MEMORIA

PLAN DE IMPLEMENTACIÓN DE LA ISO/IEC 27001: 2005

PRESENTADO POR:
CAREM GYSSELL NIETO GARCÍA

TUTOR ASIGNADO:
ANTONIO JOSE SEGOVIA HENARES

UNIVERSIDAD OBERTA DE CATALUNYA
MASTER INTERINSTITUCIONAL EN SEGURIDAD DE LA INFORMACION Y LAS TELECOMUNICACIONES
BARCELONA, ESPAÑA
2013

Tabla de Contenido

LISTADO DE FIGURAS

LISTADO DE TABLAS

0. MARCO TEORICO

1.1 ISO 27001

ISO/IEC 27001 es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales. Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

ISO/IEC 27001 es una norma adecuada para cualquier organización, grande o pequeña, de cualquier sector o parte del mundo. La norma aporta particularmente si la protección de la información es crítica, como en finanzas, sanidad sector público y tecnología de la información (TI).

Puede utilizarse para garantizar a los clientes que su información está protegida.

Beneficios:

El hecho de certificar un SGSI según la norma **ISO/IEC 27001** puede aportar las siguientes ventajas a una organización:

- Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial.
- Demuestra que se respetan las leyes y normativas que sean de aplicación.
- Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.
- Verifica que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información.
- Demuestra el compromiso de la dirección con la seguridad de la información.
- El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora.

ISO / IEC 27001 requiere que la administración:

- Examine de forma sistemática los riesgos de la organización de seguridad de información, teniendo en cuenta las amenazas, vulnerabilidades e impactos.
- Diseñe e implemente un conjunto coherente y exhaustivo de los controles de seguridad de la información y / u otras formas de tratamiento del riesgo (por ejemplo, evitar el riesgo o la transferencia de riesgos) para hacer frente a los riesgos que se consideran inaceptables, y
- Adopte un proceso de gestión global para asegurar que los controles de seguridad de la información sigan satisfaciendo las necesidades de la organización la información de seguridad sobre una base continua.

1.2 ISO 27002

ISO / IEC 27002 proporciona las mejores prácticas y recomendaciones sobre la gestión de seguridad de la información para su utilización por los responsables de iniciar, implementar o mantener la seguridad de la información de su organización.

La norma contiene los siguientes doce secciones principales:

1. Evaluación de riesgos.
2. La política de seguridad - la dirección de gestión.
3. Organización de seguridad de la información - gestión de seguridad de la información.
4. Gestión de activos - inventario y clasificación de los activos de información.
5. Recursos de la seguridad humana - Aspectos de seguridad para los empleados de la unión, el movimiento y salir de una organización.
6. Seguridad física y ambiental - la protección de las instalaciones del equipo
7. Gestión de comunicaciones y operaciones - gestión de los controles técnicos de seguridad en sistemas y redes
8. Control de acceso - la restricción de los derechos de acceso a las redes, sistemas, aplicaciones, funciones y datos
9. Obtención de información de sistemas, desarrollo y mantenimiento - la construcción de la seguridad en las aplicaciones
10. Seguridad de la información de gestión de incidentes - anticipar y responder adecuadamente a las violaciones de seguridad de la información
11. Gestión de la continuidad - la protección, conservación y recuperación de negocio críticos los procesos y sistemas
12. Cumplimiento - Conformidad asegurar con políticas de seguridad de la información, normas, leyes y reglamentos

1. Fase 1: Situación actual: Contextualización, Objetivos y Análisis Diferencial

1.3 CONTEXTUALIZACIÓN

La organización seleccionada para el Trabajo Final de Master es un establecimiento público que trabaja por el desarrollo y la protección integral de la primera infancia, la niñez, la adolescencia y el bienestar de las familias colombianas y cuenta con aproximadamente diez mil funcionarios distribuidos en 33 ciudades de Colombia.

El alcance que tendrá el Plan de Implementación de la ISO/IEC 27001:2005 es la administración de la infraestructura tecnológica (sistemas de información y plataforma tecnológica como servidores, equipos de red, equipos de seguridad) que apoya las a ctividades internas que permiten a los funcionarios llevar a cabo sus labores diarias y los servicios que el establecimiento público ofrece a la ciudadanía como son: solicitud y seguimiento a tramites tales como permisos de salida del país, adopciones, peticiones y denuncias, entre otros.

La administración de estos recursos es manejada por subcontratación con una organización con amplia experiencia en tecnología que pone a disposición aproximadamente 30 ingenieros ubicados en la sede principal (in house) que son especialistas en cada uno de los servicios contratados, como son:

- Correo
- Backups
- Almacenamiento
- Directorio activo
- Administración de servidores Windows y Linux
- Redes
- Firewall
- IDS
- Proxy
- Bases de datos sql server y Oracle
- Aplicaciones misionales

- Seguridad de la información (apoyo).

La infraestructura que soporta los procesos más críticos para la organización se encuentra ubicada en un centro de cómputo externo de tipo Tier III. Un gran porcentaje de servidores y dispositivos críticos se encuentran en alta disponibilidad, sin embargo, inicialmente no se hizo un dimensionamiento adecuado de la infraestructura por lo cual a pesar de las condiciones del centro de cómputo y de la configuración actual de los servidores se presentan constantes fallas que afectan la seguridad de la información, más específicamente en cuanto a disponibilidad, adicional a esto hay una debilidad en cuanto a la documentación de los procesos y procedimientos, no existen políticas claras y las que hay no han sido difundidas a toda la organización.

1.4 OBJETIVOS DEL PLAN DIRECTOR

Los objetivos del plan director de seguridad para la organización planteada son los siguientes:

- Identificar los riesgos a los que está expuesta la infraestructura tecnológica de la organización.
-
- Mantener la disponibilidad, integridad y confidencialidad de la información de los niños, niñas, adolecentes, familias colombianas y demás entes que lo soliciten.
-
- Mejorar la seguridad actual de la organización.

1.5 ANÁLISIS DIFERENCIAL

A continuación se relaciona el estado actual de la organización con respecto a ISO 27001 e ISO 27002, en donde revisando uno a uno los controles de la norma se muestra cuales se han aplicado y cuales no con una pequeña descripción antes de la implementación del SGSI:

ANALISIS DIFERENCIAL	
CONTROL	**REVISION**
5. Política de Seguridad	
5.1 Política de Seguridad de la Información	
5.1.1 Documento de la Política de SI	Si se tiene el documento.
5.1.2 Revisión de la Política de SI	El documento de la política está revisado y aprobado.
6. Organización de la SI	
6.1 Organización Interna	
6.1.1 Compromiso de la dirección con la seguridad de la información	Se tiene evidencia de compromiso de la dirección n en la asignación de presupuesto, capacitaciones y contratación de personal para el SGSI.
6.1.2 Coordinación de la Seguridad de la Información	La coordinación de temas de seguridad está a cargo del oficial de seguridad de la organización y tiene colaboración del oficial de seguridad del proveedor contratado y de analistas de seguridad. Adicional a esto existen líderes para los diferentes servicios que deben cumplir con las obligaciones de seguridad que se les asignen.
6.1.3 Asignación de Responsabilidades para la Seguridad de la Información	Los dueños de los activos relacionados con la infraestructura tecnológica son los especialistas del proveedor y cada uno de estos tiene un líder de la organización que es el responsable directo de cada activo.
6.1.4 Proceso de Autorización para los Servicios	Existe una política de uso de recursos tecnológicos que aplica para terceros. Sin embargo no existe una matriz de roles y recursos ni para la organización ni para terceros, por lo cual, no está definido quien debe tener o no cada servicio.
6.1.5 Acuerdos sobre Confidencialidad	El proveedor que administra la infraestructura tecnológica no firmo acuerdos de confidencialidad con la organización.
6.1.6 Contacto con las Autoridades	No se tiene claro a quien contactar en caso de incidentes, no existe un documento socializado con esta información.
6.1.7 Contacto con Grupos de Interés	La organización no ha determinado grupos de interés

Especiales	especiales, es decir, no existe documentación en la que se especifique que grupos se consultan.
6.1.8 Revisión Independiente de la SI	No aplica dentro del alcance del plan.
6.2 Partes Externas	
6.2.1 Identificación de los Riesgos	No se ha realizado una identificación de riesgos por el acceso de terceros.
6.2.2 Seguridad con los Clientes	Las políticas de seguridad aplican para los clientes, pero no se hace un apartado específico para estos, ni se socializa con las terceras partes.
6.2.3 Seguridad en los Acuerdos con Terceras Partes	Las políticas de seguridad y de uso de recursos tecnológico aplican para los clientes, pero no se hace un apartado específico para estos, ni se socializa con las terceras partes.
7. Gestión de Activos	La organización tiene un plan de gestión de activos pero terceriza la gestión de activos relacionados con infraestructura tecnológica.
7.1 Responsabilidad por los Activos	
7.1.1 Inventario de Activos	Los especialistas del proveedor son los encargados de hacer el inventario de activos.
7.1.2 Propietario de los Activos	Los propietarios de los activos son los especialistas y los responsables directos son los líderes de cada servicio que pertenecen a la organización.
7.1.3 Uso Aceptable de los Activos	Existe una política de uso de recursos tecnológicos que debe ser cumplida por los contratistas.
7.2 Clasificación de la Información	
7.2.1 Directrices de Clasificación	Se cuenta con una guía de clasificación documentada. La información se clasifica según su criticidad y sensibilidad.
Se está trabajando en conjunto con gestión documental para rotular la información.	Se está trabajando en conjunto con gestión documental para rotular la información.
8. Seguridad de los Recursos Humanos	
8.1 Antes de la Contratación Laboral	
8.1.1 Roles y Responsabilidades	No existe una matriz de roles y responsabilidades definida, ni para la organización ni para los contratistas.
8.1.2 Selección	El área de gestión humana cuenta con las listas de verificación con los perfiles para los contratistas.
8.1.3 Términos y Condiciones	No se hizo firmar un acuerdo de confidencialidad a los contratistas al inicio del proyecto ni en ningún

Laborales	momento.
8.2 Durante la Vigencia del Contrato	
8.2.1 Responsabilidades de la dirección	No se tienen claros los roles de seguridad, la dirección no ha determinado estos roles.
8.2.2 Educación, formación y concientización sobre SI	Se tiene un plan de sensibilización, sin embargo no se han incluido como grupo objetivo los contratistas.
8.2.3 Proceso Disciplinario	No se tiene un proceso disciplinario para cuando se presentan incidentes de seguridad, ni para los empleados ni para contratistas.
8.3 Terminación o Cambio de la Contratación	
8.3.1 Responsabilidades en la Terminación	Por parte de la organización no existe un procedimiento para terminación o cambio de labores de los contratistas, esto se deja a disposición del contratista. El procedimiento solo existe para la organización como tal.
8.3.2 Devolución de Activos	De la misma forma el proceso de devolución de activos se hace por parte del contratista y no tiene verificación por parte de la organización, a pesar de que el contratista está inhouse. El procedimiento solo existe para la organización como tal.
8.3.3 Retiro de los Derechos de Acceso	Existe un procedimiento de retiro de gestión de acceso peor no está documentado.
9. Seguridad Física y del Entorno	
9.1 Áreas Seguras	
9.1.1 Perímetro de Seguridad Física	La infraestructura tecnológica dentro del alcance se encuentra en un data center tipo tear III, que está ubicado en la Zona franca de la ciudad de Bogotá, cuenta con mecanismos de control de acceso, paredes y puertas seguras y personal de seguridad que controla el ingreso de personal.
9.1.2 Controles de Acceso Físico	El acceso a la zona franca solo se puede hacer con previa autorización. Se valida el ingreso tanto en la entrada a la zona franca como en la entrada a Terremark (empresa con la que se contrata), adicional a esto existe un control de acceso con tarjeta de proximidad para ingresar al data center.
9.1.3 Seguridad de Oficinas, Recintos e Instalaciones	Las oficinas en las que se encuentran los especialistas no son seguras, la puerta no tiene llave y los equipos portátiles se dejan en la noche con una guaya de seguridad con clave.
9.1.4 Protección contra Amenazas Externas y Ambientales	El data center está conectado a múltiples líneas de distribución eléctrica y de refrigeración, pero únicamente con una activa.

9.1.5 Trabajo en Áreas Seguras	Las oficinas en las que trabajan los especialistas no son seguras, las puertas no se pueden cerrar y no son supervisadas cuando están desocupadas.
9.1.6 Áreas de Carga, despacho y acceso público	La oficina de los especialistas está al lado del almacén que es un área de carga y descarga de suministros.
9.2 Seguridad de los Equipos	
9.2.1 Ubicación y Protección de los Equipos	Los servidores se encuentran seguros en el data center contratado. Los equipos portátiles de los especialistas están ubicados en una oficina sin seguridad, su única protección es una guaya.
9.2.2 Servicios de Suministro	El data center está conectado a múltiples líneas de distribución eléctrica con solo una activa.
9.2.3 Seguridad del Cableado	El data center garantiza la seguridad del cableado y que es certificado.
9.2.4 Mantenimiento de los Equipos	Se realiza mantenimiento anual de los servidores por parte de un tercero contratado por la organización.
9.2.5 Seguridad de los Equipos Fuera de las Instalaciones	Los equipos portátiles están asegurados. Existe una VPN para conectarse a la red de la organización. No se hace backup de la información ni se cifra la información confidencial.
9.2.6 Seguridad en la Reutilización o Eliminación de los Equipos	Los equipos que dejan los especialistas son formateados pero no se borra la información a bajo nivel, ni se tienen mecanismos de destrucción de estos.
9.2.7 Retiro de Activos	Para retirar los activos de la organización se debe tener una autorización previa que es solicitada en portería, de los contrario no se puede sacar.
10. Gestión de Comunicaciones y Operaciones	
10.1 Procedimientos Operacionales y Responsabilidades	
10.1.1 Documentación de los procedimientos de operación	La mayoría de procedimientos de operación no están documentados.
10.1.2 Gestión del Cambio	Se tiene un procedimiento de gestión de cambios definido y el comité se reúne semanalmente.
10.1.3 Distribución (segregación) de funciones	Se cumple la segregación de funciones debido a que cada servicio es manejado por un especialista.
10.1.4 Separación de las instalaciones	Se manejan ambientes de pruebas por aparte de los

de Desarrollo, ensayo y operación	ambientes de producción.
10.2 Gestión de la Prestación del Servicio por Terceras Partes	
10.2.1 Prestación del Servicio	Las políticas de seguridad existentes deben aplicar para los contratistas, sin embargo, no son difundidas.
10.2.2 Monitoreo y revisión de los servicios por terceros	La organización hace seguimiento al contratista por medio de un informe mensual pero no está enfocado en seguridad sino en gestión.
10.2.3 Gestión de los Cambios en los servicios por terceras partes	Los contratistas participan en el comité de gestión de cambios y toda actividad de cambios realizada debe pasar por el comité.
10.3 Planificación y Aceptación del Sistema	
10.3.1 Gestión de la Capacidad	Existe un proceso apoyado en ITIL para gestión de capacidad en el que se evalúa la capacidad de la infraestructura tecnológica.
10.3.2 Aceptación del Sistema	Se cuenta con un procedimiento para aplicaciones y su paso a producción, y se tienen guías a de seguridad para hardware.
10.4 Protección Contra Códigos Maliciosos y Móviles	
10.4.1 Controles contra códigos maliciosos	Se tiene instalada una solución de antivirus para toda la organización. Existe la política de uso de recursos tecnológicos en la que se hace referencia a la instalación de software.
10.4.2 Controles contra códigos móviles	La ejecución de código móvil si es realizada para los agentes de antivirus específicamente, pero está controlada la ejecución de otro tipo de código móvil.
10.5 Respaldo	
10.5.1 Respaldo de la Información	Se tiene una política de backup en la que se define la periodicidad de backup a servidores y a equipos del personal de la organización. No se hace backup a los equipos de los especialistas. Los backups se guardan en servidores y en cintas.
10.6 Gestión de la Seguridad de las Redes	
10.6.1 Controles de las Redes	Las redes son manejas por medio de Vlans para separar los servidores de los equipos de cómputo. Para el acceso remoto a la red existe el servicio de VPN. El canal de datos que existe entre el data center contratado y la organización es redundante así como dispositivos críticos como son firewall y switches de core.

10.6.2 Seguridad de los servicios de la red	Existe una solución de firewall, proxy e IDS, se tienes acuerdos de nivel de servicio con los proveedores de internet para garantizar el servicio.
10.7 Manejo de los Medios	
10.7.1 Gestión de los Medios Removibles	No existe un procedimiento para la gestión de medios removibles.
10.7.2 Eliminación de los Medios	No existe un procedimiento de eliminación de medios.
10.7.3 Procedimientos para el Manejo de la Información	Se tiene una guía de clasificación de la información.
10.7.4 Seguridad de la Documentación del Sistema	Se está implementando un sistema de documentación.
10.8 Intercambio de la Información	
10.8.1 Políticas y Procedimientos para el Intercambio de Información	No existen políticas y procedimientos para el intercambio de información.
10.8.2 Acuerdos para el intercambio	No existen acuerdos de intercambio.
10.8.3 Medios Físicos en tránsito	Se tiene una guía de clasificación de la información.
10.8.4 Mensajería Electrónica	Se cuenta con una restricción de acceso lógico y configuración de seguridad de Exchange.
10.8.5 Sistemas de Información del Negocio	Se cuenta con control de acceso lógico y acceso a la red.
10.9 Servicios de Comercio Electrónico	
10.9.1 Comercio Electrónico	No aplica
10.9.2 Transacciones en Línea	Existe un sistema de IDS e IPS.
10.9.3 Información disponible al público	Se cuenta con un procedimiento de paso de aplicaciones a producción y se realizan pruebas de hacking ético externas.
10.10 Monitoreo	
10.10.1 Registro de Auditorías	No se cuenta con un sistema de logs centralizado, los servidores guardan los logs localmente pero el espacio no es suficiente y se sobrescriben.
10.10.2 Monitoreo del uso del Sistema	Se cuenta con herramientas de monitoreo de los sistemas y servidores.
10.10.3 Protección de la Información del Registro	Los logs no se encuentran centralizados, ni protegidos.
10.10.4 Registros del Administrador y del Operador	Estos registros se guardan en cada servidor, pero no están centralizados por lo tanto se podrían modificar

	por el administrador.
10.10.5 Registro de Fallas	Existe una herramienta de reporte de fallas por parte de los usuarios en el que se muestra el proceso de resolución de la falla.
10.10.6 Sincronización de Relojes	Se cuenta un servidor de sincronismo de relojes.
11. Control de Acceso	
11.1 Requisitos del Negocio para el Control del Acceso	
11.1.1 Política de Control de Acceso	Existe una política de control de acceso.
11.2 Gestión del Acceso a Usuarios	
11.2.1 Registro de Usuarios	Existe un controlador de dominio para el registro de usuarios.
11.2.2 Gestión de Privilegios	Los privilegios están dados por el controlador de dominio, sin embargo no existe una matriz de roles y recursos asignados definidas ni para los empleados ni para los contratistas.
11.2.3 Gestión de Contraseñas para Usuarios	Existe una política de contraseñas que se hace cumplir por medio del controlador de dominio.
11.2.4 Revisión de los Derechos de Acceso de los Usuarios	No existe una matriz de roles y recursos asignados.
11.3 Responsabilidades de los Usuarios	
11.3.1 Uso de Contraseñas	Dentro de la política de uso de recursos tecnológicos se habla de las contraseñas como un recurso y la forma de protegerlo.
11.3.2 Equipo de Usuario Desatendido	Existe una política de bloqueo de equipos desatendidos.
11.3.3 Política de Escritorio Despejado y de Pantalla Despejada	Se tiene como directriz guardar la información crítica en un espacio asignado de la SAN para cada usuario, a esta información se le hace backup. Existe una política de bloqueo de equipos desatendidos.
11.4 Control de Acceso a las Redes	
11.4.1 Política de uso de los servicios de red	Existe una política de uso de recursos tecnológicos en el que se incluye el uso de los servicios de red.
11.4.2 Autenticación de Usuarios para Conexiones Externas	Se cuenta con una VPN y acceso lógico al correo
11.4.3 Identificación de los Equipos en las Redes	Los equipos son identificados por medio del controlador de dominio.

11.4.4 Protección de los puertos de configuración y diagnóstico remoto	Existe una protección por puertos lógicos (antivirus, IPS) no hay protección para serial, paralelo, USB.
11.4.5 Separación en las Redes	Se cuenta con VLANs.
11.4.6 Control de Conexión a las redes	Se cuenta con control de acceso lógico. Existe un firewall que controla el tráfico.
11.4.7 Control de Enrutamiento en la Red	Se cuenta con Gateway, protocolos de enrutamiento configurados y todo el tráfico pasa por firewall.
11.5 Control de Acceso al Sistema Operativo	
11.5.1 Procedimientos de Registro de Inicio Seguro	Se centraliza por el controlador de dominio y se tienen certificados digitales
11.5.2 Identificación y Autenticación de Usuarios	Se realiza por medio del controlador de dominio.
11.5.3 Sistema de Gestión de Contraseñas	Se maneja por el controlador de dominio, TODOS los sistemas tiene sistema de administración de contraseñas.
11.5.4 Uso de las utilidades del sistema	Existen GPO para limitar el acceso a los sistemas por medio del controlador de dominio. Se bloquea la descarga de software,
11.5.5 Tiempo de Inactividad de la Sesión	Existe un time-out en controlador de dominio para bloquear la sesión.
11.5.6 Limitación del tiempo de Conexión	No existe limitación de tiempos de conexión a los servidores.
11.6 Control de Acceso a las Aplicaciones y a la Información	
11.6.1 Restricción de acceso a la Información	Se restringe el acceso por medio del controlador de dominio.
11.6.2 Aislamiento de sistemas sensibles	Los servidores se encuentran en un data center externo con altas especificaciones de seguridad.
11.7 Computación Móvil y Trabajo Remoto	
11.7.1 Computación y comunicaciones móviles	No existe un control.
11.7.2 Trabajo Remoto	El acceso remoto se realiza por medio de una VPN.
12. 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	Los sistemas nuevos pasan por un proceso se pruebas antes de pasar a producción. Existe un procedimiento de gestión de cambio para actualización o cambios de sistemas.
12.2 Seguridad de las aplicaciones del sistema	
12.2.1 Validación de los datos de entrada	El área de desarrollo de la organización lleva a cabo la validación de los datos de entrada para cada aplicación. Hace parte de las pruebas antes de sacar una aplicación a producción.
12.2.2 Control de Procesamiento Interno	Se utiliza software para detección de alteraciones en librerías o archivos.
12.2.3 Integridad del Mensaje	No existe ningún control para identificar la integridad de los mensajes.
12.2.4 Validación de los datos de salida	Todas las modificaciones a los sistemas son verificadas y validadas para evitar algún problema en la continuidad de los servicios.
12.3 Controles Criptográficos	
12.3.1 Política sobre el uso de controles criptográficos	No existe una política de controles criptográficos.
12.3.2 Gestión de Claves	Existe un instructivo de adquisición y manejo de llaves digitales
12.4 Seguridad de los Archivos del Sistema	
12.4.1 Control del Software Operativo	Existen procedimientos para instalación de software.
12.4.2 Protección de los datos de prueba del sistema	Los datos utilizados para las pruebas deben ser autorizados antes de la realización de estas para evitar la fuga de información confidencial.
12.4.3 Control de acceso al código fuente de los programas	No existen acuerdos de confidencialidad para los terceros y no hay perfiles de usuarios en os servidores por lo cual podría haber acceso de cualquier administrador al código fuente.
12.5 Seguridad en los procesos de desarrollo y soporte	
12.5.1 Procedimientos de control de cambios	Se cuenta con un procedimiento de control de cambios.
12.5.2 Revisión Técnica de las aplicaciones después de los cambios en el SO	Se realiza control de cambios y una autorización de revisión y aprobación del buen funcionamiento del cambio.
12.5.3 Restricciones en los cambios a los paquetes de software	Se cuenta con un procedimiento de control de cambios.

12.5.4 Fuga de información	No existe control.
12.5.5 Desarrollo de software contratado externamente	El desarrollo de todas las aplicaciones lo hace la misma organización, sin embargo, el contratista administra los servidores en las que se alojan para lo cual garantizan la disponibilidad de estos servidores por medio del Data Center Tier III y los servidores en alta disponibilidad.
12.6 Gestión de la Vulnerabilidad Técnica	
12.6.1 Control de las Vulnerabilidades Técnicas	Se realiza análisis de riesgos y se tiene un plan de remediación de vulnerabilidades que aún no se ha implementado.
13. Gestión de los Incidentes de la Seguridad de la Información	
13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información	
13.1.1 Reporte sobre los eventos de seguridad de la información	Existe el procedimiento pero aún no ha sido divulgado.
13.1.2 Reporte sobre las debilidades en la seguridad	Ni los usuarios ni los contratistas conocen el procedimiento.
13.2 Gestión de los Incidentes y las mejoras en las SI	
13.2.1 Responsabilidades y Procedimientos	Existe un procedimiento pero no ha sido divulgado.
13.2.2 Aprendizaje debido a los incidentes de SI	No existe un mecanismo establecido para cuantificar y monitorear los incidentes de seguridad.
13.2.3 Recolección de Evidencias	Existe un procedimiento de recolección de evidencias.
14. Gestión de la Continuidad del Negocio	
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio	
14.1.1 Inclusión de la SI en el proceso de gestión de la continuidad del negocio	Se está definiendo un plan de continuidad de negocio en el que se están incluyendo aspectos de seguridad de la información. Se creó un plan de contingencia de los recursos tecnológicos, se definieron escenarios de falla, se tiene un cronograma de pruebas y se han realizado pruebas de escritorio de los escenarios.
14.1.2 Continuidad del Negocio y	No se han evaluado riesgos relacionados con

evaluación de riesgos	continuidad de negocio.
14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la SI	No se han implementado planes de continuidad, hasta el momento se han llevado a cabo pruebas de contingencia de la infraestructura.
14.1.4 Estructura para la Planificación de la continuidad del negocio	No se ha creado la estructura.
14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	No se han realizado pruebas,
15. Cumplimiento	
15.1 Cumplimiento de los Requisitos Legales	
15.1.1 Identificación de la Legislación Aplicable	Existe un contrato con el contratista en donde se especifican todos los servicios que debe ofrecer y los tiempos de cumplimiento.
15.1.2 Derechos de Propiedad Intelectual	Existe una política de uso de software no autorizado en la que se hace referencia a los derechos de autor. Existe una herramienta que muestra en inventario de software permitido.
15.1.3 Protección de los Registros de la Organización	Los registros se tienen catalogados en la guía de clasificación.
15.1.4 Protección de los Datos y privacidad de la información personal	No existe una política de protección de datos y privacidad de la información personal.
15.1.5 Prevención del uso inadecuado de los servicios de procesamiento de información	Existe una política de uso de recursos tecnológicos.
15.1.6 Reglamentación de los controles criptográficos	N/A
15.2 Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico	
15.2.1 Cumplimiento con la políticas y las normas de seguridad	No se ha realizado una auditoría interna para verificar el cumplimiento.
15.2.2 Verificación del cumplimiento técnico	No se ha realizado una auditoría interna para verificar el cumplimiento.
15.3 Consideraciones de la Auditoría de los Sistemas de Información	
15.3.1 Controles de Auditoría de los sistemas de información	No se ha realizado una auditoría interna.
15.3.2 Protección de las herramientas	No se ha realizado una auditoría.

Tabla 1 - Análisis Diferencial

de auditoría de los SI	

A continuación se muestra un gráfico en el que se refleja porcentualmente el estado de implementación de los controles aplicables:

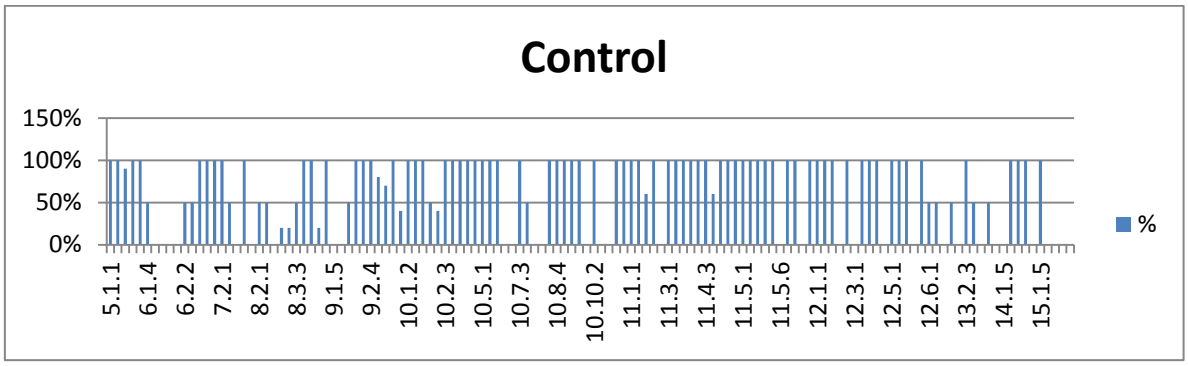

Ilustración 1- Analisis Diferencial

En cuanto a la normativa, la organización cuenta con las siguientes políticas:

POLITICA	REVISDA	APROBADA	DIFUNDIDA
Política de seguridad	SI	SI	SI
Política de uso de recursos tecnológicos.	SI	NO	NO

Tabla 2 - Políticas

2. Fase 2: Sistema de Gestión Documental

1.6 ESQUEMA DOCUMENTAL

POLITICA DE SEGURIDAD:

La política de seguridad se encuentra en el documento Política de seguridad.docx.

PROCEDIMIENTO DE AUDITORÍAS INTERNAS:

El procedimiento para llevar a cabo la auditoría se encuentra en el documento Procedimiento de auditorías internas.docx.

GESTIÓN DE INDICADORES

Los indicadores definidos para medir la eficacia del SGSI se encuentran en el documento gestión de indicadores.docx.

PROCEDIMIENTO REVISIÓN POR DIRECCIÓN

El procedimiento de revisión por la dirección se encuentra en el documento Procedimiento revisión por la dirección.docx

GESTIÓN DE ROLES Y RESPONSABILIDADES

Los roles y responsabilidades están definidas en el documento Gestión de roles y responsabilidades.docx.

METODOLOGÍA DE ANÁLISIS DE RIESGOS

La metodología de análisis de riesgos se encuentra en el documento Metodología de análisis de riesgos.docx.

DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad se podrá encontrar en el documento declaración de aplicabilidad.xlsx

3. Fase 3: Análisis de Riesgos

1.7 RESULTADOS DEL ANÁLISIS DE RIESGOS

IDENTIFICACION Y VALORACION DE ACTIVOS

Inicialmente se identifican todos los activos y se agrupan dependiendo del servicio que prestan. Teniendo en cuenta el alcance definido para el SGSI dichos activos pertenecen a los tipos: físico y de personal únicamente.

El detalle del inventario de activos se encuentra en el documento análisis_de_riesgos.xlsx en la pestaña valoración de activos en la que se define el activo, su responsable y el tipo de activo; esto en cuanto al inventario de activos.

Adicional a esto se realiza la valoración de cada uno de los activos con un método cualitativo en el que se da un valor **Alto**, **medio** y **bajo** dependiendo del grado de **confidencialidad**, **disponibilidad** e **integridad** de dichos activos.

Los resultados de esta valoración se encuentran en el archivo análisis_de_riesgos.xlsx en la pestaña valoración de activos.

También se realizó una valoración de cada activo de forma cuantitativa teniendo en cuenta aspectos como su valor de reposición, configuración, uso de activo y pérdida de oportunidad teniendo en cuenta los rangos que se muestran en la siguiente tabla:

Valoración	Rango	Valor
Muy Alta	Valor > $300.000.000	$400.000.000
Alta	$100.000.000<valor>$300.000.000	$200.000.000
Media	$50.000.000<valor >$ 100.000.000	$75.000.000
Baja	10.000.000 <valor> $50.000.000	$30.000.000
Muy baja	Valor < $10.000.000	$10.000.000

Tabla 3 - Valoración de Activos

IDENTIFICACION DE AMENAZAS

Por otro lado se identificaron las amenazas que pueden afectar los activos entre las cuales encontraron los siguientes tipos de amenaza:

- De entorno,
- Técnicas y
- Causadas por personas.

Dichas amenazas fueron determinadas teniendo en cuenta el alcance del SGSI.

El listado de amenazas identificadas se encuentra en el archivo Analisis_de_Riesgos.xlsx en la pestaña Amenazas.

AMENAZAS/VULNERABILIDADES

El análisis de amenazas se realizó según la probabilidad de ocurrencia (considerado para Magerit como vulnerabilidad), y se determinaron los siguientes valores:

Probabilidad de ocurrencia			
Descripción	**Abreviatura**	**Rango**	**Valor**
Extremadamente frecuente	EF	1 vez al día	1
Muy frecuente	MF	1 vez a la semana	52/365=0,14247
Frecuente	F	1 vez al mes	12/365=0,03288
Poco Frecuente	PF	1 vez cada 6 meses	2/365=0,005478

Muy poco frecuente	MPF	1 vez al año	1/365=0,00273
Despreciable	D	1 vez cada 2 años	0.5/365=0,00137

Tabla 4 - Amenazas vs Vulnerabilidades

El cálculo de este valor se realiza de la siguiente forma: Frecuencia estimada / Días del año.

La probabilidad de ocurrencia de una amenaza para cada activo se ve reflejado en el análisis de riesgos en el documento analisis_riesgos.xlsx en la pestaña Análisis de Riesgos.

IMPACTO

Se calculó el impacto potencial determinando diferentes niveles de impacto a los cuales se les dio un porcentaje como se ve a continuación:

IMPACTO	VALOR
Muy alto	100,00%
Alto	75,00%
Medio	50,00%
Bajo	20,00%
Muy bajo	5,00%

Tabla 5 - Impacto

En donde en caso materializarse una amenaza el impacto podría ser del 5% al 100% de pérdida del valor del activo.

El impacto de la materialización de una amenaza para cada activo se ve reflejado en el análisis de riesgos en el documento analisis_riesgos.xlsx en la pestaña Análisis de Riesgos.

A continuación se calcula el nivel de riesgo basado en el impacto y la frecuencia:

Nivel de riesgo			IMPACTO					
			Despreciable	Muy poco frecuente	Poco Frecuente	Frecuente	Muy frecuente	ente frecuente
			0,00137	0,00273	0,005478	0,03288	0,14247	1
FRECUENCIA	Muy alto	1	0,00137	0,00273	0,005478	0,03288	0,14247	1
	Alto	0,75	0,0010275	0,0020475	0,0041085	0,02466	0,1068525	0,75
	Medio	0,5	0,000685	0,001365	0,002739	0,01644	0,071235	0,5
	Bajo	0,2	0,000274	0,000546	0,0010956	0,006576	0,028494	0,2
	Muy bajo	0,05	0,0000685	0,0001365	0,0002739	0,001644	0,0071235	0,05

Tabla 6 - Nivel de Riesgo

NIVEL DE RIESGO ACEPTABLE

El riesgo aceptable es desde el cual una organización toma la decisión de aplicar o no controles sin que se generen grandes consecuencias. En ese caso el riesgo aceptable es el medio y bajo.

Riesgo aceptable	
Riesgo a tratar	

Tabla 7 - Clasificación de Riesgos

RIESGO RESIDUAL

Se calcula a partir de:

- **Impacto residual:** cuál es el impacto después de aplicar una salvaguarda.

Impacto: valor activo * %impacto
Impacto residual: impacto * (1- %de eficacia salvaguarda)

- **Frecuencia residual:** cuál es la probabilidad después de aplicar una salvaguarda

Frecuencia residual: frecuencia * (1 - % eficacia salvaguarda)

Partiendo de esto el riesgo residual se calcula:

Riesgo residual = impacto residual * frecuencia residual

Los resultados del riesgo residual se ven reflejados en el documento Analisis_riesgos.xls en la pestaña Riesgo residual.

4. Fase 4: Propuestas de Proyectos

1.8 PROPUESTAS

Las propuestas de proyectos están definidas en el documento Analisis_riesgos.xls en la pestaña plan de implementación, allí se definen:

- Controles a aplicar para mitigar los riesgos encontrados
- Riesgos que se mitigan con cada control
- Cuál es su prioridad de aplicación
- Objetivo de aplicarlo
- Actividades a realizar
- Responsables de llevar a cabo las actividades
- Recursos requeridos: físicos, tiempo, etc.
- Presupuesto necesario para su aplicación
- Tiempo requerido para su aplicación
- Porcentaje actual de aplicación del control.

5. Fase 5: Auditoría de Cumplimiento

1.9 EVALUACIÓN DE LA MADUREZ

A continuación se hace una evaluación de madurez de la seguridad con respecto a los 133 controles planteados por la ISO/IEC 27002:2005 basado en el Modelo de Madure de la Capacidad (CMM):

CONTROL	Efectividad
5. Política de Seguridad	90%
5.1 Política de Seguridad de la Información	90%
5.1.1 Documento de la Política de SI	90%

5.1.2 Revisión de la Política de SI	90%
6. Organización de la SI	90%
6.1 Organización Interna	90%
6.1.1 Compromiso de la dirección con la seguridad de la información	90%
6.1.2 Coordinación de la Seguridad de la Información	90%
6.1.3 Asignación de Responsabilidades para la Seguridad de la Información	90%
6.1.4 Proceso de Autorización para los Servicios	50%
6.1.5 Acuerdos sobre Confidencialidad	10%
6.1.6 Contacto con las Autoridades	0%
6.1.7 Contacto con Grupos de Interés Especiales	0%
6.1.8 Revisión Independiente de la SI	N/A
6.2 Partes Externas	50%
6.2.1 Identificación de los Riesgos	90%
6.2.2 Seguridad con los Clientes	10%
6.2.3 Seguridad en los Acuerdos con Terceras Partes	10%
7. Gestión de Activos	90%
7.1 Responsabilidad por los Activos	90%
7.1.1 Inventario de Activos	90%
7.1.2 Propietario de los Activos	90%
7.1.3 Uso Aceptable de los Activos	50%
7.2 Clasificación de la Información	90%
7.2.1 Directrices de Clasificación	50%
Se está trabajando en conjunto con gestión documental para rotular la información.	50%
8. Seguridad de los Recursos Humanos	50%
8.1 Antes de la Contratación Laboral	50%
8.1.1 Roles y Responsabilidades	10%
8.1.2 Selección	90%
8.1.3 Términos y Condiciones Laborales	0%
8.2 Durante la Vigencia del Contrato	50%
8.2.1 Responsabilidades de la dirección	50%
8.2.2 Educación, formación y concientización sobre SI	50%
8.2.3 Proceso Disciplinario	10%

8.3 Terminación o Cambio de la Contratación	50%
8.3.1 Responsabilidades en la Terminación	10%
8.3.2 Devolución de Activos	10%
8.3.3 Retiro de los Derechos de Acceso	50%
9. Seguridad Física y del Entorno	90%
9.1 Áreas Seguras	90%
9.1.1 Perímetro de Seguridad Física	100%
9.1.2 Controles de Acceso Físico	90%
9.1.3 Seguridad de Oficinas, Recintos e Instalaciones	90%
9.1.4 Protección contra Amenazas Externas y Ambientales	90%
9.1.5 Trabajo en Áreas Seguras	90%
9.1.6 Áreas de Carga, despacho y acceso público	90%
9.2 Seguridad de los Equipos	90%
9.2.1 Ubicación y Protección de los Equipos	90%
9.2.2 Servicios de Suministro	100%
9.2.3 Seguridad del Cableado	100%
9.2.4 Mantenimiento de los Equipos	90%
9.2.5 Seguridad de los Equipos Fuera de las Instalaciones	50%
9.2.6 Seguridad en la Reutilización o Eliminación de los Equipos	50%
9.2.7 Retiro de Activos	90%
10. Gestión de Comunicaciones y Operaciones	90%
10.1 Procedimientos Operacionales y Responsabilidades	90%
10.1.1 Documentación de los procedimientos de operación	50%
10.1.2 Gestión del Cambio	100%
10.1.3 Distribución (segregación) de funciones	90%
10.1.4 Separación de las instalaciones de Desarrollo, ensayo y operación	90%
10.2 Gestión de la Prestación del Servicio por Terceras Partes	50%
10.2.1 Prestación del Servicio	50%
10.2.2 Monitoreo y revisión de los servicios por terceros	50%
10.2.3 Gestión de los Cambios en los servicios por terceras partes	90%

10.3 Planificación y Aceptación del Sistema	90%
10.3.1 Gestión de la Capacidad	90%
10.3.2 Aceptación del Sistema	90%
10.4 Protección Contra Códigos Maliciosos y Móviles	50%
10.4.1 Controles contra códigos maliciosos	50%
10.4.2 Controles contra códigos móviles	90%
10.5 Respaldo	90%
10.5.1 Respaldo de la Información	90%
10.6 Gestión de la Seguridad de las Redes	90%
10.6.1 Controles de las Redes	90%
10.6.2 Seguridad de los servicios de la red	90%
10.7 Manejo de los Medios	50%
10.7.1 Gestión de los Medios Removibles	0%
10.7.2 Eliminación de los Medios	0%
10.7.3 Procedimientos para el Manejo de la Información	90%
10.7.4 Seguridad de la Documentación del Sistema	50%
10.8 Intercambio de la Información	50%
10.8.1 Políticas y Procedimientos para el Intercambio de Información	0%
10.8.2 Acuerdos para el intercambio	0%
10.8.3 Medios Físicos en tránsito	90%
10.8.4 Mensajería Electrónica	90%
10.8.5 Sistemas de Información del Negocio	90%
10.9 Servicios de Comercio Electrónico	90%
10.9.1 Comercio Electrónico	N/A
10.9.2 Transacciones en Línea	90%
10.9.3 Información disponible al público	90%
10.10 Monitoreo	50%
10.10.1 Registro de Auditorías	10%
10.10.2 Monitoreo del uso del Sistema	90%
10.10.3 Protección de la Información del Registro	10%

10.10.4 Registros del Administrador y del Operador	10%
10.10.5 Registro de Fallas	100%
10.10.6 Sincronización de Relojes	90%
11. Control de Acceso	90%
11.1 Requisitos del Negocio para el Control del Acceso	90%
11.1.1 Política de Control de Acceso	100%
11.2 Gestión del Acceso a Usuarios	50%
11.2.1 Registro de Usuarios	100%
11.2.2 Gestión de Privilegios	50%
11.2.3 Gestión de Contraseñas para Usuarios	50%
11.2.4 Revisión de los Derechos de Acceso de los Usuarios	0%
11.3 Responsabilidades de los Usuarios	90%
11.3.1 Uso de Contraseñas	50%
11.3.2 Equipo de Usuario Desatendido	100%
11.3.3 Política de Escritorio Despejado y de Pantalla Despejada	100%
11.4 Control de Acceso a las Redes	90%
11.4.1 Política de uso de los servicios de red	100%
11.4.2 Autenticación de Usuarios para Conexiones Externas	100%
11.4.3 Identificación de los Equipos en las Redes	90%
11.4.4 Protección de los puertos de configuración y diagnóstico remoto	50%
11.4.5 Separación en las Redes	100%
11.4.6 Control de Conexión a las redes	100%
11.4.7 Control de Enrutamiento en la Red	100%
11.5 Control de Acceso al Sistema Operativo	90%
11.5.1 Procedimientos de Registro de Inicio Seguro	90%
11.5.2 Identificación y Autenticación de Usuarios	100%
11.5.3 Sistema de Gestión de Contraseñas	90%
11.5.4 Uso de las utilidades del sistema	90%
11.5.5 Tiempo de Inactividad de la Sesión	100%

11.5.6 Limitación del tiempo de Conexión	10%
11.6 Control de Acceso a las Aplicaciones y a la Información	90%
11.6.1 Restricción de acceso a la Información	50%
11.6.2 Aislamiento de sistemas sensibles	100%
11.7 Computación Móvil y Trabajo Remoto	50%
11.7.1 Computación y comunicaciones móviles	0%
11.7.2 Trabajo Remoto	100%
12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	90%
12.1 Requisitos de Seguridad de los Sistemas de Información	90%
12.1.1 Análisis y especificación de los requisitos de seguridad	90%
12.2 Seguridad de las aplicaciones del sistema	50%
12.2.1 Validación de los datos de entrada	90%
12.2.2 Control de Procesamiento Interno	90%
12.2.3 Integridad del Mensaje	0%
12.2.4 Validación de los datos de salida	90%
12.3 Controles Criptográficos	50%
12.3.1 Política sobre el uso de controles criptográficos	0%
12.3.2 Gestión de Claves	90%
12.4 Seguridad de los Archivos del Sistema	50%
12.4.1 Control del Software Operativo	50%
12.4.2 Protección de los datos de prueba del sistema	90%
12.4.3 Control de acceso al código fuente de los programas	0%
12.5 Seguridad en los procesos de desarrollo y soporte	90%
12.5.1 Procedimientos de control de cambios	90%
12.5.2 Revisión Técnica de las aplicaciones después de los cambios en el SO	90%
12.5.3 Restricciones en los cambios a los paquetes de software	90%
12.5.4 Fuga de información	0%

12.5.5 Desarrollo de software contratado externamente	90%
12.6 Gestión de la Vulnerabilidad Técnica	90%
12.6.1 Control de las Vulnerabilidades Técnicas	90%
13. Gestión de los Incidentes de la Seguridad de la Información	50%
13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información	50%
13.1.1 Reporte sobre los eventos de seguridad de la información	50%
13.1.2 Reporte sobre las debilidades en la seguridad	50%
13.2 Gestión de los Incidentes y las mejoras en las SI	50%
13.2.1 Responsabilidades y Procedimientos	50%
13.2.2 Aprendizaje debido a los incidentes de SI	0%
13.2.3 Recolección de Evidencias	50%
14. Gestión de la Continuidad del Negocio	50%
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio	50%
14.1.1 Inclusión de la SI en el proceso de gestión de la continuidad del negocio	50%
14.1.2 Continuidad del Negocio y evaluación de riesgos	0%
14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la SI	10%
14.1.4 Estructura para la Planificación de la continuidad del negocio	0%
14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	0%
15. Cumplimiento	90%
15.1 Cumplimiento de los Requisitos Legales	90%
15.1.1 Identificación de la Legislación Aplicable	90%
15.1.2 Derechos de Propiedad Intelectual	90%
15.1.3 Protección de los Registros de la Organización	90%
15.1.4 Protección de los Datos y privacidad de la información personal	0%

15.1.5 Prevención del uso inadecuado de los servicios de procesamiento de información	90%
15.1.6 Reglamentación de los controles criptográficos	N/A
15.2 Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico	0%
15.2.1 Cumplimiento con la políticas y las normas de seguridad	0%
15.2.2 Verificación del cumplimiento técnico	0%
15.3 Consideraciones de la Auditoría de los Sistemas de Información	0%
15.3.1 Controles de Auditoría de los sistemas de información	0%
15.3.2 Protección de las herramientas de auditoría de los SI	0%

Tabla 8 - Evaluación de Madurez

1.10 PRESENTACIÓN DE RESULTADOS

A continuación se muestran los resultados de la evaluación de madurez en términos porcentuales con la finalidad de conocer el estado de seguridad de la organización:

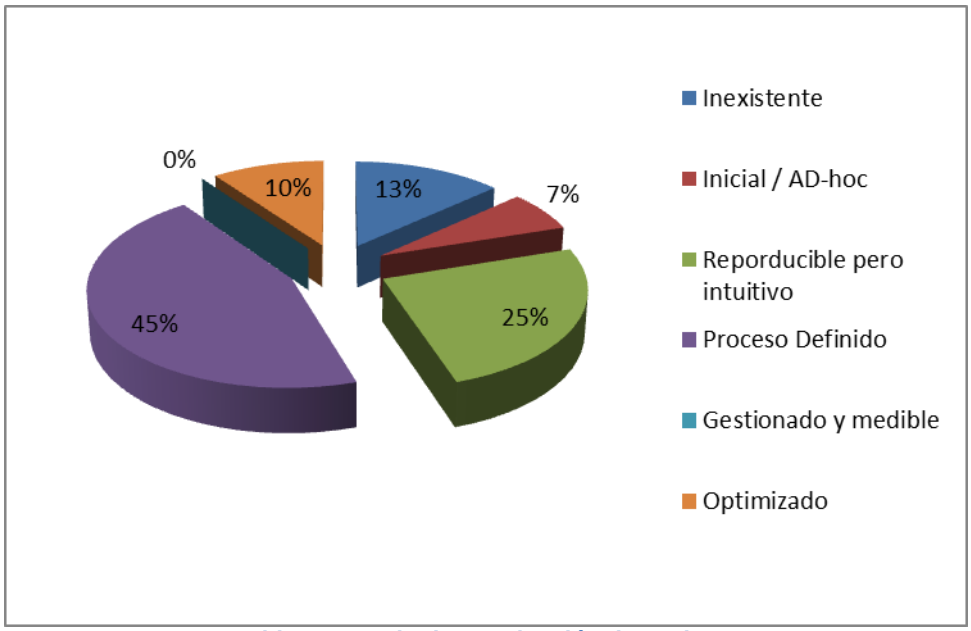

Tabla 9 - Resultados Evaluación de Madurez