad.

2.2.5 Gestión de Roles y Responsabilidades.

El Sistema de Gestión de Seguridad de la Información debe tener un equipo conformado para que se responsabilice todo lo referente al SGSI. Este equipo de trabajo se encuentra en el organigrama de la entidad conformado por el grupo de Seguridad de la Información donde se encuentra un comité de seguridad.

2.2.5.1 Comité de Seguridad:

- Revisar y aprobar las normas de seguridad de la información y las responsabilidades generales de seguridad definidas para los

empleados, contratistas y demás personas que interactúen con los recursos informáticos y de telecomunicaciones del ente o que tengan acceso a su información.

- Especificar los objetivos, estrategias y planeación de la seguridad de la información del ente.
- Avalar y aprobar la ejecución de proyectos de seguridad de información
- Evaluar planes de acción para mitigar y/o eliminar riesgos.
- Realizar revisiones del SGSI basándose en esta revisión la dirección debe tomar decisiones y acciones relativas a la mejora de la eficiencia del SGSI, actualización de la evaluación de riesgos y del plan de tratamiento de riesgos, modificación de los procedimientos y controles que afectan la seguridad de la información en respuestas a cambios internos o externos, requerimientos de seguridad, niveles de riesgo y criterios de aceptación del riesgo.

Las personas que harán parte de este comité serán las siguientes:

- Representantes de la Dirección.
- Responsable de Seguridad de la Informática.
- Responsable de infraestructura, sistemas y comunicaciones.
- Responsable del Área de Recursos Humanos
- Responsable Jurídico.
- Responsable Auditoria

2.2.5.2 Responsabilidades.

- **Representantes de la Dirección**: la Dirección es responsable que los empleados a su cargo, conozcan y apliquen las políticas de seguridad.
- **Responsable de seguridad Informática**: Sera responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la Entidad.
- **Responsable de infraestructura, sistemas y comunicaciones**: cumplirá funciones relativas a la seguridad de los sistemas de información lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la Política de Seguridad de la Información.
- **Responsable del Área de Recursos Humanos**: Notificara a todo el personal que ingrese a la entidad de sus obligaciones respecto del cumplimiento de la política de Seguridad y de todas aquellas normas, procedimientos y prácticas que de ella surjan.
- **Responsable Jurídico**: Verificara el cumplimiento de la Política de seguridad, en la gestión de todos los contratos, acuerdos o cualquier otro documentación de la entidad para con sus funcionarios o terceros,

Así mismo asesorara en materia legal e lo que se refiere a la seguridad de la información.

- **Responsable Auditoria**: practicar auditorías periódicas sobre los sistemas de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por la Política y por las normas, procedimientos y prácticas que de ella surjan

2.2.6 Metodología de Análisis de Riesgos.

El análisis de riesgos es una tarea que cualquier organización debe realizar antes de cualquier implementación basada en la seguridad de la información por esta razón el análisis de riesgo a desarrollar está definido bajo la metodología MAGERIT que es de carácter público, perteneciente al Ministerio de Administraciones Públicas y fue elaborado por el Consejo Superior de Administración Publica. Trata de una metodología para conocer el riesgo al que está sometido una información y como de seguro o inseguro se encuentra.

A continuación se describe las etapas del proceso que sigue MAGERIT y consta de tres etapas.

1. **PLANIFICACIÓN:** En esta etapa se establecen las consideraciones necesarias para dar inicio al proyecto.

2. **ANÁLISIS DE RIESGO:** Permite determinar cómo es, cuanto vale y como de protegidos se encuentras los activos. En esta etapa se constituye en el núcleo central de MAGERIT y su correcta aplicación condiciona la validez y utilidad de todo el proyecto.

Los Objetivos del Análisis de Riesgo son:

- Identificar los activos relevantes que poseen la organización.
- Identificar las amenazas a las que están expuestos dichos activos.
- Determinar si existen salvaguardas para los activos.
- Estimar el impacto si una amenaza llegara a materializarse.

Los elementos de Análisis de Riesgos:

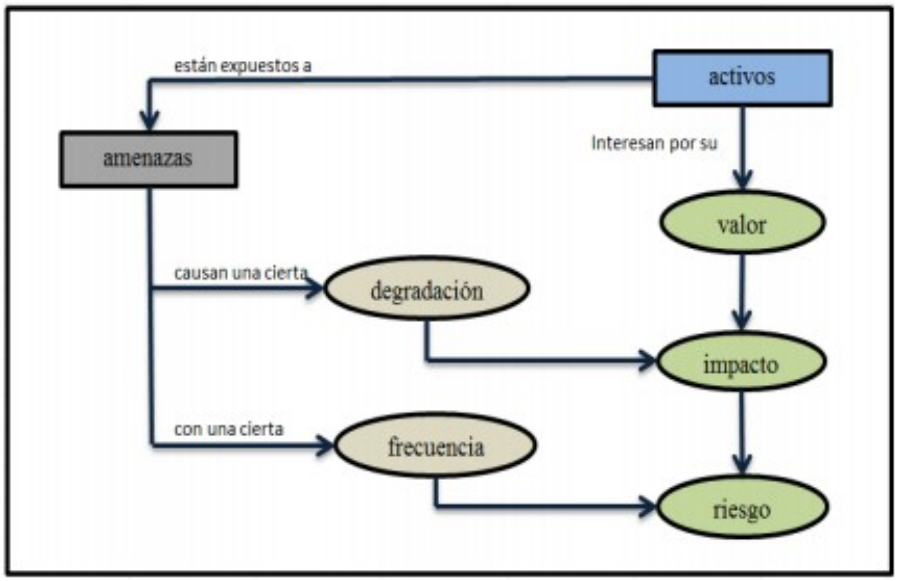
1. Caracterización de Activos: Esta actividad es reconocer los activos que componen los procesos necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección. En este grupo encontramos la identificación de los activos y la valoración de los activos

2. Caracterización de las Amenazas: Son los eventos que les pueden pasar a los activos desencadenando un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos, estas pueden ser por accidentes, errores, amenazas intencionales presenciales o remotas. En este grupo encontramos la identificación de las amenazas y la valoración de las amenazas

3. Caracterización de la Salvaguardas son mecanismos de defensa utilizados para que aquellas amenazas no causen tanto daño.

4. Análisis de riesgo residual una vez finalizada la aplicación de salvaguarda se deberá calcular el riesgo incluyendo la reducción resultante después de la aplicación de las salvaguardas.

La siguiente figura describe todo el proceso de análisis de riesgo.



Los parámetros que se utilizaran durante el análisis de riesgos serán los siguientes.

- Valor de los activos: se asignara un valor al objeto analizado.

Valoración	Abreviatura	Valor
Muy alta	MA	10
Alta	A	7-9
Media	M	4-6
baja	B	1-3
Despreciable	D	0

- Frecuencia o probabilidad de ocurrencia y se encuentra definida estimaciones anuales.

Descripción	Frecuencia	Valor
Muy frecuente	A diario	100
Frecuente	Mensualmente	10
Normal	Una vez al año	1
Poco frecuente	Cada varios años	1/10
Muy infrecuente	Cada varios años	1/100

Impacto: es el tanto por ciento del activo que se pierde en caso de que un impacto suceda sobre el.

Impacto	Rango
Muy Alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy Bajo	5%

Dimensiones de seguridad

A	Autenticidad
C	Confidencialidad
I	Integridad
D	Disponibilidad
T	trazabilidad

3. GESTIÓN DE RIESGO: Permite la selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

A continuación se explica con un ejemplo las fases que hacen parte de la metodología Magerit.

1. Fase Planificación:
   En esta fase es lograr sensibilizar a la Dirección de la Entidad de la necesidad de elaborar un proyecto relacionado con la seguridad de la información, se determina los participantes del proyecto y se elabora el calendario de la realización de las distintas etapas que corresponden al proyecto para finalmente hacer el lanzamiento del proyecto.

2. Fase Análisis de Riesgo.

- Identificación de los Activos que componen el dominio para el ejemplo se tomara el Gestor de BBDD
- Valoración de los activos

Ámbito	Activo	Valor	Aspectos Críticos				
			A	C	I	D	T
Aplicacion	Gestor BBDD	Alta	7	8	9	9	9

- Caracterización de las amenazas se identifican las amenazas sobre cada activo y se valora la amenaza estimando la frecuencia de ocurrencia de cada amenaza sobre cada activo

ACTIVO	FRECUENCIA	[A]	[C]	[I]	[D]	[T]
Gestor BD Oracle		100%	100%	100%	100%	100%
[I.5] Avería de origen Físico o Lógico	1				50%	30%
[E.1] Errores de los usuarios	100			10%	1%	
[E.2]Errores del administrador	2	50%	10%	20%	20%	50%
[E.3] Errores de Monitorización (log)	1					60%
[E.4] Errores de Configuración	1	50%	10%	10%	50%	60%
[E.8] Difusión de Software dañino	100	70%	10%	10%	10%	10%
[E.9] Errores de (re) encaminamiento	0.1	30%	10%	1%		30%
[E.14] Escapes de Información	1		30%			
[E.20] Vulnerabilidades de los Programas	1		20%	20%	10%	
[E.21] Errores de mantenimiento / actualización de programas	10		10%	10%	10%	
[A4]Manipulación de la configuración	1	30%	50%	50%	50%	50%
[A5]Suplantación de la identidad del usuario	10	80%	100%	100%		
[A6]Abuso de privilegios de acceso	2		50%	10%		
[A8]Difusión de Software dañino	100	80%	100%	100%	100%	80%
[A9] (Re) encaminamiento de mensajes	1	50%	100%	10%		70%
[A11] Acceso no autorizado	1	60%	50%	20%		
[A14]Interceptación de información	0.1		100%			

- Impacto Potencial: se valoriza el impacto sobre los activos

ACTIVO	FRECUENCIA	Valor USD	[A]	[C]	[I]	[D]	[T]	Frecuencia*Impacto*Valor

SERVIDOR DE APLICACIONES			USD 90.000,00	100%	100%	50%	100%	100%	
	[N2]Daños por Agua	0,1					100%	20%	USD 30.000,00
	[N*]Desastres Naturales	0,1					100%	70%	USD 30.000,00
	[I5] Avería de origen físico o lógico	1					50%	50%	USD 150.000,00
	[I.6]Corte del suministro Eléctrico	1					100%	20%	USD 300.000,00
	[I7 Condiciones Inadecuadas de Temperatura y/o humedad	10					100%	60%	USD 3.000.000,00
	[I.11] Emanaciones electromagnéticas	1			1%				USD 3.000,00
	[E2]Errores de del Administrador	10		50%	70%	20%	50%	30%	USD 1.500.000,00
	[E4]Errores de Configuración	2		50%	10%	10%	50%	40%	USD 300.000,00
	[E23] Errores de mantenimiento / Actualización de equipos	1					10%		USD 30.000,00
	[A4]Manipulación de la Configuración	1		60%	50%	50%	50%	50%	USD 150.000,00
	[A6]Abuso de privilegios de acceso	2			50%	10%			USD 60.000,00
	[A7] Uso no previsto	1					10%		USD 30.000,00
	[A11]Acceso no autorizado	1		50%	50%	10%	20%		USD 60.000,00
	[A14]Intercepta ción de Información (escucha)	0,1			50%				USD 15.000,00
	[A24] Denegación del servicio	10					100%		USD 3.000.000,00
	[A25] Robo	1			10%		100%		USD 300.000,00

- Riesgo residual

ACTIVO		FRECUENCIA	Valor USD	[A]	[C]	[I]	[D]	[T]	Frecuencia*Impacto*Valor	Salvaguarda	Descripcion de Salvaguarda	Reduccion del riesgo	Nuevo Valor
SERVIDOR DE APLICACIONES			USD 90.000,00	100%	100%	50%	100%	100%					
	[N2]Daños por Agua	0,1					100%	20%	USD 30.000,00	NO			
	[N*]Desastres Naturales	0,1					100%	70%	USD 30.000,00	NO			
	[I5] Avería de origen físico o lógico	1					50%	50%	USD 150.000,00	NO			
	[I.6]Corte del suministro Eléctrico	1					100%	20%	USD 300.000,00	NO			
	[I7 Condiciones Inadecuadas de Temperatura y/o humedad	10					100%	60%	USD 3.000.000,00	SI	Sistema de refrigeracion	70%	USD 900.000,00
	[I.11] Emanaciones electromagnéticas	1			1%				USD 3.000,00	NO			
	[E2]Errores de del Administrador	10		50%	70%	20%	50%	30%	USD 1.500.000,00	SI	Sistema d emonitoreo y alertas	70%	USD 450.000,00
	[E4]Errores de Configuración	1		50%	10%	10%	50%	40%	USD 150.000,00	NO			

	[E23] Errores de mantenimiento / Actualización de equipos	1					10%		USD 30.000,00	NO			
	[A4]Manipulación de la Configuración	1		60%	50%	50%	50%	50%	USD 150.000,00	NO			
	[A6]Abuso de privilegios de acceso	1			50%	10%			USD 30.000,00	NO			
	[A7] Uso no previsto	1					10%		USD 30.000,00	NO			
	[A11]Acceso no autorizado	1		50%	50%	10%	20%		USD 60.000,00	NO			
	[A14]Interceptación de Información (escucha)	0,1			50%				USD 15.000,00	NO			
	[A24] Denegación del servicio	10					100%		USD 3.000.000,00	SI	Sistema de monitoreo y alertas	70%	USD 900.000,00
	[A25] Robo	1			10%		100%		USD 300.000,00	NO			

2.2.7 Declaración de Aplicabilidad.

Incluida en el anexo “C” de este documento.

2.3 RESULTADOS

Con el esquema documental, tendremos establecidas las bases de nuestro Sistema de Gestión de Seguridad de la Información, ya que sobre estos documentos y/o políticas/procedimientos se llevarán a cabo las diferentes actividades de implantación.

3. ANALISIS DE RIESGOS

3.1 INTRODUCCIÓN

En esta fase es la más importante del proceso de seguridad de la información, en el siguiente capítulo se desarrollara el análisis de riesgos y su gestión donde se incluye las actividades relacionadas como inventario de activos, valoración de activos, y dimensiones de seguridad.

3.2 INVENTARIO DE ACTIVOS

Nuestro primer punto para dar inicio a esta fase es la de analizar los activos vinculados a la información. Para poder llevar a cabo la metodología podemos agrupar los activos acordes con la metodología MAGERIT que se encuentra en el libro 2 Catalogo de Elementos, que lo clasifica de la siguiente manera:

- Instalaciones: Identifica los lugares físicos donde se hospedan los sistemas de información y comunicaciones.
- Hardware: Son bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
- Aplicación: Que permiten manejar datos.
- Datos: Constituye el elemento fundamental como lo es la información.
- Red: Son los medios de transporte que llevan datos de un sitio a otro
- Servicios: Satisfacen las necesidades institucionales.
- Equipamiento Auxiliar: son los medios utilizados con el fin de dar cumplimiento a las funciones.
- Personal: Identifica las personas relacionadas con los sistemas de información

Ámbito	Activo
INSTALACIONES	CPD
	Área Operaciones
	Área administrativa
	Área Logística y Abastecimiento
	Otras Áreas
HARDWARE	Servidor web
	Servidor de Dominio
	Servidor Firewall
	Servidor BBDD
	Servidor de aplicaciones
	Servidor de Correo
	Servidor Antivirus
	Servidor SAP
	Pc usuarios
	Tabletas
	Equipo Biométrico
	impresoras
	Fotocopiadoras
APLICACIÓN	S.O. Server 2008

	S. O. Linux
	Gestor BD Oracle
	Servidor de Correo (Zimbra)
	Cód. fuente aplicaciones
	Software (Info Logística y Abastecimiento)
	Software personal (Info Talento humano)
	Software Operacional (info Operaciones)
	Aplicación Biométrica
	Licencias S.O
	Licencias de Aplicación
	Licencia Ofimática
	Licencia SAP
	Antivirus Kaspersky
DATOS	Información Personal
	Información Logística
	Información operacional
	Backup Información
RED	LAN
	Router
	Líneas Telefonía
	Central Telefónica
	Switch
	Internet
SERVICIOS	Servicios Correo Electrónico
	Portal de Información (pág. web)
	Seguridad Ciudadana
	Videoconferencia
EQUIPAMIENTO AUXILIAR	Suministro Eléctrico
	SAI
	Climatización
	Cableado Estructurado
	Cámara de Vigilancia
	AACC industriales
	Destructora de Información
PERSONAL	Administrativos
	Empleados
	Personal subcontratado
	Administrador Sistemas
	Proveedores

Análisis de Activos

3.2.1 Dimensiones de Seguridad y Valoración de los activos.

Una vez se haya determinado el inventario de activos es importante la valoración de los activos en función de la valoración ACIDT, que permitirá en fases posteriores escoger salvaguardas teniendo en cuenta y dando prioridad a los aspectos críticos de la entidad.

Las dimensiones de seguridad según la valoración ACIDT se utilizan para valorar las consecuencias de la materialización de un amenaza y son: confidencialidad, integridad y disponibilidad, también se puede añadir la autenticidad y la trazabilidad. Para cada dimensión en un activo se le asociara una valoración según la escala que va de 0 a 10 d definidos en la versión 3 de Magerit.

Dimensiones de Seguridad		
A	Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
C	Confidencialidad	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
I	Integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
D	Disponibilidad	Propiedad o Características de los activos consistentes en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
T	Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Valoración de los Activos		
Va	Valor	Criterio
MA- Muy Alta	10	Daño muy grave a la organización
A - Alta	7-9	Daño grave a la organización
M- Medio	4-6	Daño importante a la organización
B- Bajo	1-3	Daño menor a la organización
D- Deficiente	0	Irrelevante para la organización

La siguiente tabla describe los activos de la entidad con sus respectivas dimensiones de seguridad, lo que permite identificar el valor de cada activo para la entidad y la importancia del activo en relación a las dimensiones de seguridad.

Ámbito	**Activo**	**Valor**	**Aspectos Críticos**				
			A	**C**	**I**	**D**	**T**
INSTALACIONES	CPD	Alta	7	8	9	9	9
	Área Operaciones	Medio	3	5	6	6	3
	Área administrativa	Medio	3	9	6	3	3
	Área Logística y Abastecimiento	Alta	6	7	6	6	6
	Área comercial	Medio	3	6	6	3	3
	Otras Áreas	Bajo	2	3	3	3	3
HARDWARE	Servidor web	Alta	8	9	8	9	8
	Servidor de Dominio	Alta	7	9	7	8	7
	Servidor Firewall	alta	7	9	9	9	8
	Servidor BBDD	alta	8	8	8	9	8
	Servidor de aplicaciones	Alta	9	9	8	9	8
	Servidor de Correo	Alta	9	9	8	8	8
	Servidor Antivirus	Media	7	7	5	7	6
	Servidor SAP	alto	9	8	7	9	8
	Pc usuarios	Medio	6	6	5	3	3
	tabletas	Medio	6	6	5	3	3
	Equipo Biométrico	Alto	8	7	7	8	8
	impresoras	Bajo	3	3	3	3	3
	Fotocopiadoras	Bajo	3	3	3	3	3
APLICACIÓN	S.O. Server 2008	Medio	6	8	6	6	6
	S. O. Linux	Medio	5	8	6	6	6
	Gestor BD Oracle	Alto	9	10	10	7	8
	Servidor de Correo (Zimbra)	Alta	8	8	8	6	8
	Cód. fuente aplicaciones	Medio	9	7	7	3	8
	Software (Info Logística y Abastecimiento)	Alta	9	8	8	8	8

	Software personal (Info Talento humano)	Alta	9	9	8	8	8
	Software Operacional (info Operaciones)	Alta	8	7	8	8	8
	Aplicación Biométrica	Medio	8	6	8	6	6
	Licencias S.O	Bajo	2	3	1	1	1
	Licencias de Aplicación	Bajo	2	3	1	1	1
	Licencia Ofimática	Bajo	2	3	1	1	1
	Licencia SAP	Medio	5	4	2	3	2
	Antivirus Kaspersky	Medio	3	6	2	6	3
DATOS	Información Personal	Alta	8	8	8	8	8
	Información Logística	Alta	8	9	8	8	8
	Información operacional	Alta	8	9	7	9	7
	Backup Información	Alta	9	9	9	9	8
RED	LAN	Alta	7	8	7	8	6
	Router	Alta	8	8	7	9	7
	Líneas Telefonía	Medio	7	9	6	6	6
	Central Telefónica	Alta	7	9	7	9	6
	Switch	alta	7	9	7	8	6
	Internet	alta	8	6	7	8	6
SERVICIOS	Servicios Correo Electrónico	Medio	8	8	6	4	7
	Portal de Información (pág. web)	Medio	5	3	7	8	5
	Seguridad Ciudadana	alta	7	8	7	8	7
	Videoconferencia						
EQUIPAMIENTO AUXILIAR	Suministro Eléctrico	Medio	5	0	2	9	5
	SAI	Medio	5	1	3	8	5
	Climatización	Medio	6	1	3	8	5
	Cableado Estructurado	Medio	6	1	6	8	6
	Cámara de Vigilancia	Medio	5	6	6	6	5
	AACC Industriales	Medio	4	3	5	3	3
	Destructora de Información	Medio	5	6	5	6	5
PERSONAL	Administrativos	Alto	7	8	7	7	7
	Empleados	Alto	7	8	7	8	8
	Personal subcontratado	Alto	7	9	7	8	7
	Administrador Sistemas	Alto	8	8	8	8	8
	Proveedores	Alto	7	8	7	8	7

3.3 ANÁLISIS DE AMENAZAS

Una vez realizada la tabla anterior se debe analizar la exposición de estos activos a amenazas y como pueden afectar a estos. Las amenazas son eventos inesperados que pueden causar daños a los sistemas de información para la clasificación de las amenazas se ha utilizado Magerit el cual en su libro 2 Catalogo de Elementos presenta un catálogo de amenazas posible sobre los activos de un sistema de información A continuación se exponen las amenazas a las que está expuesta la entidad, la información recopilada da lugar a una tabla resumen para cada tipo de activo se analizará la frecuencia con que puede producirse la amenaza se modela como una tasa anual de correspondencia, así como su impacto en las distintas dimensiones de la seguridad del activo.

Descripción	Frecuencia	Valor
Muy frecuente	A diario	100
Frecuente	Mensualmente	10
Normal	Una vez al año	1
Poco frecuente	Cada varios años	0,1
Muy infrecuente	Cada varios años	0.01

Tabla de Frecuencia

Descripción del Impacto	Valor
Muy alto	100%
alto	75%
Medio	50%
Bajo	20%

Muy Bajo	5%

Tabla de Impacto

Para este análisis se tomó cada activo del inventario de activos frente las posibles amenazas que pueden llegar a afectar y se determinó la frecuencia en dicha amenaza se pueda materializar en el activo

ACTIVO	FRECUENCIA	[A]	[C]	[I]	[D]	[T]
INSTALACIONES						
CPD		100%	100%	100%	100%	100%
[N1] Fuego	0,1				100%	100%
[N2] Daños por agua	O,1				50%	100%
[N*] Desastres Naturales	0,1				100%	100%
[I1] Fuego	O,1				100%	100%
[I2] Daños por agua	O,1				50%	50%
[A7] Uso no previsto	1				50%	
[A11] Acceso no autorizado	10	100%	100%	70%		
ÁREA OPERACIONES		50%	50%	50%	100%	50%
[N1] Fuego	O,1				100%	50%
[N2] Daños por agua	0,1				50%	50%
[N*] Desastres Naturales	0.1				100%	50%
[I1] Fuego	0,1				50%	50%
[I2] Daños por agua	0,1				50%	50%
[A7] Uso no previsto	1				50%	
[A11] Acceso no autorizado	10	100%	30%	30%		
ÁREA ADMINISTRATIVA		50%	50%	50%	100%	50%
[N1] Fuego	O,1				100%	50%
[N2] Daños por agua	0,1				50%	50%
[N*] Desastres Naturales	0.1				100%	50%
[I1] Fuego	0,1				50%	50%
[I2] Daños por agua	0,1				50%	50%
[A7] Uso no previsto	1				50%	
[A11] Acceso no autorizado	10	100%	70%	100%		
ÁREA LOGISTICAY ABASTECIMIENTO		50%	50%	50%	100%	50%
[N1] Fuego	O,1				100%	50%
[N2] Daños por agua	0,1				50%	50%
[N*] Desastres Naturales	0.1				100%	50%
[I1] Fuego	0,1				50%	50%
[I2] Daños por agua	0,1				50%	50%
[A7] Uso no previsto	1				50%	
[A11] Acceso no autorizado	10	100%	70%	100%		
OTRAS ÁREAS		50%	50%	50%	50%	50%
[N1] Fuego	O,1				50%	50%
[N2] Daños por agua	0,1				50%	50%
[N*] Desastres Naturales	0.1				50%	50%
[I1] Fuego	0,1				50%	50%
[I2] Daños por agua	0,1				50%	50%
[A7] Uso no previsto	1				50%	
[A11] Acceso no autorizado	10	100%	10%	10%		

Debido a la cantidad de datos que genera el análisis se puede ver el análisis completo en el Anexo D- ANÁLISIS DE AMENAZAS

3.4 IMPACTO POTENCIAL

Una vez realizada la tabla anterior, y dado que conocemos los valores de los diferentes activos, podemos determinar el impacto potencial de la materialización de las amenazas, que representen riesgos para el cumplimiento de los objetivos institucionales. Para calcular el impacto potencial se realiza a través del siguiente calculo Frecuencia*Impacto*Valor.

Frecuencia= Frecuencia o probabilidad de ocurrencia de los eventos.
Impacto= Consecuencia que puede producir la materialización de dicha amenaza.
Valor= Valor asignado al activo por parte de la entidad en su importancia no es el valor comercial.

Para la determinación del nivel aceptable del riesgo la entidad estableció que todo lo que esté por debajo de USD$1.200.000 será asumido como aceptable, pero o que esté por encima de este valor serán seleccionada para el diseño e implementación de salvaguardas. El valor resaltado en rojo representa el mayor valor de riesgo.

ACTIVO		FRECUENCIA	Valor USD	[A]	[C]	[I]	[D]	[T]	Frecuencia*Impacto*Valor
INSTALACIONES									
CPD			USD 300.000,00	100%	100%	100%	100%	100%	
	[N1] Fuego	0,1					100%	100%	USD 30.000,00
	[N2] Daños por agua	0,1					50%	100%	USD 15.000,00
	[N*] Desastres Naturales	0,1					100%	100%	USD 30.000,00
	[I1] Fuego	0,1					100%	100%	USD 30.000,00
	[I2] Daños por agua	0,1					50%	50%	USD 15.000,00
	[A7] Uso no previsto	1					50%		USD 150.000,00
	[A11] Acceso no autorizado	10		100%	100%	70%			USD 2.100.000,00

Debido a la cantidad de datos que genera el análisis se puede ver el análisis completo en el Anexo E- IMPACTO POTENCIAL.

3.5 RIESGO RESIDUAL

De acuerdo a los objetivos trazados por la dirección de la institución, se define que aquellos activos que superan el margen establecido por la entidad, se deberán establecer una serie de salvaguardas que ayuden a mitigar el riesgo. Luego se vuelve a cuantificar el riesgo para determinar si queda por debajo del margen establecido lo que quiere decir que el control disminuye el riesgo.

ACTIVO		FRECUENCIA	Valor USD	[A]	[C]	[I]	[D]	[T]	Frecuencia*Impacto*Valor	Salvaguarda	Descripcion de Salvaguarda	Reduccion del riesgo	Nuevo Valor
INSTALACIONES													
CPD			USD 300.000,00	100%	100%	100%	100%	100%					
	[N1] Fuego	0,1					100%	100%	USD 30.000,00	NO			
	[N2] Daños por agua	0,1					50%	100%	USD 15.000,00	NO			
	[N*] Desastres Naturales	0,1					100%	100%	USD 30.000,00	NO			
	[I1] Fuego	0,1					100%	100%	USD 30.000,00	NO			
	[I2] Daños por agua	0,1					50%	50%	USD 15.000,00	NO			
	[A7] Uso no previsto	1					50%		USD 150.000,00	NO			
	[A11] Acceso no autorizado	10		100%	100%	70%			USD 2.100.000,00	SI	Video vigilancia, Equipos Biometricos	70%	USD 630.000,00

Debido a la cantidad de datos que genera el análisis se puede ver el análisis completo en el Anexo F- RIESGO RESIDUAL.

3.6 RESULTADOS

Mediante el análisis de amenazas observamos que las que genera más impacto en nuestros activos son aquellas de origen humano, lo que implica tomar las medidas pertinentes del caso con el fin de mitigar el riesgo.

4. PROPUESTAS DE PROYECTOS

4.1 INTRODUCCIÓN

Llegados a este punto, conocemos el nivel de riesgo actual en la entidad, por lo que es el momento de plantear proyectos que mejoren el estado de la seguridad. Los tres proyectos planteados se encuentran enmarcados en el plazo de corto- mediano y largo plazo

4.2 PROPUESTAS PROYECTOS

4.2.1 **Protección contra Software Malicioso.**

4.2.1.1 Objetivos del Proyecto

Proteger integridad de la información y de software con el fin de evitar ataques destructivos de la información.

4.2.1.2 Alcance

Este proyecto abarca, instalaciones, aplicativos, datos, servicios como es:

- Servidor Web
- Controlador de Dominio.
- Firewall
- BBDD
- Aplicaciones (Logística, Operación, Talento Humano.
- Correo Electrónico Zimbra
- Antivirus Karspesky
- CPD

4.2.1.3 Salvaguardas Técnicas.

Herramientas de antivirus, seguridad perimetral y sistemas de detección de intrusos con los sistemas de alertas y monitoreo

4.2.1.4 Descripción

Este proyecto busca establecer controles que reduzcan la probabilidad de ocurrencia, reduciendo el riesgo de la negación del servicio mediante una adecuada gestión de la red. Para la realización de este proyecto será apoyado por el personal de Telemática conformado por ARADI (*Área de Administración de la*

Información), GUSIN (*Grupo Seguridad de la Información*), GRUIM (*Grupo de Implementación Tecnológica*), GRUDE (*Grupo Proyección y Desarrollo de Tecnología*) y por Ultimo Personal de la Empresa Contratista.

4.2.1.5 Implicaciones en la Entidad.

Protección en tiempo real de la infraestructura contra software malicioso, y actuación inmediata ante las amenazas.

4.2.1.6 Impacto Estratégico

Reputación de la Entidad.
Protección de los datos confidenciales

4.2.1.7 Tiempo Estimado

El tiempo estimado para este proyecto es de 5 meses, teniendo en cuenta que la implementación se hará de manera simultánea en las otras sedes del territorio nacional

Fase	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5
Evaluación estado Actual					
Fase Precontractual - Contractual(Acuerdo con Terceros					
Ejecución Trabajos (Instalación-Configuración-capacitación)					
Puesta en Marcha					
Informe Implementación					

4.2.1.8 Costos

La fuente de financiación para la ejecución del proyecto se hará con recursos asignado acuerdo a vigencia presupuestal el costo total del proyecto es de USD $45.000, valor que incluye el IVA para un tiempo de ejecución de 5 meses para la presente vigencia.

4.2.2 **Mejora en los Controles Seguridad Lógica y Físico**

4.2.2.1Objetivos del Proyecto.

Optimizar a través de mejores prácticas la reducción de errores no intencionados, asegurando la continuidad del negocio.

4.2.2.2 Alcance

Este proyecto cobija Instalaciones, Hardware, Aplicativos, Datos y Servicios como es:

- CPD
- Área de Operaciones
- Servidor Web
- Servidor de Dominio
- Servidor Firewall
- Servidor BBDD
- Servidor de Aplicaciones
- Servidor de Correo
- Servidor Antivirus
- Pc
- Equipo Biométrico
- SW Info Logística
- SW talento Humano
- SW Operaciones
- Aplicación Biométrica

4.2.2.3 Salvaguardas Técnica.

Dispositivos físicos para el control de acceso como son los equipos biométricos y la video vigilancia, procedimientos de acceso con registro de bitácora para el ingreso controlado a las salas de crisis. Para el control de accesos lógicos se instalaran un IDS, Sistema de Detección de Intrusos, se establecen procedimientos de cambios de contraseñas, se establecen herramientas dedicadas a este servicio, se implementaran una solución de NAC para evitar los intentos de escucha o Sniffing de información en la red y las conexiones no autorizadas.

4.2.2.4 Descripción.

Este proyecto busca fortalecer los controles de seguridad tanto lógico y física, que pueden afectar los activos en la Entidad frente a errores no intencionados del personal. Para la realización de este proyecto será apoyado por el personal de Telemática conformado por ARADI (*Área de Administración de la Información*), GUSIN (*Grupo Seguridad de la Información*), GRUIM (*Grupo de Implementación Tecnológica*), GRUDE (*Grupo Proyección y Desarrollo de Tecnología*) y por Ultimo Personal de la Empresa Contratista.

4.2.2.5 Implicaciones en la Entidad.

Se fortalecerá la seguridad física y lógica de la entidad de manera que se incremente la confianza y ayude a contribuir a una cultura de prevención.

4.2.2.6 Impacto.

Aumento de la Satisfacción tanto personal interno como externo.
Se minimiza el riesgo.

4.2.2.7 Tiempo Estimado.

El tiempo estimado es de 7 meses teniendo en cuenta que la implementación se hará de manera simultánea en las otras sedes del territorio nacional.

Fase	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7
Evaluación estado Actual							
Fase Precontractual - Contractual(Acuerdo con Terceros							
Ejecución Trabajos (Instalación-Configuración-capacitación)							
Puesta en Marcha							
Informe Implementación							

4.2.2.8 Costos.

La fuente de financiación para la ejecución del proyecto se hará con recursos asignado acuerdo a vigencia presupuestal el costo total del proyecto es de USD $100.000, valor que incluye el IVA para un tiempo de ejecución de 7 meses para la presente vigencia.

4.2.3 **Continuidad y Recuperación del Negocio**

4.2.3.1 Objetivos del Proyecto

Establecer un plan de continuidad y recuperación del negocio ante posibles incidencias.

4.2.3.2 Alcance

Este proyecto cobija Instalaciones, Hardware, Aplicativos, Datos y Servicios como es:

- CPD
- Servidores de Dominio, BBDD, aplicaciones etc..
- Backup de las aplicaciones.

- Servicios de red, redundantes para atender las conexiones provenientes de los enlaces principales.

4.2.3.3 Salvaguarda Técnica y física.

Protección integral de los sistemas de información con la implementación de controles y los sistemas de refrigeración, disponibilidad de copias de seguridad, conectividad con los sistemas de respaldos, para asegurar la conectividad desde el exterior en caso de caída de los sistemas

4.2.3.4 Descripción

Este proyecto busca desarrollar procedimientos regulares para mantener respaldos continuos de los procesos críticos de la Entidad. Para la realización de este proyecto será apoyado por el personal de Telemática conformado por ARADI (*Área de Administración de la Información*), GUSIN (*Grupo Seguridad de la Información*), GRUIM (*Grupo de Implementación Tecnológica*), GRUDE (*Grupo Proyección y Desarrollo de Tecnología*) y por Ultimo Personal de la Empresa Contratista.

4.2.3.5 Implicaciones en la Entidad.

Proteger la continuidad de la Entidad en caso de incidentes.

4.2.3.6 Impacto Estratégico

Aumento de la confianza de la Entidad por conocimientos de los procedimientos a realizar en caso de incidencias.

4.2.3.7 Tiempo Estimado

El tiempo estimado es de 12 meses teniendo en cuenta que la implementación se hará de manera simultánea en las otras sedes del territorio nacional.

Fase	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12
Evaluación estado Actual												
Fase Precontractual - Contractual(Acuerdo con Terceros												
Ejecución Trabajos												
Documentación												
Puesta en Marcha												
Informe Implementación												

4.2.3.8 Costos

La fuente de financiación para la ejecución del proyecto se hará con recursos asignado acuerdo a vigencia presupuestal el costo total del proyecto es de USD $150.000, valor que incluye el IVA para un tiempo de ejecución de 12 meses para la presente vigencia.

4.3 RESULTADOS

Después de analizar la propuesta de proyectos podemos ver el nuevo panorama en el que ha influido positivamente en la Entidad en los cuales podemos ver los beneficios como:

- Una gestión adecuada de los riesgos.
- Facilita el logro de los objetivos institucionales.
- Hace que la Entidad sea más segura y consciente de sus riesgos.
- Aporta confianza a los sistemas de información.
- Reducción eficaz mediante los controles adecuados.
- Aprovechamiento de oportunidades de negocio

5 AUDITORIA DE CUMPLIMIENTO

5.1 INTRODUCCIÓN

Llegados a esta fase, es el momento de evaluar el cumplimiento de la empresa respecto a los controles definidos por la norma ISO/IEC 27001:2005 y determinar cuáles controles serán implementados y cuales no con el fin de mejorar la seguridad en la Entidad.

5.2 PLAN DE AUDITORIA.

Objetivo (s) de la Auditoría	Alcance de la Auditoria	Criterios de Auditoria y Documentos de Referencia
Verificar el grado de cumplimiento del SGSI de conformidad con la norma ISO 27001:2005	Todos los controles del ISO/IEC 27001:2005	ISO 27001:2005

Etapa	Actividad	Responsable
1	Decidir la realización de la auditoria	Representante de la Dirección
2	Definir los objetivos, alcance y criterios de auditoria	Representante de la Dirección
3	Coordinar con los responsables de las áreas involucradas la fecha y hora de ejecución de la auditoria.	Representante de la Dirección
4	Seleccionar al Equipo Auditor y nombrar el Auditor Líder	
5	Llevar a cabo la reunión de apertura y señalar el objetivo y el alcance de la auditoria.	Auditor Interno Líder
6	Llevar a cabo la auditoria	Equipo Auditor
7	Levantar los hallazgos de auditoria	Equipo Auditor
8	Elaborar informe de la auditoria	Auditor Interno Líder
9	Realizar la reunión de cierre donde se informan los resultados obtenidos de la auditoria	Auditor Interno Líder

Firmas de Aceptación y Aprobación del Plan de Auditoria:		
Puesto	Nombre	Firma
Auditor Líder:	María Martínez	
Director del área Auditado:	Pablo Jaimes	

5.3 METODOLOGÍA

La metodología utilizada para el análisis del sistema de gestión de seguridad de la información o SGSI corresponde al Modelo de Madurez de la Capacidad CMM en el que se utiliza una escala 0% al 100%, en donde el 100%corresponde a la optimización de los procesos.

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

5.4 EVALUACIÓN DE LA MADUREZ

La evaluación se ha realizado tomando como referencia el estándar internacional de la Norma UNE- ISO 27001:2007 que agrupa un total de 133 controles o salvaguardas sobre las recomendaciones de buenas prácticas para la gestión de

la seguridad de la información organizado en un total de 11 áreas y 39 objetivos de control así como los controles descriptos en la norma une ISO/IEC 27002:2005.

CONTROLES ISO 2002:2005				
	POLÍTICA DE SEGURIDAD			% Cumplimiento
5.1	Política de seguridad de la información			95%
5.1.1	Documento de política de seguridad de la información	El documento se le han hecho actualización que van acorde con los cambios tecnológicos que ha tenido la entidad.	4, GESTIONABLE Y MEDIBLE	
5.1.2	Revisión de la política de seguridad de la información	La dirección revisa y aprueba la nueva política de seguridad.	4, GESTIONABLE Y MEDIBLE	
	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN			86%
6.1	Organización interna.			82%
6.1.1	Compromiso de la Dirección con la seguridad de la información.	A nivel nacional se crearon comités de gestión de la seguridad de la información con el apoyo por parte de la dirección y asigna funciones y responsabilidades a través de directivas	4, GESTIONABLE Y MEDIBLE	
6.1.2	Coordinación de la seguridad de la información	existe un plan para las actividades desarrolladas donde son coordinadas y asignadas a los diferentes funciones que tienen el comité	4, GESTIONABLE Y MEDIBLE	
6.1.3	Asignación de responsabilidades relativas a la seg. de la información	Existen los procedimientos de asignación de responsabilidades en especial aquellos que están directamente relacionados con la seguridad.	4, GESTIONABLE Y MEDIBLE	
6.1.4	Proceso de autorización de recursos para el tratamiento de la información	existe un proceso de autorización para los nuevos recursos	4, GESTIONABLE Y MEDIBLE	
6.1.5	Acuerdos de confidencialidad	existen los acuerdos de confidencialidad, pero no son revisados de forma periódica	3, DEFINIDA	

6.1.6	Contacto con las autoridades	Existen de procedimientos ante una eventualidad en las instalaciones, sin embargo en cuanto a la seguridad de la información no se han establecidos los procedimientos necesarios.	3, DEFINIDA	
6.1.7	Contacto con grupos de especial interés	No existe relaciones con proveedores en materia de seguridad solo se hacen capacitaciones.	0, INEXISTENTE	
6.1.8	Revisión independiente de la seguridad de la información.	Se hacen revisiones dos veces al año de MECI que incluye revisión en materia de seguridad.	4, GESTIONABLE Y MEDIBLE	
6.2	Terceros			90%
6.2.1	Identificación de los riesgos derivados del acceso de terceros	Se establecen acuerdos con terceros,	3.DEFINIDA	
6.2.2	Tratamiento de la seguridad en la relación con los clientes	se establecen controles	3, DEFINIDA	
6.2.3	Tratamiento de la seguridad en contratos con terceros	Cuando se realiza un contrato por prestación de servicios se incluye unas cláusulas de seguridad, pero no se es riguroso con este tema.	3, DEFINIDA	
	GESTIÓN DE ACTIVOS			94%
7.1	Responsabilidad sobre activos			95%
7.1.1	Inventarios de activos	Se realiza inventarios de equipos y se ha establecido un control de los equipos que se han dado de baja.	4, GESTIONABLE Y MEDIBLE	
7.1.2	Propiedad de los activos	Se le asigna a un propietario, ya que los activos entran al almacén y antes de salir lleva la placa de inventarios y se le asigna a un usuario.	4, GESTIONABLE Y MEDIBLE	
7.1.3	Uso aceptable de los activos	Existe documento en el uso aceptable de recursos	4, GESTIONABLE Y MEDIBLE	
7.2	Clasificación de la información			93%
7.2.1	Directrices de clasificación	la información es clasificada de acuerdo al nivel de criticidad, pero se está seguimiento rigurosos de la directriz	3, DEFINIDA	

7.2.2	Etiquetado y manipulado de la información	existe el documento donde se clasifica la información se etiqueta el tipo de información y la manipulación que se debe tener, si la información es de carácter secreto , ultrasecreto y confidencial	4, GESTIONABLE Y MEDIBLE	
	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS			52%
8.1	Antes del empleo			95%
8.1.1	Funciones y responsabilidades	Existe un manual de funciones para todo el personal que se encuentra a nomina, pero en los casos de personal por prestación de servicios se tiene establecidos un documento donde se describan las responsabilidades respecto a la seguridad.	4, GESTIONABLE Y MEDIBLE	
8.1.2	Investigación de antecedentes	Se realiza estudios de seguridad de personas y se le pide el certificado de antecedentes antes de las contrataciones.	4, GESTIONABLE Y MEDIBLE	
8.1.3	Términos y condiciones de contratación	se firma una clausula legal,	4, GESTIONABLE Y MEDIBLE	
8.2	Durante el empleo			23%
8.2.1	Responsabilidades del cese o cambio	No existe una guía de uso aceptable de recursos.	1, INICIAL	
8.2.2	Concienciación, formación y capacitación en seg. De la información	si existe capacitaciones pero no son frecuentes	2, REPETIBLE	
8.2.3	Proceso disciplinario.	No existe un procedimiento acerca de qué hacer con respecto a las violaciones de seguridad que realicen los empleados.	1, INICIAL	
8.3	Cese del empleo o cambio de puesto de trabajo			38%
8.3.1	Responsabilidades del cese o cambio	Se están realizando procedimiento con respecto al cese o cambio de puesto de personal.	1, INICIAL	
8.3.2	Devolución de activos	Se está implementando el procedimiento de devolución de activos.	1, INICIAL	
8.3.3	Retirada de los derechos de acceso	Existe un procedimiento documentado respecto a la supresión de derechos de accesos.	4, GESTIONABLE Y MEDIBLE	
	SEGURIDAD FÍSICA Y DEL ENTORNO			90%

9.1	Áreas seguras			98%
9.1.1	Perímetro de seguridad física	Existe controles para el acceso al complejo los visitantes deben tener una autorización de alguien que labore internamente para tener acceso, se realiza el trámite de un formato donde se especifique los datos de la persona que entra. Una vez autorizada la persona quien facilito su acceso debe acompañarlo al lugar donde se desplace no es posible el acceso a las instalaciones físicas sin autorización.	5, Optimizado	
9.1.2	Controles físicos de entrada	El acceso a zona restringida existen controles para el acceso.	5, Optimizado	
9.1.3	Seguridad de oficinas, despachos e instalaciones	El CPD tiene el sistema biométrico para tener control en el acceso.	4, GESTIONABLE Y MEDIBLE	
9.1.4	Protección contra las amenazas externas y de origen ambiental	El CPD se está instalando protecciones contra amenazas externas.	4, GESTIONABLE Y MEDIBLE	
9.1.5	Trabajo en áreas seguras	Si existen áreas en las cuales se especifican en una directiva el trabajo en esas áreas.	4, GESTIONABLE Y MEDIBLE	
9.1.6	Áreas de acceso público y de carga y descarga	Las áreas de acceso al público siempre están un encargado para el acompañamiento en el lugar.	5, Optimizado	
9.2	Seguridad de los equipos			83%
9.2.1	Emplazamiento y protección de equipos	existe procedimientos para la protección de equipos	4, GESTIONABLE Y MEDIBLE	
9.2.2	Instalaciones de suministro	Existe planta eléctrica en donde se maneja la información critica	1. INICIAL	
9.2.3	Seguridad de cableado	existe control en algunos centros donde solo es accedido por personal autorizados	4, GESTIONABLE Y MEDIBLE	
9.2.4	Mantenimiento de los equipos	los equipos se monitorean constantemente, EXISTE PLAN DE CONTINGENCIA	4, GESTIONABLE Y MEDIBLE	
9.2.5	Seguridad de los equipos fuera de las instalaciones	Se tiene el mismo control de los equipos que están dentro de las instalaciones.	4, GESTIONABLE Y MEDIBLE	
9.2.6	Reutilización o retirada segura de equipos	Se implementó retiradas de equipos.	4, GESTIONABLE Y MEDIBLE	

	9.2.7	Retirada de materiales propiedad de la empresa	Existen controles pero aún existen debilidades	4, GESTIONABLE Y MEDIBLE	
		GESTIÓN DE COMUNICACIONES Y OPERACIONES			81%
10.1		Responsabilidades y procedimientos de operación			71%
	10.1.1	Documentación de los procedimientos de operación	existe procedimientos de las operaciones	4, GESTIONABLE Y MEDIBLE	
	10.1.2	Gestión de cambios	Existe el proceso de control de cambios pero no todos los formatos aplican a las situaciones.	3, DEFINIDA	
	10.1.3	Segregación de tareas	Se segregan funciones y tareas.	3, DEFINIDA	
	10.1.4	Separación de los recursos de desarrollo, prueba y operación	Se están realizando procedimientos	1, INICIAL	
10.2		Gestión de la provisión de servicios por terceros			95%
	10.2.1	Provisión de servicios	se tiene control sobre los acuerdos, existe una política de revisión	4, GESTIONABLE Y MEDIBLE	
	10.2.2	Supervisión y revisión de los servicios prestados por terceros	Se revisan los niveles de servicios de terceros, existe una política para la gestión de servicios.	4, GESTIONABLE Y MEDIBLE	
	10.2.3	Gestión del cambio en los servicios prestados por terceros	Se gestionan los cambios, tiene una política para la gestión de cambios.	4, GESTIONABLE Y MEDIBLE	
10.3		Planificación y aceptación del sistema			90%
	10.3.1	Gestión de capacidades	se realiza proyecciones anuales de las necesidades futuras	3, DEFINIDA	
	10.3.2	Aceptación del sistema	Se están realizando las pruebas antes de entrar en ejecución.	3, DEFINIDA	
10.4		Protección contra el código malicioso y descargable			95%
	10.4.1	Controles contra el código malicioso	Se tiene una consola de antivirus. Firewall	4, GESTIONABLE Y MEDIBLE	
	10.4.2	Controles contra el código descargado en el cliente	Se tienen barreras perimetrales.	4, GESTIONABLE Y MEDIBLE	
10.5		Copias de seguridad			90%
	10.5.1	Copias de seguridad de la información	Se hacen copias de seguridad pero no se cuenta con las herramientas para hacerlas, actualmente las copias se hacen locales. Pero existen procedimientos	3, DEFINIDA	
10.6		Gestión de la seguridad de las redes			95%

10.6.1	Controles de red	se tienen implementados control de acceso se han adaptado dispositivos avanzados para detectar comportamientos extraños en la red	4, GESTIONABLE Y MEDIBLE	
10.6.2	Seguridad de los servicios de red	se tienen identificados las características de seguridad	4, GESTIONABLE Y MEDIBLE	
10.7	Manipulación de los soportes			48%
10.7.1	Gestión de soportes extraíbles	El uso de soportes extraíbles no está autorizado sin embargo existen controles.	3. DEFINIDA	
10.7.2	Retirada de soportes	No existe una política de retirada de soportes, pero se han empleado procedimientos	3. DEFINIDA	
10.7.3	Procedimientos de manipulación de la información	existen controles pero no un procedimiento	1. INICIAL	
10.7.4	Seguridad de la documentación del sistema	Se tiene un control.	4, GESTIONABLE Y MEDIBLE	
10.8	Intercambio de información			39%
10.8.1	Políticas y procedimientos de intercambio de información	existe procedimiento	4, GESTIONABLE Y MEDIBLE	
10.8.2	Acuerdos de intercambio	Se están implementando acuerdos de intercambios	1. INICIAL	
10.8.3	Soportes físicos en transito	Si existe pero no se utiliza el procedimiento para todos los casos.	3, DEFINIDA	
10.8.4	Mensajería electrónica	se tiene protección dela información contenida en los correos	4, GESTIONABLE Y MEDIBLE	
10.8.5	Sistemas de información empresariales	La conexión se gestiona correctamente.	4, GESTIONABLE Y MEDIBLE	
10.9	Servicios de comercio electrónicos			95%
10.9.1	Comercio electrónico	no aplica		
10.9.2	Transacciones en línea	no aplica		
10.9.3	Información públicamente disponibles	la información pública está protegida de modificaciones	4, GESTIONABLE Y MEDIBLE	
10.10	Supervisión			94%
10.10.1	Registros de auditoría	se registran los eventos, se le hace seguimiento	4, GESTIONABLE Y MEDIBLE	
10.10.2	Supervisión del uso del sistema	se supervisa el uso de los sistemas	4, GESTIONABLE Y MEDIBLE	
10.10.3	Protección de la información de los registros	se protegen la información de los registros	4, GESTIONABLE Y MEDIBLE	
10.10.4	Registros de administración y operación	Existe un procedimiento de revisión.	4, GESTIONABLE Y MEDIBLE	

10.10.5	Registros de fallos	se tiene u software que permita monitorizar las conexiones de red	4, GESTIONABLE Y MEDIBLE	
10.10.6	Sincronización del reloj	se tiene sincronizados los reloj	3, DEFINIDA	
	CONTROL DE ACCESO			69%
11.1	Requisitos de negocio para el control de acceso			90%
11.1.1	Política de control de acceso	Si hay política de control de acceso pero no se cumple dicha política.	3, DEFINIDA	
11.2	Gestión de acceso de usuario			74%
11.2.1	Registro de usuario	Se tiene un procedimiento.	4, GESTIONABLE Y MEDIBLE	
11.2.2	Gestión de privilegios	se gestionan los privilegios	4, GESTIONABLE Y MEDIBLE	
11.2.3	Gestión de contraseñas de usuario	se gestionan las contraseñas y se establece tiempo de caducidad.	4, GESTIONABLE Y MEDIBLE	
11.2.4	Revisión de los derechos de acceso de usuario	se estan implementando procedimientos	1. INICIAL	
11.3	Responsabilidades de usuario			95%
11.3.1	Uso de contraseñas	existen una guía de recomendaciones para elegir contraseñas	4, GESTIONABLE Y MEDIBLE	
11.3.2	Equipo de usuarios desatendido	existe la política	4, GESTIONABLE Y MEDIBLE	
11.3.3	Política de puestos de trabajo despejado y pantalla limpia	existe la política	4, GESTIONABLE Y MEDIBLE	
11.4	Control de acceso a la red			54%
11.4.1	Política de uso de los servicios en red	existe política	4, GESTIONABLE Y MEDIBLE	
11.4.2	Autenticación de usuario para conexiones externas	existe política	4, GESTIONABLE Y MEDIBLE	
11.4.3	Identificación de los equipos en las redes	hay creadas vlan que nos permite identificar los equipos en la red,y un controlador de dominio.	4, GESTIONABLE Y MEDIBLE	
11.4.4	Protección de los puertos de diagnóstico y configuración remotos	existen medidas de protección tanto logica como fisica	4, GESTIONABLE Y MEDIBLE	
11.4.5	Segregación de las redes	las redes están segregadas	4, GESTIONABLE Y MEDIBLE	
11.4.6	Control de la conexión a la red	existe controles de conexión a la red	4, GESTIONABLE Y MEDIBLE	
11.4.7	Control de encaminamiento (routing) de red	existe controles de encaminamiento de red	4, GESTIONABLE Y MEDIBLE	
11.5	Control de acceso al sistema operativo			63%

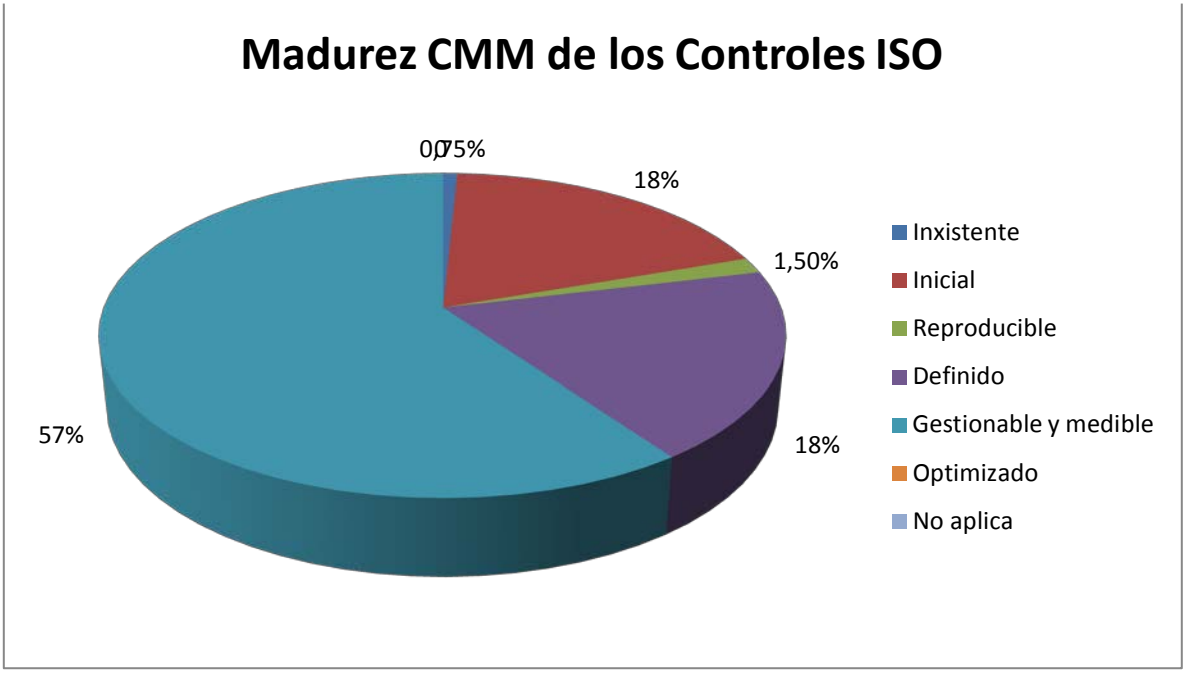
	11.5.1	Procedimientos seguros de inicio de sesión	existe mecanismos de inicio de sesión	4, GESTIONABLE Y MEDIBLE	
	11.5.2	Identificación y autenticación de usuario	existe mecanismos de identificación y autenticación de usuario	4, GESTIONABLE Y MEDIBLE	
	11.5.3	Sistemas de gestión de contraseñas	existe el sistema de gestión de contraseñas	4, GESTIONABLE Y MEDIBLE	
	11.5.4	Uso de los recursos del sistema	Las aplicaciones innecesarias son eliminadas del sistema	4, GESTIONABLE Y MEDIBLE	
	11.5.5	Desconexión automática de sesión	Se estan implementando procedimientos para la desconexion automatica de sesion	1. INICIAL	
	11.5.6	Limitación del tiempo de conexión	se estan realizando procedimientos para la limitacion de las ventaas de conexión	1. INICIAL	
11.6		Control de acceso a las aplicaciones y a la información			95%
	11.6.1	Restricción del acceso a la información	existe políticas en las restricciones de acceso de la información	4, GESTIONABLE Y MEDIBLE	
	11.6.2	Aislamiento de sistemas sensibles	si existe aislamiento de los sistemas sensibles	4, GESTIONABLE Y MEDIBLE	
11.7		Ordenadores portátiles y teletrabajo			10%
	11.7.1	Ordenadores portátiles y comunicaciones móviles	se estan crenado directivas para el uso de dispositivos moviles	1. INICIAL	
	11.7.2	Teletrabajo	no aplica		
		ADQUISICIÓN DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN			69%
12.1		Requisitos de seguridad de los sistemas de información			90%
	12.1.1	Análisis y especificación de los requisitos de seguridad	se asumen las debilidades y se estan realizando evaluaciones para verificar la seguridad en la entidad.	3, DEFINIDA	
12.2		Tratamiento correcto de las aplicaciones			74%
	12.2.1	Validación de los datos de entrada	si existen los controles que protegen las aplicaciones	4, GESTIONABLE Y MEDIBLE	
	12.2.2	Control del procesamiento interno	existe un control para la integridad de los datos y evitar ataques	4, GESTIONABLE Y MEDIBLE	
	12.2.3	Integridad de los mensajes	existen controles para verificar la integridad de los mensajes	4, GESTIONABLE Y MEDIBLE	
	12.2.4	Validación de los datos de salida	los usuarios tienen informacion suficiente para que se pueda evaluar	1. INICIAL	
12.3		Controles criptográficos			53%

	12.3.1	Política de uso de los controles criptográficos	existe sw para utilizarlo en la informacion secreta	4, GESTIONABLE Y MEDIBLE	
	12.3.2	Gestión de claves	Existe un sistema de gestion de claves.	1. INICIAL	
12.4		Seguridad de los archivos del sistema			10%
	12.4.1	Control de software en explotación	Existe controles de sw	1. INICIAL	
	12.4.2	Protección de los datos de prueba del sistema	Existe protección de los datos de pruebas	1. INICIAL	
	12.4.3	Control de acceso al código fuente de los programas	Existe un control al código fuente	1. INICIAL	
12.5		Seguridad en los procesos de desarrollo y soporte			95%
	12.5.1	Procedimientos de control de cambios	si existe los procedimientos y permiten trazar una auditoria	4, GESTIONABLE Y MEDIBLE	
	12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	si existe el procedimientos	4, GESTIONABLE Y MEDIBLE	
	12.5.3	Restricciones a los cambios en los paquetes de software	todos los cambios son evaluados y probados	4, GESTIONABLE Y MEDIBLE	
	12.5.4	Fugas de información	existe controles no es permitio el uso de memoras usb, camaras,portatiles personales	4, GESTIONABLE Y MEDIBLE	
	12.5.5	Externalización del desarrollo de software	se realizan contratos para el desarrollo de algunos software	4, GESTIONABLE Y MEDIBLE	
12.6		Gestión de las vulnerabilidades técnica			90%
	12.6.1	Control de las vulnerabilidades técnicas	se han realizado gestion de vulnerabilidades	3. DEFINIDA	
		GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN			28%
13.1		Notificación de eventos y puntos débiles de seguridad de la información			10%
	13.1.1	Notificación de los eventos de seguridad de la información	se esta implementando la documentación de sistema de gestión de incidencias	1. INICIAL	
	13.1.2	Notificación de puntos débiles de seguridad	se esta implementando las notificaciones de los puntos débiles	1. INICIAL	
13.2		Gestión de incidentes y mejoras de seguridad de la información			47%
	13.2.1	Responsabilidades y procedimientos	se esta implementando un esquema de procedimientos de incidencias	2. REPETIBLE	
	13.2.2	Aprendizaje de los incidentes de seguridad de la información	se tienen los mecanismos de aprendizaje sobre los incidentes de seguridad	3. DEFINIDA	
	13.2.3	Recopilación de evidencias	se sigue un procedimientos de las incidencias detectadas	3. DEFINIDA	
		GESTION DE LA CONTINUIDAD DEL NEGOCIO			42%

14.1		Aspectos de seguridad de la información en el proceso de la gestión de la continuidad del negocio			42%
	14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	Se esran implementano una gestión de continuidad	3. DEFINIDA	
	14.1.2	Continuidad del negocio y evaluación de riesgos	se tienen un plan de continuidad ni evaluación de riesgos	3. DEFINIDA	
	14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información	idem	1, INICIAL	
	14.1.4	Marco de referencia para la planificación de la cont. Del negocio	idem	1, INICIAL	
	14.1.5	Pruebas, mantenimiento y revaluación de planes de continuidad	idem	1, INICIAL	
		CUMPLIMIENTO			75%
15.1		Cumplimiento de los requisitos legales			80%
	15.1.1	Identificación de la legislación aplicable	se cumple un 80% las legislaciones vigentes	4, GESTIONABLE Y MEDIBLE	
	15.1.2	Derechos de propiedad intelectual	En el plan de inversion se invluyeron licenciamiento de sw para cimplir totalmente con los derechos de propiedad intelectual	3. DEFINIDA	
	15.1.3	Protección de los documentos de la organización	se le da un tratamiento especial a los documentos una vez van a ser archivados	4, GESTIONABLE Y MEDIBLE	
	15.1.4	Protección de datos y privacidad de la información de carácter personal	el tratamiento de la información de carácter personal se estan realizndo procedimeintos	4, GESTIONABLE Y MEDIBLE	
	15.1.5	Prevención del uso indebido de recursos de tratamiento de la información	se ahn realizado reuniones que permiten establecer el tratamiento de la informacion.	1. INICIAL	
	15.1.6	Regulación de los controles criptográficos	la documentación cumple con los controles criptográficos	4, GESTIONABLE Y MEDIBLE	
15.2		Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico			93%
	15.2.1	Cumplimiento de las políticas y normas de seguridad	se le hace un seguimiento de las evidencias	3, DEFINIDA	
	15.2.2	Comprobación del cumplimiento técnico	se realizan auditorias de meci el cual se generan informes con las novedades detectadas para mejora	4, GESTIONABLE Y MEDIBLE	
15.3		Consideraciones sobre las auditorias de los sistemas de información			53%
	15.3.1	Controles de auditoria de los sistemas de información	en las auditorias se hace el levantamiento de novedades y se toman acciones	4, GESTIONABLE Y MEDIBLE	
	15.3.2	Protección de las herramientas de auditoria de los Sist. información	se estan implementando herramientas de auditoria	1, INICIAL	

5.5 PRESENTACIÓN DE RESULTADOS

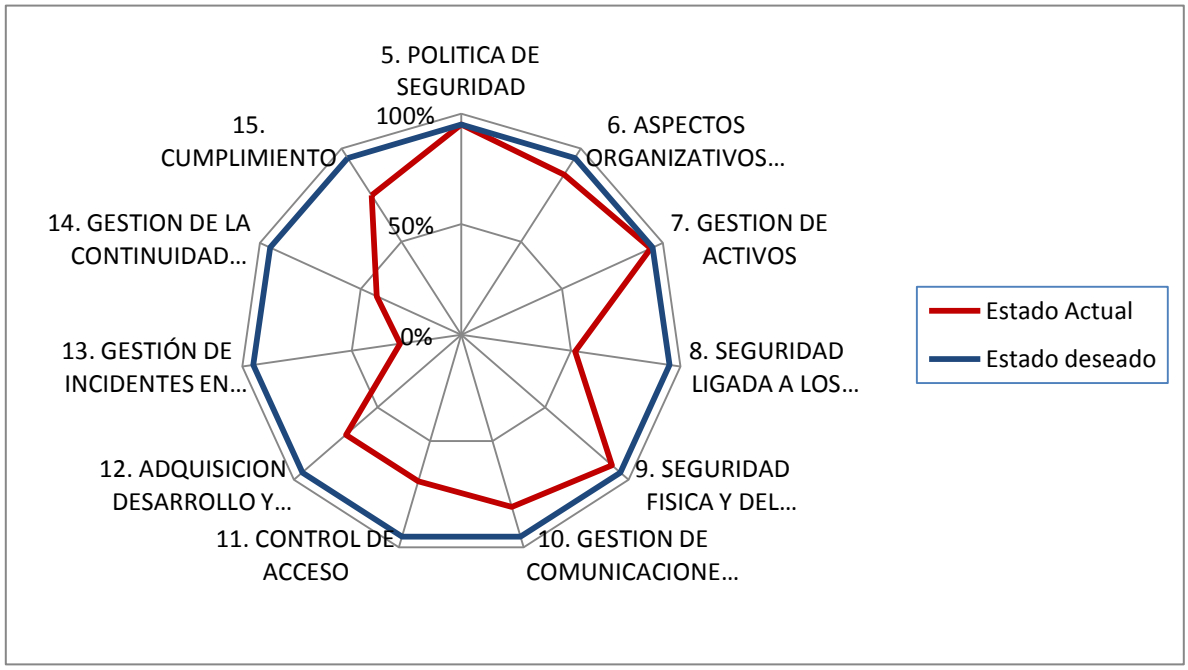
5.5.1 Estado de madurez de los controles



5.5.2 Porcentaje de cumplimiento por dominio

5. POLÍTICA DE SEGURIDAD	**95%**
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**86%**
7. GESTIÓN DE ACTIVOS	**94%**
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**52%**
9. SEGURIDAD FÍSICA Y DEL ENTORNO	**90%**
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES	**81%**

11. CONTROL DE ACCESO	**69%**
12. ADQUISICIÓN DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	**69%**
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	**28%**
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**42%**
15. CUMPLIMIENTO	**75%**



De la anterior graficas podemos evaluar que el nivel de cumplimiento en la mayoría de los controles se encuentra en un nivel aceptable de implementación de los controles planteados en la ISO/IEC 27001.

5.6 INFORME DE AUDITORIAS

Fecha: _24-12-2013_____

Informe No.:	Auditores:
01	Maria Martínez
Auditoria No.	Sandra Perez
01	

Resumen de los Hallazgos de Auditoria:		
Objetivo de la Auditoria: Verificar el grado de cumplimiento del SGSI acuerdo a la norma ISO 27001:2005		
Alcance: Todos los controles de la norma ISO 27001:2005		
Criterio de Auditoria: ISO 27001:2005		
Auditores Maria Martinez, Sandra Perez		
Fecha de Auditoria 21 -12-2013		
Acuerdo a las auditorias interna al SGSI detectamos lo siguientes hallazgos:		
10.4 Protección contra el código malicioso y descargable	Posibilidad de mejora	La entidad cuenta con sistema de detección de intruso, firewall y antivirus, pero se ha detectado que los desarrolladores poseen privilegios de administrador sobre algunos servidores lo que posibilita la difusión de sw malicioso
11.1.1 Política de Control de acceso	No conformidad Menor	Se ha contastado que no hay un proceso estricto de control de ingreso al CPD
12.4.3 control de acceso al código fuente de los programas	No conformidad Menor	Se ha constatado que los desarrolladores poseen privilegios de administrador en el servidor que les permite realizar modificaciones y actualizaciones del código fuente, utilizando una cuenta única de administrador por lo que no puede ser rastreado quien ha realizado dicha información.
14.1.2a continuidad del negocio	No conformidad Mayor	No hay un plan estratégico para la continuidad del negocio, se debería desarrollar un plan de mantenimiento para asegurar la disponibilidad de información tras interrupciones o falla de los procesos críticos
Se puede observar que el sistema en algunos procesos necesitan fortalecer para estar preparados para la auditoria de revisión del mismo.		

BIBLIOGRAFIA

Portal de Soluciones técnicas y organizativas a los controles de la Norma Internacional ISO/IEC 27002. http://www.iso27002.es/

Sistema de gestión de la seguridad de la información. UOC Daniel/Silvia Garre

Compilación de Norma del SGSI http://www.qualypedia.org/ISO%2027001.S-7-3-Resultados-de-la-revision.ashx.

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Ministerio de Administraciones Públicas, http://administracionelectronica.gob.es

Análisis de Riesgo http://www.securityartwork.es/2012/04/26/analisis-de-riesgos-con-magerit-en-el-ens-ii/.

Metodología Magerit http://www.acis.org.co/fileadmin/Conferencias/ConfArmandoCarvajMayo8.pdf.

GLOSARIO DE TERMINOS

SGSI(Sistema de Gestión de la Seguridad de la Información) : Sistema de gestión que comprende la política, la estructura organizativa, los procedimientos , los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información.

ISO 27001: 2005: Es una norma reconocida mundialmente para los sistemas de Gestión de Seguridad de la Información, la cual indica los controles a seguir al momento de diseñar e implementar un sistema de seguridad de la información.

AMENAZA: Es un evento que pueden desencadenar un incidente en la organización, produciendo daños materiales o perdidas inmateriales en sus activos.

IMPACTO: Consecuencia de la materialización de una amenaza.

RIESGO: Posibilidad de que se produzca un impacto determinado en un activo en un dominio o en toda la Organización.

VULNERABILIDAD: Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

ATAQUE: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

ANEXOS

ANEXO A - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

ANEXO B - PROCEDIMIENTOS DE AUDITORIA INTERNA

ANEXO C - DECLARACIÓN DE APLICABILIDAD

ANEXO D - ANÁLISIS DE AMENAZAS

ANEXO E - IMPACTO POTENCIAL

ANEXO F - RIESGO RESIDUAL