UNIVERSIDAD ABIERTA DE CATALUÑA
MASTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TIC
TRABAJO DE FINAL DE MASTER
SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

PLAN MAESTRO PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN
BASADO EN LA NORMA NTC - ISO/IEC 27001:2013

HÉCTOR ANDRÉS MAFLA TRUJILLO

DIRECTOR:
ANTONIO JOSÉ SEGOVIA HENARES

Junio 2018

Plan Maestro para la Implementación de un Sistema de Gestión de Seguridad de la Información

Basado en la norma NTC - ISO/IEC 27001:2013

Carrera 13 # 33 – 01
Bogotá, D.C.
p. 555-8056
w. 300-5559743
servicio_cliente@manejodeobras.gov.co
www.manejodeobras.gov.co

Tabla de contenido

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

0. Normas de referencia

Para el presente trabajo se han elegido como referencia, las normas técnicas colombianas NTC – ISO/IEC 27001:2013 y GTC – ISO/IEC 27002:2015, las cuales son idénticas por traducción (IDT) a la ISO/IEC 27001:2013 e ISO 27002:2013 respectivamente. Lo anterior por la facilidad para su consecución en mi país, Colombia.

Es bien sabido que las normas más conocidas, las que más se siguen como referencia para implementar sistemas de gestión de seguridad de la información son las ISO de la familia 27000. De ellas la 27001 que es certificable, pues define los requisitos para que un tercero audite y de fe, de que un sistema en particular los cumple.

De la mano de ella, se presenta otra norma, que no es certificable, pues se ha considerado como un código de buenas prácticas, está la norma ISO/IEC 27002:2014.

A continuación, una síntesis de lo que ha sido la historia de las dos normas:

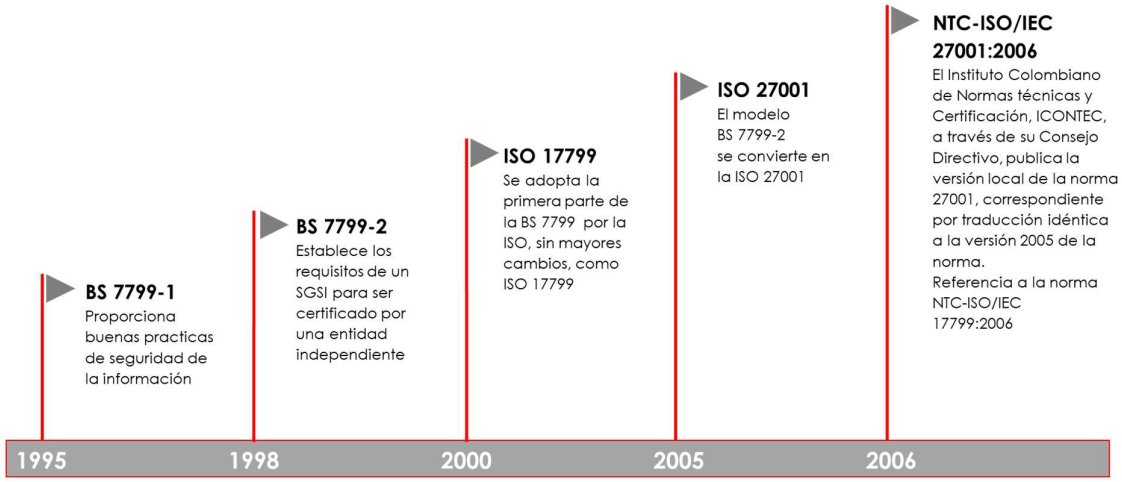


Ilustración 1. Historia de las normas de referencia. Parte 1. Fuente: Propia.

Para el caso de la versión colombiana de la norma 27002, ha sido catalogada como Guía Técnica y fue publicada en 2015. Sin embargo, como se manifestó previamente, es una traducción idéntica de la norma ISO/IEC 27002:2014

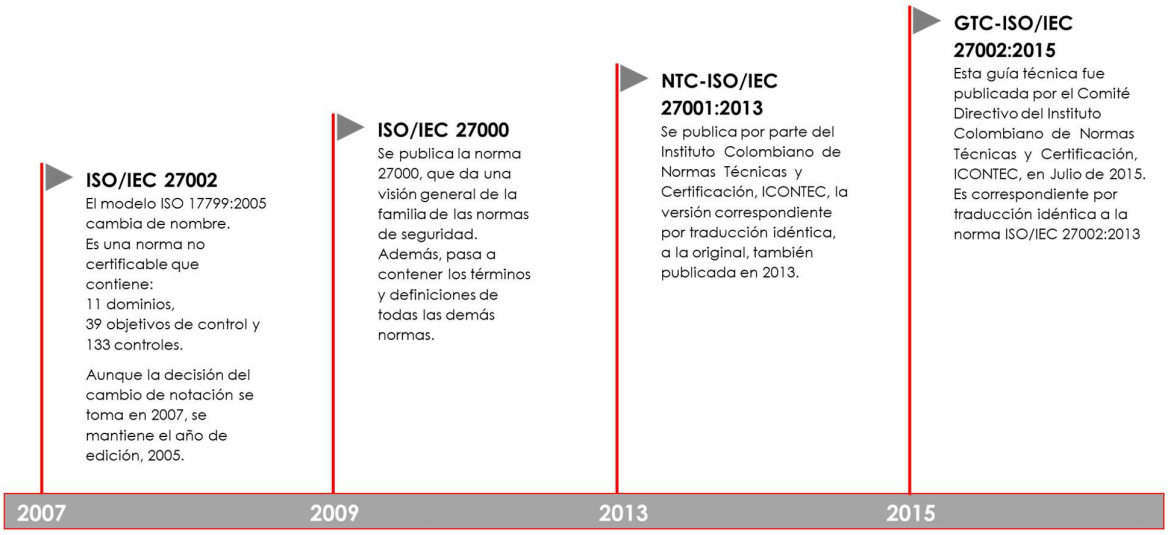


Ilustración 2. Historia de las normas de referencia. Parte 2. Fuente: Propia.

1. Situación actual

En este apartado se presenta una breve descripción de la Empresa de Manejo de Obras, su objeto social, una breve descripción de su plataforma de T.I. y un análisis diferencial del estado de la Empresa frente a las normas NTC - ISO/IEC 27001:2013 y 27002:2015.

1.1. Contextualización

La Empresa de Manejo de Obras fue creada mediante el Acuerdo 56 de 1972 del Concejo Distrital. Tiene como misión "Generar bienestar en los habitantes de la ciudad mejorando la calidad de vida, mediante el desarrollo de infraestructura para el transporte, contribuyendo a la construcción de una ciudad incluyente, sostenible y moderna".

La Empresa hoy está conformada por 493 trabajadores, entre contratistas y empleados de carrera administrativa.

Se encuentra ubicada en la ciudad de Bogotá, D.C., en la Calle del Churo # 13-44.

La estructura jerárquica es la siguiente:

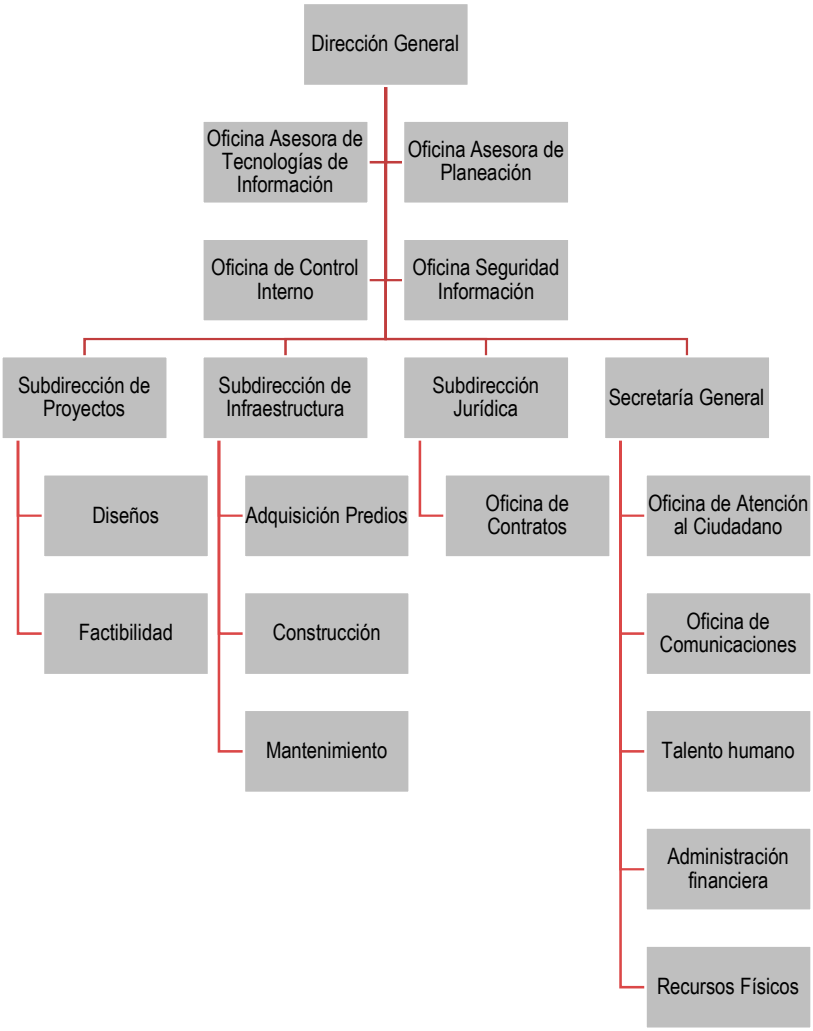


Ilustración 3. Organigrama de la Empresa. Fuente: propia

La Empresa de Manejo de Obras tiene la siguiente plataforma tecnológica:

- Un (1) Centro de Procesamiento de Datos – CPD
  - Un (1) sistema de aire acondicionado de precisión en alta disponibilidad
  - Un (1) sistema de detección y extinción de fuego, basado en gas FM200
  - Dos (2) UPS (Sistema de alimentación ininterrumpida de energía eléctrica)
- 50 servidores físicos:
  - 20 con Windows Server 2012
  - 10 con Linux Ubuntu Server
  - 20 Servidores para virtualización
- 60 Servidores virtuales
  - 20 servidores para producción de algunos S.I desarrollados internamente
  - 20 servidores para desarrollo
  - 20 servidores para pruebas

- Dos (2) switches de Core
- Cuatro (4) switches Top of Rack (ToR)
- 10 switches de borde
- Dos (2) canales de internet (1 principal + 1 de respaldo)
- Una (1) solución de almacenamiento SAN
- Una solución de backup, con software Veritas
- Un (1) RAC de base de datos Oracle
- Siete (7) Sistemas de información
  - Un S.I. de inteligencia de negocio (BI)
  - Un ERP (Sistema administrativo y financiero + Personal y nómina + Almacén)
  - Un S.I. para gestión de proyectos de obra
  - Un CMS
  - Un S.I. para gestión de planes de mejoramiento
  - Un S.I para gestión de activos de información
  - Un S.I de gestión documental.
- Seguridad perimetral

  Un firewall Fortinet en alta disponibilidad, con los módulos:
  - Fortigate,
  - Fortianalyzer y
  - FortiSandbox
- Un antivirus corporativo para "endpoint" de siguiente generación

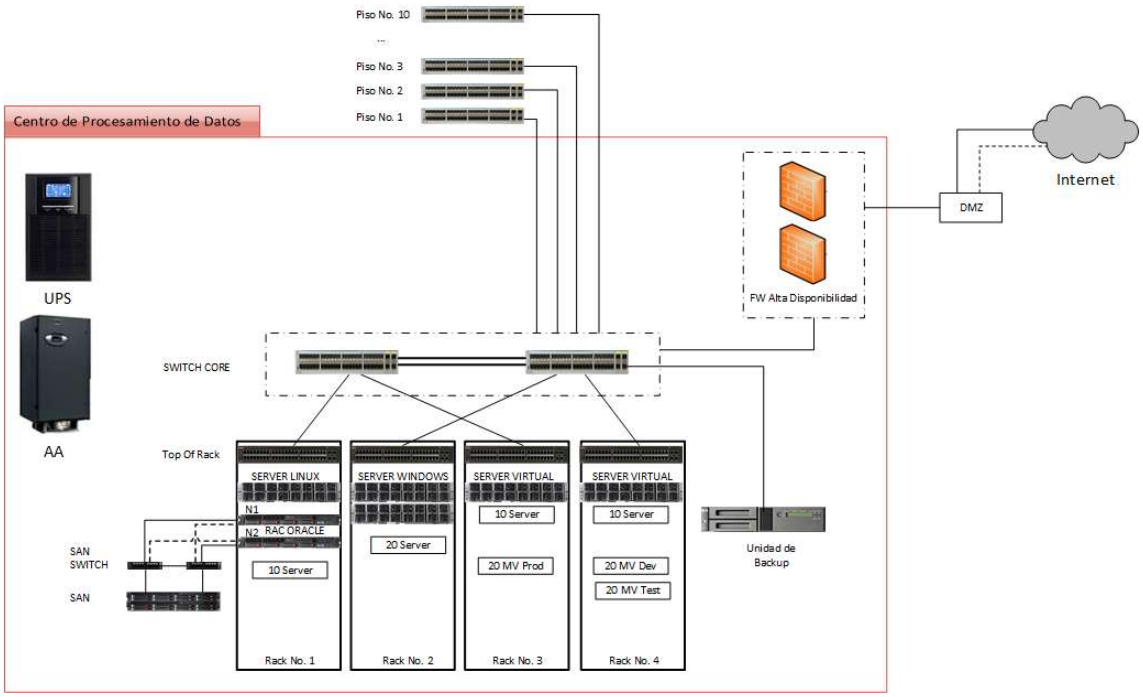


Ilustración 4. Diagrama de red a alto nivel. Fuente: Propia.

1.2. Alcance

El Sistema de Gestión de Seguridad de la Información de la Empresa de Manejo de Obras, cubrirá todos sus procesos, se ejecutará la sede principal. Aplicará a los servidores públicos, contratistas de apoyo a la gestión, terceros que prestan servicios y demás usuarios que accedan a la información institucional.

1.3. Objetivos

1.3.1. General

Definir y desarrollar un plan maestro para la implementación de un sistema de gestión de seguridad de la información, para que sea un punto de referencia en el aseguramiento de la confidencialidad, integridad y disponibilidad de la información necesaria para el desarrollo de los proyectos.

1.3.2. Específicos

- Analizar el estado actual del SGSI de la Empresa de Manejo de Obras.
- Definir y elaborar los documentos necesarios para la operación del SGSI.
- Aplicar la metodología de riesgos definida sobre los activos identificados.
- Definir proyectos que permitan el tratamiento de los riegos hacia su mitigación.
- Medir el cumplimiento del SGSI mediante una auditoría.

2. Análisis diferencial

Este tipo de análisis es muy útil cuando se requiere conocer el estado actual de algo, frente a un punto de comparación; en este caso, se pretende conocer cuál es el estado actual del sistema de gestión de seguridad de la información de la Empresa de Manejo de Obras; sus puntos de comparación son la norma técnica colombiana NTC – ISO/IEC 27.001:2013 y la guía técnica colombiana NTC – ISO/IEC 27.002:2015.

Otro punto muy importante de un análisis diferencial, es que permite identificar la brecha existente entre el estado actual y el punto de comparación, para que una vez se cuente con ella, se pueda definir un plan de acción u hoja de ruta a seguir para cumplir con el propósito inicial, que para efectos prácticos es el mismo punto de comparación mencionado en el párrafo previo.

A continuación, se presenta este análisis en dos subcapítulos separados.

2.1. Análisis diferencial NTC - ISO/IEC 27001:2013

Para realizar el análisis diferencial, se tomó un modelo realizado internamente, que permite mediante la calificación de 3 criterios, identificar el nivel de cumplimiento de cada requerimiento de la norma de referencia. Estos criterios y sus correspondientes valores son:

- ¿Existe mecanismo que lo implementa?
  - No 0%

- Si 30%
- ¿Se aplica?
  - Nunca 0%
  - Algunas veces 20%
  - Siempre 40%
- ¿Genera resultados?
  - No 0%
  - Si 30%

Entonces:

si el requerimiento tiene un control que lo implementa:	30%
si el control se aplica siempre:	40%
y, si genera resultados:	30%
TOTAL	100%

Por el contrario, si el requerimiento no tiene un mecanismo que lo implementa, este se califica en cero (0), es decir, los otros criterios no son tenidos en cuenta.

Asimismo, si el requerimiento tiene un mecanismo que lo implementa, pero nunca es aplicado, este se califica en 30% y no se tiene en cuenta el criterio "¿Genera resultados?". Sin embargo, si el mecanismo que lo implementa se aplica algunas veces, se suman 30% por la existencia del mecanismo y 20% por el criterio de aplicación, dando un valor del 50% para dicho requerimiento. En este punto, sí se tiene en cuenta el valor del criterio "¿Genera resultados?", que si es no, no sumará al porcentaje del requerimiento, pero si por el contrario sí genera resultados, se le suma el 30% de este criterio al 50% previo, por lo tanto el total sería 80%.

En la siguiente tabla se muestran las posibles combinaciones de los criterios de valoración de los requerimientos y su calificación total, siempre y cuando haya un mecanismo que implemente el control, pues como ya se explicó, si no existe dicho mecanismo, la calificación total es cero (0):

¿Existe mecanismo que lo implementa?	¿Se aplica?	¿Genera Resultados?	Porcentaje de cumplimiento
Si	Nunca	No	30
Si	Nunca	Si	30
Si	Algunas veces	No	50
Si	Algunas veces	Si	80
Si	Siempre	No	70
Si	Siempre	Si	100

Tabla 1. Criterios de valoración de los requerimientos de la norma. Fuente: Propia.

Una vez explicada la metodología de evaluación del análisis diferencial, o análisis de brechas, se presenta el resumen del diagnóstico realizado en la siguiente tabla.

RESUMEN ANÁLISIS DIFERENCIAL NTC – ISO/IEC 27.001		
Numeral	**Requisito a cumplir**	**Porcentaje de cumplimiento**
4	Contexto de la organización	100
5	Liderazgo	68
6	Planificación	86
7	Soporte	80
8	Operación	80
9	Evaluación del desempeño	60
10	Mejora	86
	Porcentaje de implementación del SGSI:	80

Tabla 2. Resumen del análisis diferencial del SGSI frente a la norma de referencia. Fuente: Propia

Nota: En la columna porcentaje de cumplimiento se pueden encontrar valores distintos a los mostrados en la tabla 1, pues al ser un resumen de todos los criterios, se toma como promedio por cada numeral de la norma.

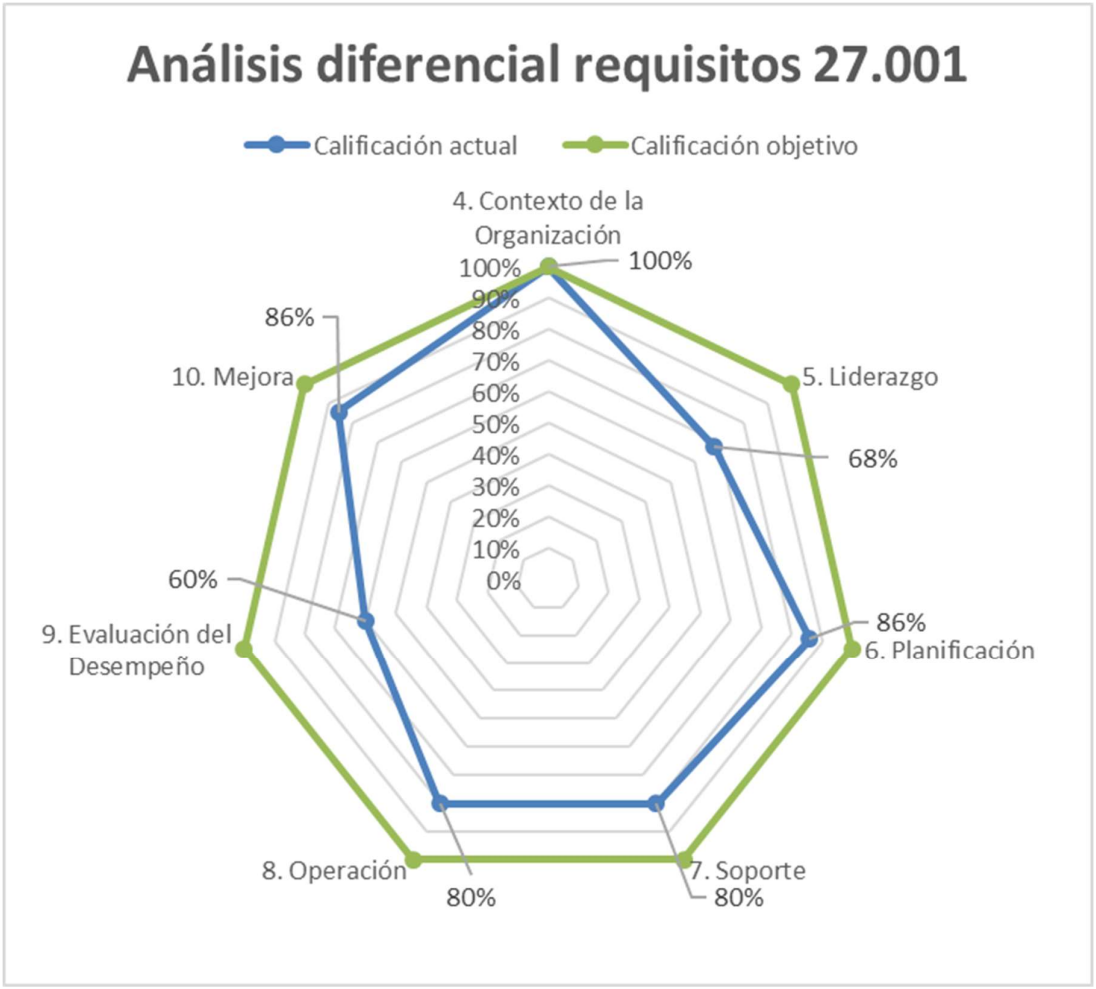


Ilustración 5. Análisis diferencial frente a los requisitos de la norma NTC - ISO/IEC 27.001. Fuente: Propia

2.2. Análisis diferencial GTC - ISO/IEC 27002:2015

Para este análisis se empleó un instrumento similar al mencionado previamente, para el análisis de la norma certificable. A continuación, se presentan los criterios y los posibles valores:

- Estado (de implementación)
  - Sin implementar 0%
  - Iniciado 10%
  - Parcialmente Implementado 20%
  - Totalmente Implementado 40%
- ¿Se aplica?
  - Nunca 0%
  - Algunas Veces 20%
  - Siempre 40%
- ¿Genera resultados?
  - No 0%
  - Sí 20%

Entonces:

si el control está totalmente implementado:	40%
si el control se aplica siempre:	40%
y, si genera resultados:	20%
TOTAL	100%

Para este análisis, también se tuvo en cuenta el valor de los criterios "Estado" y "¿Se aplica?", de manera que si el control no está implementado (Estado), la calificación es cero (0), y no se tienen en cuenta los otros dos criterios. Si el control está en estado iniciado, el control se califica con 10% de este criterio más el 10% del valor del criterio ¿se aplica? y no se tiene en cuenta el criterio "¿genera resultado?". Si el control está en estado "Parcialmente implementado", su calificación será 20% más el 20% del valor del criterio "¿se aplica?" más el 20% del valor del criterio "¿genera resultados?". Finalmente, si el control está Totalmente implementado, los demás criterios toman su valor pleno.

A continuación, en la tabla 3 se presenta el resumen del análisis diferencial de la implementación de los controles sugeridos por la Guía Técnica GTC – ISO/IEC 27.002.

RESUMEN ANÁLISIS DIFERENCIAL GTC – ISO/IEC 27.002			
Numeral	**Nombre Dominio**	**Cumplimiento por dominio**	**Promedio cumplimiento de los 114 controles**
A.5	Políticas de seguridad de la información	100%	**55%**
A.6	Organización de la seguridad de la información	48%	
A.7	Seguridad de los recursos humanos	38%	
A.8	Gestión de activos	68%	
A.9	Control de acceso	73%	

RESUMEN ANÁLISIS DIFERENCIAL GTC – ISO/IEC 27.002			
Numeral	**Nombre Dominio**	**Cumplimiento por dominio**	**Promedio cumplimiento de los 114 controles**
A.10	Criptografía	60%	
A.11	Seguridad física y del entorno	87%	
A.12	Seguridad de las operaciones	62%	
A.13	Seguridad de las comunicaciones	69%	
A.14	Adquisición, desarrollo y mantenimiento de sistemas	41%	
A.15	Relación con los proveedores	29%	
A.16	Gestión de incidentes de seguridad de la información	23%	
A.17	Aspectos de seguridad de la información de la gestión de continuidad de negocio	7%	
A.18	Seguridad de las comunicaciones	72%	

Tabla 3. Resumen análisis diferencial frente a la Guía Técnica GTC – ISO/IEC 27.002. Fuente: propia.

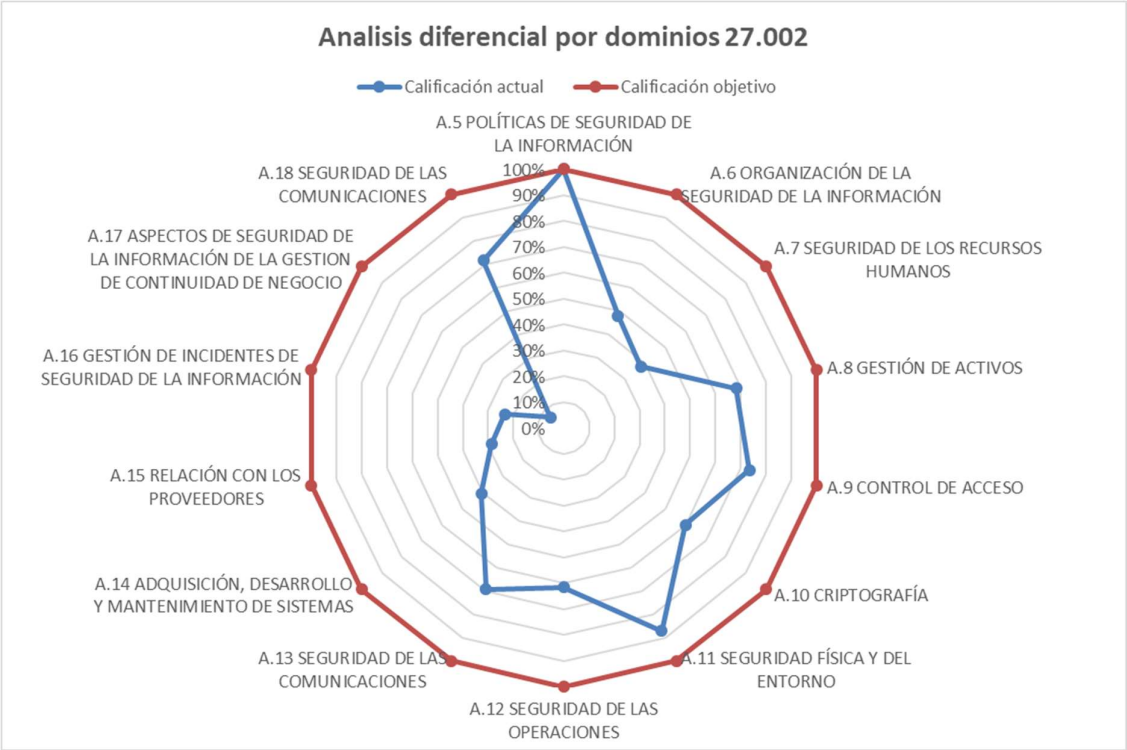


Ilustración 6. Análisis diferencial frente a los requisitos de la guía GTC - ISO/IEC 27.002. Fuente: Propia.

En el **anexo 1** se presenta el análisis detallado de todos los controles de la norma. En este archivo, el análisis se presenta en 2 hojas de contenido, una para el estándar certificable NTC – ISO/IEC 27001:2013 y otra para los controles sugeridos por Guía Técnica Colombiana GTC-ISO/IEC 27002: 2015. En el archivo anexo se incluye una hoja llamada "Portada", que presenta un resumen del análisis, para que en caso de que un lector desprevenido tenga acceso solamente a ese documento, pueda tener un panorama general del estado del SGSI de la Empresa.

2.3. Conclusiones del análisis diferencial

Se puede observar, tanto en la tabla 2 como en la ilustración 2, que el SGSI de la Empresa de Manejo de Obras, tiene un buen nivel de cumplimiento de los requisitos de la norma 27.001. Sin embargo, en los numerales 5 (Contexto de la organización) y 9 (Evaluación del desempeño) se presenta un desfase significativo, pues el numeral 5 está evaluado en 68% y el 9 en 60%. En este sentido, las tareas del plan de acción deberán estar enfocadas a mejorar el cumplimiento de estos requisitos.

Asimismo, los requisitos soporte y operación, están calificados en 80% por lo que también se hace necesario definir tareas para ajustar su cumplimiento.

Finalmente, frente a los requisitos planificación y mejora, que se encuentran en un 86% de avance, deben continuar su implementación para lograr llegar al 100%, por lo que se requiere definir tareas específicas en el plan de acción que estén orientadas a ello.

En el documento anexo, se incluyó también una hoja electrónica que servirá como plantilla para la elaboración del plan de acción y seguimiento.

3. Gestión Documental

Para la Empresa de Manejo de Obras, es claro que uno de los elementos importantes del SGSI es la documentación de las Políticas, Manuales de Gestión, Procedimientos, Guías, Instructivos y Formatos. A continuación, se presentan los documentos que la Empresa ha elaborado, y más adelante los que están pendientes por elaborar.

3.1. Política General de Seguridad

La Empresa de Manejo de Obras se compromete a generar las condiciones de seguridad necesarias en términos de confidencialidad, integridad y disponibilidad adecuadas a la información que ella produce y maneja, en todos sus medios de conservación y divulgación, con los recursos asignados para administrar de forma efectiva los riesgos asociados a sus activos de información, aumentar la credibilidad y confianza de las partes interesadas, implementar estrategias para el mejoramiento continuo y cumplir con la normatividad vigente.

Esta política fue adoptada mediante la resolución interna 34113 de 2015.

3.2. Política de Seguridad

La Empresa de Manejo de Obras ha adoptado las políticas obligatorias de seguridad de la información mediante la resolución 34217 de 2015, la cual puede ser consultada en el anexo 2 Políticas Seguridad de la Información. Estas políticas son de obligatorio cumplimiento por todos los colaboradores de la Empresa, tanto trabajadores de carrera administrativa,

contratistas de apoyo a la gestión, contratistas de obra, como terceros vinculados por outsourcing.

3.3. Procedimiento de Auditorías Internas

En la Empresa de Manejo de Obras, el procedimiento de auditoría interna se viene ejecutando desde 2014, y en él se describen los pasos que la Oficina de Control Interno debe seguir para realizar auditorías de primera parte, además de definir una serie de políticas operativas para desarrollar esta labor, tal como la independencia de los auditores, las instancias que deben aprobar el programa anual de auditoría, la obligación de definir un plan para cada ejercicio de auditoría que se realice, que la actuación de los auditores deberá estar en marcada dentro de los principios y valores establecidos en el código de ética y que para los ejercicios de auditoría el enfoque estará basado en evidencias, entre otros.

El documento del procedimiento en cuestión, se encuentra en el Anexo 3 Procedimiento Auditorías Internas.

3.4. Gestión de Indicadores

Los indicadores del Sistema de Gestión de Seguridad de la Información, de la Empresa de Manejo de Obras se gestionan con el documento DU-PE-01, el cual se puede consultar en el anexo 4 Metodología Indicadores. En él básicamente se encuentran dos (2) secciones, una llamada definición e identificación de indicadores, y otra llamada seguimiento. En la primera se encuentran campos como:

- Número: Es un ordinal de la tabla de indicadores
- Control asociado: Se refiere al número y texto descriptivo del control al cual se está haciendo seguimiento mediante este indicador.
- Nombre indicador: Indica a qué se refiere el indicador.
- Objetivo: Qué se quiere medir con el indicador.
- Tipo: Podrá ser uno de estos valores eficacia, eficiencia o efectividad.
- Fórmula: Se refiere a la fórmula con la cual se calculará el indicador.
- Fuente de datos: De donde se toma la información para el reporte del indicador.
- Unidad de medida: Hace referencia a la Unidad en la cual está dado el valor final del indicador.
- Frecuencia de medición: Cada cuanto se medirá un indicador. Se puede dar caso de tener un indicador "no periódico".
- Meta anual: Es el valor programado para cada año del indicador.
- Responsable: Es el rol del responsable de reportar la medición del indicador.

En la sección de seguimiento se reporta el valor de cada indicador al momento del corte, de acuerdo con la periodicidad de su medición y se contrasta contra el valor planeado.

3.5. Procedimiento Revisión por Dirección

"La Alta Dirección debe revisar el SGSI de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacias continuas."[1]

Para ello se ha elaborado el procedimiento revisión por la dirección, que define los pasos que se deben llevar a cabo para que el representante de la Dirección General realice una reunión de forma programada, donde se presentará el estado del Sistema de Gestión de Seguridad de la Información a los demás directivos que conforman la "Alta Dirección", se analizarán sus oportunidades de mejora. El principal producto de este procedimiento es el informe de la revisión, el cual se tendrá que conservar como registro.

Este procedimiento se encuentra en el anexo 5 Procedimiento Revisión Por la Dirección.

3.6. Gestión de Roles y Responsabilidades

En la Empresa de Manejo de Obras, el Sistema de Gestión de la Seguridad de la información está conformado por todos sus funcionarios y contratistas, y desde la Dirección General hasta el más bajo de los cargos asistenciales, tiene una responsabilidad frente al Sistema. Estas se reflejan en la Guía de Roles y Responsabilidades Frente al SGSI, que puede ser consultada en el Anexo 6a Guía de Roles y responsabilidades frente al SGSI.

3.7. Metodología de Análisis de Riesgos

Para la Empresa de Manejo de Obras, la gestión de los riesgos se realiza bajo la metodología del Departamento Administrativo de la Función Pública, de Colombia, la cual está basada en el estándar ISO 31000. Para más detalles, se pueden consultar los anexos: Anexo 7a DocumentoPolíticaAdministracióndelRiesgo y Anexo 7b ManualAdministracióndelRiesgo.

3.8. Declaración de Aplicabilidad

La Declaración de Aplicabilidad para Empresa de Manejo de Obras es más que una simple lista de controles aplicados o por aplicar. Es una manera de tener bajo control las medidas de seguridad implementadas y aquellas que están en proceso de implementación.

Para conocer más en detalle este documento, se pueden consultar los anexos: Anexo 8a Resolución Declaración de Aplicabilidad SGSI y Anexo 8b Declaración de Aplicabilidad.

[1] Norma técnica colombiana NTC-ISO-IEC 27001:2013. Numeral 9.3 Revisión por la dirección

4. Análisis de Riesgos

El análisis de riesgos es la etapa en la administración del riesgo para comprender la naturaleza del riesgo y determinar su nivel[2], mediante un proceso sistemático, que ha sido definido en el Manual de Administración del Riesgo [ver. Anexo 7b].

Como muchos sistemas de gestión, el SGSI de La Empresa de Manejo de Obras se basa en el análisis de riesgos para poder definir planes y proyectos que permitan la protección de la información. Para ello es indispensable la identificación de sus activos de información o activos organizacionales.

4.1. Inventario de Activos Organizacionales

Un activo es "todo tipo de elemento que requiere la organización para poder realizar las actividades de negocio que le son propias."[3]

Es una buena práctica agrupar los activos organizacionales para facilitar su tratamiento, para el presente plan se consideran los siguientes tipos de activos: Instalaciones (I), Hardware(HW), Software (Sw), Datos (D), Red (R), Servicios (S), Equipamiento auxiliar (Aux), Personal (P). En la siguiente tabla se presenta el inventario de activos organizacionales, agrupados de acuerdo con la tipificación anterior.

Tabla 4. Inventario de activos - (D)Datos. Fuente: propia.

INVENTARIO DE ACTIVOS – TIPO: DATOS						
CODIGO	**NOMBRE DEL ACTIVO**	**CANT**	**DESCRIPCIÓN**	**DEPENDENCIA ENTRE ACTIVOS**	**PROPIETARIO**	**TIPO DE ACTIVO**
(D.01)	Configuración fortigate	1	Reglas o políticas de configuración y filtrado del firewall	(HW.06)	Oficina TI	Datos
(D.03)	Configuración antivirus	1	Reglas o políticas de configuración del antivirus	(SW.13)	Oficina TI	Datos
(D.04)	Código fuente de los sistemas de información	4	Código fuente de las aplicaciones desarrolladas internamente, al cual se le hace un control de versiones	(D.05) - (SW.01)	Oficina TI	Datos
(D.05)	Licenciamiento software comercial	1	Documentación digital y electrónica que permite el uso de software adquirido	(I.05)	Oficina TI	Datos
(D.06)	hojas de vida de los empleados		Curriculum vitae de los empleados	(SW.05)	Talento Humano	Datos
(D.07)	Archivo físico no digitalizado		Documentación variada que aún no ha sido digitalizada.	(Aux.04) – (I.06)	Recursos físicos	Datos
(D.08)	Contratos		Contratos formalizados	(SW.05)	Oficina de Contratos	Datos

[2] Tomado de: anexo 7b: Manual de administración del riesgo.
[3] Tomado del módulo 2. Análisis de riesgos PID_00177810, por Daniel Cruz Allende.

INVENTARIO DE ACTIVOS – TIPO: DATOS						
CODIGO	NOMBRE DEL ACTIVO	CANT	DESCRIPCIÓN	DEPENDENCIA ENTRE ACTIVOS	PROPIETARIO	TIPO DE ACTIVO
(D.09)	Correspondencia radicada		Correspondencia de entrada a la Empresa.	(SW.10) - (SW.14)	Recursos fisicos	Datos
(D.10)	Datos del sistema ERP		Esquemas con los datos del sistema ERP	(SW.14)	Oficina TI	Datos
(D.11)	Datos del sistema de proyectos de obra		Esquemas con los datos del sistema de información de proyectos de obra.	(SW.14)	Oficina TI	Datos
(D.12)	Datos del CMS		Esquemas con los datos del sistema de los portales web de la Empresa	(SW.14)	Oficina TI	Datos
(D.13)	Datos de planes de mejoramiento		Esquemas con los datos del sistema de información de planes de mejoramiento.	(SW.14)	Oficina TI	Datos
(D.14)	Datos del sistema de activos de información		Esquemas con los datos del sistema de información de activos de información.	(SW.14)	Oficina TI	Datos
(D.15)	datos del sistema de gestión documental.		Esquemas con los datos del sistema de información de gestión documental.	(SW.14)	Oficina TI	Datos

Tabla 5. Inventario de activos - (Aux)Equipamiento auxiliar. Fuente: propia.

INVENTARIO DE ACTIVOS – TIPO: EQUIPAMIENTO AUXILIAR						
CODIGO	NOMBRE DEL ACTIVO	CANT	DESCRIPCIÓN	DEPENDENCIA ENTRE ACTIVOS	PROPIETARIO	TIPO DE ACTIVO
(Aux.01)	Sistema de aire Acondicionado de precisión	1	Sistema de control ambiental para el CPD	(I.01)	Oficina TI	Equipamiento auxiliar
(Aux.02)	Sistema de detección y extinción de fuego	1	Sistema de prevención y control de fuego para el CPD	(I.01)	Oficina TI	Equipamiento auxiliar
(Aux.03)	Sistema de alimentación ininterrumpida de energía eléctrica	2	UPS para los equipos alojados en el CPD	(I.01)	Oficina TI	Equipamiento auxiliar
(Aux.04)	Archivadores		Elementos para almacenar carpetas legajadoras	(I.05)	Oficina TI	Equipamiento auxiliar

Tabla 6. Inventario de activos - (HW)Hardware. Fuente: propia.

INVENTARIO DE ACTIVOS – TIPO: HARDWARE						
CODIGO	NOMBRE DEL ACTIVO	CANT	DESCRIPCIÓN	DEPENDENCIA ENTRE ACTIVOS	PROPIETARIO	TIPO DE ACTIVO
(HW.01)	Servidores físicos Win2012	20	Servidores de procesamiento	(I.01) - (Aux.01) - (Aux.02) - (Aux.03)	Oficina TI	Hardware
(HW.02)	Servidores físicos Linux Ubuntu	10	Servidores de procesamiento	(I.01) - (Aux.01) - (Aux.02) - (Aux.03)	Oficina TI	Hardware

INVENTARIO DE ACTIVOS – TIPO: HARDWARE						
CODIGO	NOMBRE DEL ACTIVO	CANT	DESCRIPCIÓN	DEPENDENCIA ENTRE ACTIVOS	PROPIETARIO	TIPO DE ACTIVO
(HW.03)	Servidores físicos host para virtualizar	20	Servidores para virtualización	(I.01) - (Aux.01) - (Aux.02) - (Aux.03)	Oficina TI	Hardware
(HW.04)	Solución almacenamiento SAN	1	Solución corporativa para almacenamiento de información	(I.01) - (Aux.01) - (Aux.02) - (Aux.03)	Oficina TI	Hardware
(HW.05)	Solución backup	1	Equipos que conforman la solución de backup	(I.01) - (Aux.01) - (Aux.02) - (Aux.03)	Oficina TI	Hardware
(HW.06)	Fortigate	1	Firewall	(I.01) - (Aux.01) - (Aux.02) - (Aux.03)	Oficina TI	Hardware

Tabla 7. Inventario de activos - (I)Instalaciones. Fuente: propia.

INVENTARIO DE ACTIVOS – TIPO: INSTALACIONES						
CODIGO	NOMBRE DEL ACTIVO	CANT	DESCRIPCIÓN	DEPENDENCIA ENTRE ACTIVOS	PROPIETARIO	TIPO DE ACTIVO
(I.01)	Centro de Procesamiento de Datos – CPD	1	Corresponde al sitio físico donde funcionan todos los equipos tecnológicos que conforman el centro de procesamiento de datos.	(I.05)	Oficina TI	Instalaciones
(I.02)	Cuartos de cableado	9	Encerramientos en cada piso utilizados para proteger los switches de cableado horizontal	(I.05)	Oficina TI	Instalaciones
(I.03)	Oficinas directivos	20	Puestos de trabajo con puerta	(I.05)	Recursos físicos	Instalaciones
(I.04)	Puestos de trabajo	745	Puestos de trabajo abiertos	(I.05)	Recursos físicos	Instalaciones
(I.05)	Edificio principal	1	Sede principal de la Empresa	N/A	Recursos físicos	Instalaciones
(I.06)	Archivo central	1	Instalaciones físicas apropiadas y acondicionadas para la conservación de información en papel	(I.05)	Recursos físicos	Instalaciones
(I.07)	Recepción	1	Punto de ingreso a las instalaciones dela Entidad	(I.05)	Recursos físicos	Instalaciones

Tabla 8. Inventario de activos - (R)Red. Fuente: propia.

INVENTARIO DE ACTIVOS – TIPO: RED						
CODIGO	NOMBRE DEL ACTIVO	CANT	DESCRIPCIÓN	DEPENDENCIA ENTRE ACTIVOS	PROPIETARIO	TIPO DE ACTIVO
(R.01)	Switch de Core	2	Equipo activo de comunicación de red principal, ubicado en el CPD	(I.01) - (Aux.01) - (Aux.02) - (Aux.03)	Oficina TI	Red
(R.02)	Switch Top of Rack	4	Equipo activo de comunicación de red, ubicado en cada rack	(I.01) - (Aux.01) - (Aux.02) - (Aux.03)	Oficina TI	Red
(R.03)	Switch de borde	10	equipo activo de comunicación de red, ubicado en cada piso	(I.01) - (I.02)	Oficina TI	Red

INVENTARIO DE ACTIVOS – TIPO: RED						
CODIGO	NOMBRE DEL ACTIVO	CANT	DESCRIPCIÓN	DEPENDENCIA ENTRE ACTIVOS	PROPIETARIO	TIPO DE ACTIVO
(R.04)	Canales Internet	2	Canal de red que permite la conectividad con la red Internet	(I.01) - (Aux.01) - (Aux.02) - (Aux.03)	Oficina TI	Red

Tabla 9. Inventario de activos - (S)Servicios. Fuente: propia.

INVENTARIO DE ACTIVOS – TIPO: SERVICIOS						
CODIGO	NOMBRE DEL ACTIVO	CANT	DESCRIPCIÓN	DEPENDENCIA ENTRE ACTIVOS	PROPIETARIO	TIPO DE ACTIVO
(S.01)	Correo electrónico	1	Servicio prestado por un tercero	(R.04)	Oficina TI	Servicios
(S.02)	Intranet	1	Micrositio web de consulta interna	(SW.01)	Oficina TI	Servicios
(S.03)	Página web	1	Sucursal virtual de la empresa	(R.04)	Oficina TI	Servicios
(S.04)	Carpetas compartidas	2	Servicio para almacenamiento de información laboral no estructurada	(HW.01) - (HW.04)	Oficina TI	Servicios
(S.05)	Directorio activo	1	Servicios de directorio	(HW.01)	Oficina TI	Servicios

Tabla 10. Inventario de activos - (SW)Software. Fuente: propia.

INVENTARIO DE ACTIVOS – TIPO: SOFTWARE						
CODIGO	NOMBRE DEL ACTIVO	CANT	DESCRIPCIÓN	DEPENDENCIA ENTRE ACTIVOS	PROPIETARIO	TIPO DE ACTIVO
(SW.01)	Servidores virtuales producción	20	Servidores que a través del modelo de virtualización permiten la operación de aplicaciones o servicios en producción	(HW.03)	Oficina TI	Software
(SW.02)	Servidores virtuales desarrollo	20	Servidores que a través del modelo de virtualización permiten definir ambientes separados para desarrollo	(HW.03)	Oficina TI	Software
(SW.03)	Servidores virtuales pruebas	20	Servidores que a través del modelo de virtualización permiten definir ambientes separados para pruebas	(HW.03)	Oficina TI	Software
(SW.04)	Sistema B.I	1	Sistema de Información de Inteligencia de Negocios	(SW.01)	Dirección general	Software
(SW.05)	Sistema ERP	1	sistema de información que incluye módulos: administrativo y financiero + Personal y nómina + Almacén	(SW.01)	Secretaría general	Software
(SW.06)	Sistema Proyectos de Obra	1	Sistema de información para la gestión de proyectos, mediante la metodología PMI	(HW.02) - (S.05)	Subdirección de infraestructura	Software
(SW.07)	CMS	1	Gestor de contenidos para la intranet y el portal web	(HW.02)	Oficina de comunicaciones	Software

INVENTARIO DE ACTIVOS – TIPO: SOFTWARE						
CODIGO	NOMBRE DEL ACTIVO	CANT	DESCRIPCIÓN	DEPENDENCIA ENTRE ACTIVOS	PROPIETARIO	TIPO DE ACTIVO
(SW.08)	S.I. Planes de Mejoramiento	1	Sistema para la gestión de los planes de mejoramiento, que se generan como producto de las auditorías	(HW.02) - (S.05)	Oficina de control interno	Software
(SW.09)	S.I. Activos de Información	1	Sistema para la gestión de los activos de información organizacionales	(HW.02) - (S.05)	Oficina de seguridad de la información	Software
(SW.10)	S.I. Gestión documental	1	Sistema para la gestión de la correspondencia y el archivo	(HW.02) - (S.05)	Secretaría general	Software
(SW.11)	Fortianalyzer	1	Herramienta que facilita el análisis de las posibles amenazas e ineficiencias de la red	(HW.06)	Oficina TI	Software
(SW.12)	Fortisandbox	1	Herramienta para el análisis de los archivos digitales que circulan por la red de la entidad	(HW.06)	Oficina TI	Software
(SW.13)	Antivirus	1	Software de tipo corporativo que detecta la presencia de malware en los diferentes medios de almacenamiento de un computador	(HW.02)	Oficina TI	Software
(SW.14)	Bases de datos de los SI	1	Repositorio de la información estructura	(HW.02)	Oficina TI	Software
(SW.15)	RAC base de datos Oracle	1	Sistema de alta disponibilidad para la base de datos. Conformado por 2 nodos	(HW.02)	Oficina TI	Software
(SW.16)	Firmware fortigate	1	"Software" interno del firewall, que permite su operación	(HW.06)	Oficina TI	Software
(SW.17)	Sistema Operativo Ubuntu	30	Sistema Operativo de código abierto muy empleado en el ámbito de servidores	(HW.02)	Oficina TI	Software
(SW.18)	Sistema Operativo Windows	80	Sistema operativo de propiedad de Microsoft	(HW.01)	Oficina TI	Software
(SW.19)	Hipervisor	20	Aplicación de software que permite la ejecución de varios sistemas operativos en una misma máquina, de manera simultanea	(HW.03)	Oficina TI	Software

Tabla 11. Inventario de activos - (P) Personas. Fuente: propia.

INVENTARIO DE ACTIVOS – TIPO: PERSONAS						
CÓDIGO	NOMBRE DEL ACTIVO	CANT	DESCRIPCIÓN	DEPENDENCIA ENTRE ACTIVOS	PROPIETARIO	TIPO DE ACTIVO
(P.01)	Director	1	N/A	N/A	Dirección general	Personal
(P.02)	Subdirector de Proyectos	1	N/A	N/A	Subdirección de proyectos	Personal
(P.03)	Subdirector de Infraestructura	1	N/A	N/A	Subdirección de infraestructura	Personal

INVENTARIO DE ACTIVOS – TIPO: PERSONAS						
CÓDIGO	NOMBRE DEL ACTIVO	CANT	DESCRIPCIÓN	DEPENDENCIA ENTRE ACTIVOS	PROPIETARIO	TIPO DE ACTIVO
(P.04)	Subdirector Jurídico	1	N/A	N/A	Subdirección jurídica	Personal
(P.05)	Jefe Contratación	1	N/A	N/A	Oficina de contratos	Personal
(P.06)	Secretario General	1	N/A	N/A	Secretaría general	Personal
(P.07)	Jefe Administración Financiera	1	N/A	N/A	Administración financiera	Personal
(P.08)	Jefe Recursos Físicos	1	N/A	N/A	Recursos físicos	Personal
(P.09)	Administrador Base de Datos	2	N/A	N/A	Oficina TI	Personal
(P.10)	Oficial de Seguridad	1	N/A	N/A	Oficina TI	Personal
(P.11)	Arquitecto de TI	2	N/A	N/A	Oficina TI	Personal
(P.12)	Operador CPD	3	N/A	N/A	Oficina TI	Personal
(P.13)	Webmaster	1	N/A	N/A	Oficina TI	Personal
(P.14)	Operador de Redes y Comunicaciones	2	N/A	N/A	Oficina TI	Personal
(P.15)	Responsable Mesa de Servicios	1	N/A	N/A	Oficina TI	Personal
(P.16)	Operador Mesa de Servicios	5	N/A	N/A	Oficina TI	Personal

4.2. Valoración de los activos

La valoración de los activos se debe pensar de tal modo que se tenga en cuenta el valor y la importancia que tienen para la Empresa. Otra manera de valorar los activos es definir un modelo jerárquico, que permita dar un mayor valor a aquellos activos de los cuales dependen otros, tal como se muestra en la siguiente ilustración:

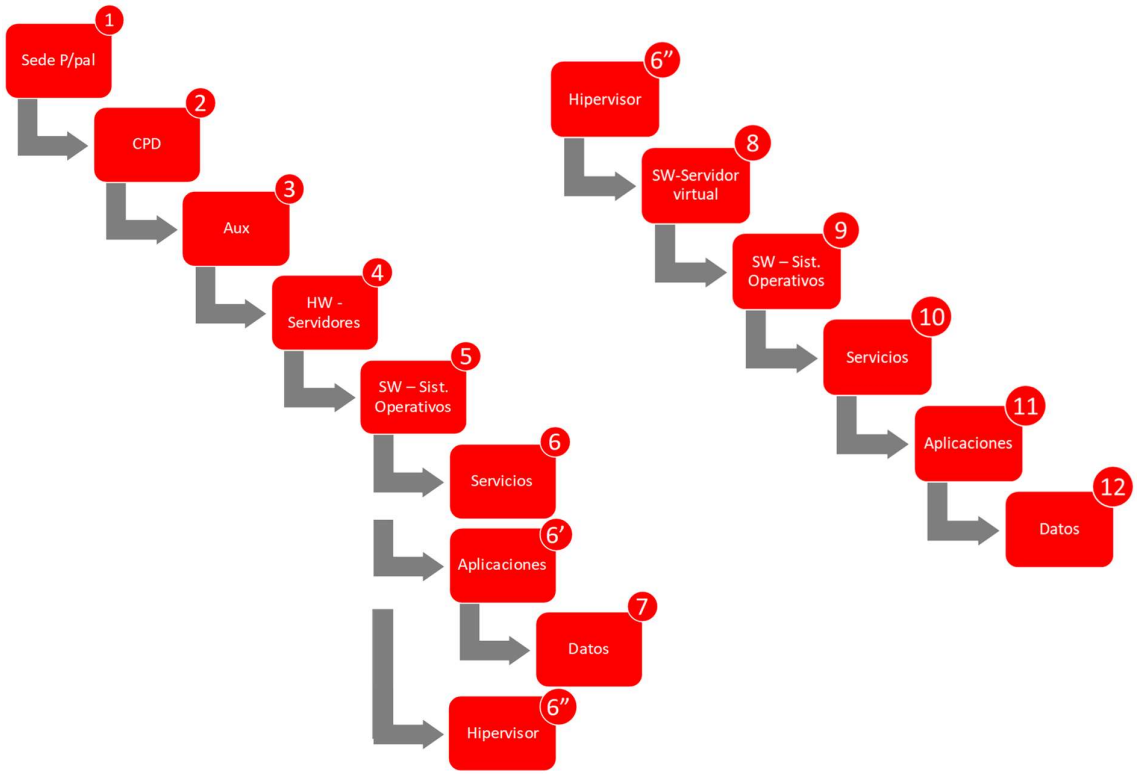


Ilustración 7. Jerarquía para la valoración de activos. Fuente: Propia.

En la ilustración 7 se puede apreciar el modelo jerárquico planteado. Por ejemplo, si falla el hipervisor, todos los activos que dependen de él, muy probablemente también van a presentar una falla o no estarán disponibles.

4.3. Dimensiones de Seguridad

Para la Empresa de Manejo de Obras las dimensiones ACIDA con las cuales se valorarán los activos de información son las siguientes:

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. [UNE 71504: 2008].

Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE - ISO/IEC 27001:2007].

Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004].

Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008].

Trazabilidad: del inglés Accountability. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008].

Después de haber explicado las dimensiones, es preciso tener de presente la escala de 5 criterios que se empleará durante la valoración:

Tabla 12. Valoración de las dimensiones de seguridad. Fuente: Modelo TFM UOC

VALOR	CRITERIO
5	Daño muy grave para la empresa
4	Daño grave para la empresa
3	Daño importante para la empresa
2	Daño menor para la empresa
1	Irrelevante para la empresa

4.4. Tabla Resumen

En la siguiente tabla se resume la valoración de los activos previamente identificados, de acuerdo a las cinco dimensiones ya citadas también.

Tabla 13. Valoración de los activos. Fuente: Propia.

INVENTARIO DE ACTIVOS								
TIPO DE ACTIVO	CODIGO	NOMBRE DEL ACTIVO	[A]	[C]	[I]	[D]	[T]	IMPORTANCIA DEL ACTIVO
Datos	(D.01)	Configuración fortigate	5	5	5	5	4	Muy alto
Datos	(D.02)	Firmware fortigate	5	1	5	5	4	Alto
Datos	(D.03)	Configuración antivirus	5	5	5	5	4	Muy alto
Datos	(D.04)	Código fuente de los sistemas de información	5	4	5	4	3	Muy alto
Datos	(D.05)	Licenciamiento software comercial	5	1	5	4	5	Alto
Datos	(D.06)	hojas de vida de los empleados	4	5	5	4	3	Muy alto
Datos	(D.07)	Archivo físico no digitalizado	4	5	5	4	3	Muy alto
Datos	(D.08)	Contratos	3	2	5	3	2	Medio
Datos	(D.09)	Correspondencia radicada	3	2	4	4	3	Alto
Datos	(D.10)	S.I. de inteligencia de negocio (BI)	3	3	3	3	2	Medio
Datos	(D.11)	Datos del sistema ERP	2	4	3	4	2	Medio
Datos	(D.11)	Datos del sistema de proyectos de obra	2	2	3	4	1	Medio

INVENTARIO DE ACTIVOS								
TIPO DE ACTIVO	CODIGO	NOMBRE DEL ACTIVO	[A]	[C]	[I]	[D]	[T]	IMPORTANCIA DEL ACTIVO
Datos	(D.12)	Datos del CMS	2	2	3	4	2	Medio
Datos	(D.13)	Datos de planes de mejoramiento	3	2	3	3	2	Medio
Datos	(D.14)	Datos del sistema de activos de información	3	3	2	3	2	Medio
Datos	(D.15)	datos del sistema de gestión documental.	3	4	3	3	2	Medio
Equipamiento auxiliar	(Aux.01)	Sistema de aire Acondicionado de precisión				5		Alto
Equipamiento auxiliar	(Aux.02)	Sistema de detección y extinción de fuego				5		Alto
Equipamiento auxiliar	(Aux.03)	Sistema de alimentación ininterrumpida de energía eléctrica				5		Alto
Equipamiento auxiliar	(Aux.04)	Sistema de control de acceso al CPD				5		Alto
Equipamiento auxiliar	(Aux.05)	Archivadores				3		Medio
Hardware	(HW.01)	Servidores físicos Win2012	2	4	4	3	3	Alto
Hardware	(HW.02)	Servidores físicos Linux Ubuntu	2	4	4	3	3	Alto
Hardware	(HW.03)	Servidores físicos host para virtualizar	2	4	4	4	3	Alto
Hardware	(HW.04)	Solución almacenamiento SAN	2	4	5	3	3	Alto
Hardware	(HW.05)	Solución backup	2	4	5	3	3	Alto
Hardware	(HW.06)	Fortigate	2	4	5	3	3	Alto
Instalaciones	(I.01)	Centro de Procesamiento de Datos – CPD	2	5	5	4	4	Alto
Instalaciones	(I.02)	Cuartos de cableado	2	4	5	4	3	Alto
Instalaciones	(I.03)	Oficinas directivos	3	3	2	4	4	Alto
Instalaciones	(I.04)	Puestos de trabajo	2	3	3	1	4	Medio
Instalaciones	(I.05)	Edificio principal	2	2	4	4	3	Medio
Instalaciones	(I.06)	Archivo central	3	5	5	4	3	Alto
Red	(R.01)	Switch de Core	4	3	3	5	5	Alto
Red	(R.02)	Switch Top of Rack	4	3	3	5	5	Alto
Red	(R.03)	Switch de borde	4	3	3	4	5	Alto
Red	(R.04)	Canales Internet	2	2	4	5	3	Alto
Servicios	(S.01)	Correo electrónico	5	4	4	4	3	Alto
Servicios	(S.02)	Intranet	5	3	4	4	5	Muy alto
Servicios	(S.03)	Página web	5	3	4	4	5	Muy alto
Servicios	(S.04)	Carpetas compartidas	5	4	5	3	3	Alto
Servicios	(S.05)	Directorio activo	5	5	5	5	3	Muy alto
Software	(SW.01)	Servidores virtuales producción	2	4	4	4	3	Alto
Software	(SW.02)	Servidores virtuales desarrollo	2	4	4	4	3	Alto
Software	(SW.03)	Servidores virtuales pruebas	2	4	4	4	3	Alto

INVENTARIO DE ACTIVOS								
TIPO DE ACTIVO	CODIGO	NOMBRE DEL ACTIVO	[A]	[C]	[I]	[D]	[T]	IMPORTANCIA DEL ACTIVO
Software	(SW.04)	Sistema B.I	2	5	4	5	2	Alto
Software	(SW.05)	Sistema ERP	2	5	4	4	3	Alto
Software	(SW.06)	Sistema Proyectos de Obra	2	3	4	5	3	Alto
Software	(SW.07)	CMS	2	3	3	4	3	Medio
Software	(SW.08)	S.I. Planes de Mejoramiento	2	1	4	3	3	Medio
Software	(SW.09)	S.I. Activos de Información	2	3	4	2	3	Medio
Software	(SW.10)	S.I. Gestión documental	3	5	4	5	3	Alto
Software	(SW.11)	Fortianalyzer	2	2	3	1	2	Bajo
Software	(SW.12)	Fortisandbox	2	2	3	4	3	Medio
Software	(SW.13)	Antivirus	3	2	4	5	3	Alto
Software	(SW.14)	Bases de datos de los SI	4	4	5	5	4	Muy alto
Software	(SW.15)	RAC base de datos Oracle	3	3	5	5	3	Alto
Software	(SW.16)	Firmware fortigate	5	1	5	5	4	Alto
Software	(SW.17)	Sistema Operativo Ubuntu	4	1	3	3	2	Medio
Software	(SW.18)	Sistema Operativo Windows	4	1	3	3	2	Medio
Software	(SW.19)	Hipervisor	4	2	3	4	2	Medio
Personal	(P.01)	Director	5			5		Bajo
Personal	(P.02)	Subdirector de Proyectos	5			5		Bajo
Personal	(P.03)	Subdirector de Infraestructura	5			5		Bajo
Personal	(P.04)	Subdirector Jurídico	5			5		Bajo
Personal	(P.05)	Jefe Contratación	5			5		Bajo
Personal	(P.06)	Secretario General	5			5		Bajo
Personal	(P.07)	Jefe Administración Financiera	5			5		Bajo
Personal	(P.08)	Jefe Recursos Físicos	5			5		Bajo
Personal	(P.09)	Administrador Base de Datos	5			5		Bajo
Personal	(P.10)	Oficial de Seguridad	5			4		Bajo
Personal	(P.11)	Arquitecto de TI	5			4		Bajo
Personal	(P.12)	Operador CPD	5			5		Bajo
Personal	(P.13)	Webmaster	4			4		Bajo
Personal	(P.14)	Operador de Redes y Comunicaciones	4			4		Bajo
Personal	(P.15)	Responsable Mesa de Servicios	4			4		Bajo
Personal	(P.16)	Operador Mesa de Servicios	1			3		Muy bajo

4.5. Análisis de Amenazas

Una amenaza, de acuerdo con la norma ISO 27000 es, palabras más, palabras menos: "la causa potencial de un incidente no deseado, que puede ocasionar daños a un sistema u organización", por lo que es preciso tenerlas siempre muy presentes y hacer un estudio (análisis) a conciencia.

Lo primero entonces es, conocer las posibles amenazas y saber que pueden ser de origen natural o humano, y que pueden ser accidentales o voluntarias. Para el presente estudio se tendrán en cuenta las amenazas del catálogo ofrecido por la norma ISO 27005, como se muestra en la siguiente tabla:

Tabla 14. Amenazas comunes. Fuente: Norma ISO 27005

Amenazas más Comunes	
A-1.	**Naturales**
A-1.1	Desastre Natural - Temblor (Sísmicos)
A-1.2	Desastre Natural - Huracán, Tifón, Vendaval (Climático)
A-1.3	Desastre Natural - Inundación
A-1.4	Desastre Natural - Rayos, tormenta eléctrica (Meteorológico)
A-1.5	Desastre Natural - Cenizas, Lava (Volcánicos)
A-2.	**Del entorno**
A-2.1	Ataque malicioso - Explosivos
A-2.2	Ataque malicioso - Aparato incendiario
A-2.3	Ataque malicioso - Químicos
A-2.4	Ataque malicioso - Daño premeditado / Vandalismo
A-2.5	Ataque malicioso - Uso de armas (actos de guerra / inquietud civil)
A-2.6	Ataque malicioso - Radiación electromagnética
A-2.7	Ataque malicioso - Intención de robo
A-2.8	Ataque malicioso - Manipulación de datos o software
A-2.9	Ataque malicioso - Manipulación de equipo informático
A-2.10	Ataque malicioso - Acceso a servicios del sitio
A-2.11	Acción Industrial - (Espionaje)
A-2.12	Acceso no autorizado al Sitio - (Sector)
A-2.13	Acceso no autorizado al Edificio
A-2.14	Acceso no autorizado a la Sala - (Oficina)
A-3.	**Del Medio Ambiente**
A-3.1	Daño Accidental - Nave Aérea (Accidente importante)
A-3.2	Daño Accidental - Colisión Vehicular (Accidente importante)
A-3.3	Daño Accidental - Material del Edificio
A-3.4	Daño Accidental - Incendio (Fuego)
A-3.5	Daño Accidental - Agua o Suciedad (Daño por agua)
A-3.6	Daño Accidental - Falla de Aire Acondicionado

Amenazas más Comunes	
A-3.7	Daño Accidental - Extremos de temperatura / humedad
A-3.8	Daño Accidental - Contaminación Química (Contaminación)
A-3.9	Daño Accidental - Roturas por personal o equipos (Destrucción del equipo o los medios)
A-3.10	Daño Accidental - Radiación electromagnética (Perturbaciones debidas a la radiación)
A-3.11	Daño Accidental - durante la construcción del edificio / mantenimiento
A-3.12	Contaminación por polvo / polen / esporas (Corrosión, congelamiento)
A-3.13	Daño animal (roedores / insectos / bacteriológico)
A-3.14	Daño Accidental - Impulso electromagnético (PEM) (Perturbaciones debidas a la radiación)
A-4.	**Por Suministro**
A-4.1	Falla de suministro de energía
A-4.2	Falla de suministro de energía de respaldo (UPS)
A-4.3	Subidas de Voltaje / fluctuaciones
A-4.4	Carga electrostática
A-4.5	Falla de suministro de agua o de aire acondicionado
A-4.6	Falla en el suministro de combustible (Gasolina u otros)
A-4.7	Falla / Degradación de equipo informático
A-4.8	Falla / Degradación de sistema de comunicaciones
A-4.9	Falla de comunicaciones de largo alcance (canales dedicados, fibra óptica)
A-4.10	Suministro de personal por muerte y/o lesiones
A-5.	**Por Software**
A-5.1	Uso ilegal de software
A-5.2	Uso de Software por usuarios no autorizados
A-5.3	Uso de Software ilegal o Software malicioso
A-5.4	Falla de software / corrupción
A-5.5	Descuido o Falla para usar parches de software para mejorar debilidades de seguridad conocidas
A-5.6	Importación / Exportación ilegal de software
A-5.7	Robo de Software (o aplicaciones de la organización)
A-5.8	Descarga no controlada de software
A-5.9	Virus de arranque (virus boot)
A-5.10	Virus de archivo
A-5.11	Virus de macros
A-5.12	Código Troyano o Programas de propagación (worms)
A-5.13	Encubrimiento de identidad de usuario
A-5.14	Intento sistemático de uso de contraseñas
A-5.15	Uso inapropiado de equipo de comunicaciones
A-5.16	Uso inapropiado de medios de almacenamiento
A-5.17	Acceso a los sistemas / documentos por el personal de mantenimiento y aseo
A-5.18	Mal Uso de recursos
A-5.19	Abuso de derechos de usuario
A-5.20	Abuso de derechos de administrador

Amenazas más Comunes	
A-5.21	Ingeniería Social
A-5.22	Lectura / Copia / Remoción no autorizada de documentos archivados
A-5.23	Interrupción del servicio durante instalación / actualización al equipo
A-5.24	Documentos dejados en la fotocopiadora, impresora, scanner, fax
A-5.25	Rechazo intencional de comunicaciones
A-5.26	Lectura / copia no autorizada de comunicaciones recibidas
A-5.27	Robo de equipo (de cómputo, de telecomunicaciones, de almacenamiento de datos)
A-5.28	Robo de equipo móvil (portátil, tableta, smartphone)
A-5.29	Infiltración de comunicaciones
A-5.30	Comunicaciones a rutas equivocadas
A-5.31	Mal uso de puertos de acceso remoto para administración o diagnóstico
A-5.32	Re - ruteo de comunicaciones
A-5.33	Análisis de tráfico
A-5.34	Engaño o suplantación de direcciones IP
A-5.35	Engaño de Servicios de directorio de nombres (DNS)
A-5.36	Análisis de flujo de mensaje
A-5.37	Bombas de correo electrónico
A-5.38	Sobrecarga deliberada de servicio
A-5.39	Interceptación de líneas de comunicación
A-5.40	Manipulación de líneas de comunicación
A-6.	**Acciones No Autorizadas**
A-6.1	Uso no autorizado de equipos
A-6.2	Uso de instalaciones de red en forma no autorizada
A-6.3	Uso no autorizado de medios de almacenamiento
A-6.4	Conexión a equipo no autorizado
A-6.5	Uso no autorizado de sistemas informáticos
A-6.6	Uso de software en forma no autorizada
A-6.7	Acceso a red por usuario no autorizado
A-6.8	Procesamiento Ilegal de los datos
A-6.9	Uso no autorizado de datos almacenados en plantas telefónicas
A-6.10	Divulgación de datos o documentos
A-7.	**Por Operación**
A-7.1	Deterioro de los medios de almacenamiento
A-7.2	Errores de transmisión
A-7.3	Error operacional del personal
A-7.4	Error en la ejecución del mantenimiento
A-7.5	Falla técnica de los componentes de red
A-7.6	Falla de los servicios de comunicación
A-7.7	Falla para recibir información
A-7.8	Daño a las líneas de comunicación

Amenazas más Comunes	
A-7.9	Sobrecarga de tráfico de datos en las redes
A-7.10	Enlaces que permanecen activos al completar comunicaciones a través de las redes
A-7.11	Déficit de personal
A-7.12	Errores de Usuario
A-7.13	Exposición de contraseña
A-7.14	Exposición de documentos / datos
A-7.15	Comunicación descuidada de información a receptor no autorizado
A-7.16	Coacción al personal
A-7.17	Engaño / Chantaje al personal
A-7.18	Copia no controlada de documentos
A-7.19	Eliminación no controlada de documentos
A-8.	**Por Control**
A-8.1	Uso no controlado de recursos
A-8.2	Uso no controlado de enlaces de comunicación
A-8.3	Pérdida de confidencialidad
A-8.4	Perdida de disponibilidad a usuarios autorizados
A-8.5	Infracción a la ley de derechos de autor
A-8.6	Degradación del tiempo de respuesta
A-8.7	Degradación de disponibilidad
A-8.8	Manipulación de datos inadvertida
A-8.9	Eliminación negligente de datos
A-8.10	Conversación cruzada
A-8.11	Degradación de documentos en papel
A-8.12	No disponibilidad de respaldos
A-8.13	Corrupción de los datos (electrónicos o físicos)
A-8.14	Negación de Servicios
A-8.15	Robo / Pérdida de equipo / Datos del operador
A-8.16	Manipulación de equipo de operador por familiar o visitante
A-8.17	Falla para respaldar datos / documentos
A-8.18	Falla para cambiar contraseñas regularmente
A-8.19	Falla para usar medidas de seguridad proporcionadas
A-8.20	Falla en los datos respaldados
A-8.21	Abuso de medidas de seguridad - Seguimientos, mal uso de señales de acceso
A-8.22	Mal uso de los servicios de correo
A-8.23	Publicidad adversa de medios protegidos (Entrevistas no autorizadas)
A-8.24	Tiempo de respuesta extendido a través de diferentes zonas de tiempo / horas de trabajo
A-8.25	Brecha de legislación
A-8.26	Explotación de debilidad conocida
A-8.27	Recuperación de medios de almacenamiento o procesamiento reciclados o desechados
A-8.28	Uso de datos de provenientes de fuente no confiables

Amenazas más Comunes	
A-8.29	Emisión o detección de la ubicación (posición) de equipo o funcionario
A-9.	**Aspectos Generales**
A-9.1	Falta de seguimiento de auditoria
A-9.2	Dificultad para hacer verificaciones
A-9.3	Dificultad de validación
A-9.4	Deficiente control de metodología de codificación de la información
A-9.5	Dificultad para encontrar fallas y/o problemas
A-9.6	Registros inadecuados de cambios / modificaciones
A-9.7	Oportunidad para acceso a sistemas por "puertas traseras" no controladas
A-9.8	Rendimiento no esperado de los procesos
A-9.9	Usuarios desconocidos
A-9.10	Improbabilidad de pruebas completas de plataformas, sistemas o procesos
A-9.11	Frustración del usuario

Una vez listadas las amenazas, es necesario mencionar que para la evaluación se empleará la siguiente tabla de frecuencias:

Tabla 15. Frecuencia de ocurrencia de la amenaza. Fuente: Manual Administración del Riesgo

FRECUENCIA		
Valor	**Concepto**	**Explicación**
5	Casi segura	Se conoce que ha ocurrido en el último año.
4	Alta	Se conoce que ha ocurrido en los dos últimos años.
3	Posible	Se conoce que ha ocurrido en los últimos 5 años
2	Baja	Se conoce que ha ocurrido por lo menos una vez en la Entidad. Aunque no en los últimos 5 años.
1	Remota	Existe la probabilidad, aunque no se conoce que haya ocurrido en la Entidad

Tabla 16. Niveles de medición del impacto. Fuente: Manual Administración del Riesgo

IMPACTO	
#	**NIVEL**
5	Catastrófico
4	Mayor
3	Moderado
2	Menor
1	Insignificante

A continuación, se presenta la valoración de los activos frente a las amenazas. Para lo cual se agruparon los activos por tipo y se tomaron las amenazas que aplican a cada tipo.

Tabla 17. Valoración de amenazas para Activos de tipo Datos. Elaboración propia.

VALORACIÓN DE AMENAZAS							
DATOS		FREC.	[A]	[C]	[I]	[D]	[T]
(D.01) Configuración fortigate		3	50%	75%	100%	100%	
(D.02) Firmware fortigate		3	50%	75%	100%	100%	
(D.03) Configuración antivirus		3	50%	75%	100%	100%	
(D.04) Código fuente de los sistemas de información		3	50%	75%	100%	100%	
(D.05) Licenciamiento software comercial		3	50%	75%	100%	100%	
(D.06) hojas de vida de los empleados		3	50%	75%	100%	100%	
(D.07) Archivo físico no digitalizado		3	50%	75%	100%	100%	
(D.08) Contratos		3	50%	75%	100%	100%	
(D.09) Correspondencia radicada		3	50%	75%	100%	100%	
LISTA DE AMENAZAS							
A-2.	**Del entorno**						
A-2.1	Ataque malicioso - Explosivos	1				75%	
A-2.2	Ataque malicioso - Aparato incendiario	1				100%	
A-2.3	Ataque malicioso - Químicos	1				50%	
A-2.4	Ataque malicioso - Daño premeditado / Vandalismo	1				100%	
A-2.7	Ataque malicioso - Intención de robo	2				100%	
A-2.8	Ataque malicioso - Manipulación de datos o software	1				100%	
A-2.9	Ataque malicioso - Manipulación de equipo informático	2				75%	
A-2.11	Acción Industrial - (Espionaje)	1				50%	
A-2.13	Acceso no autorizado al Edificio	2				20%	
A-2.14	Acceso no autorizado a la Sala - (Oficina)	3				75%	
A-3.	**Del Medio Ambiente**						
A-3.4	Daño Accidental - Incendio (Fuego)	3				75%	
A-3.5	Daño Accidental - Agua o Suciedad (Daño por agua)	3				50%	
A-3.8	Daño Accidental - Contaminación Química (Contaminación)	1				50%	
A-3.9	Daño Accidental - Roturas por personal o equipos (Destrucción del equipo o los medios)	2				100%	
A-3.11	Daño Accidental - durante la construcción del edificio / mantenimiento	2				25%	
A-3.12	Contaminación por polvo / polen / esporas (Corrosión, congelamiento)	3				15%	
A-3.13	Daño animal (roedores / insectos / bacteriológico)	2				50%	
A-5.	**Por Software**						
A-5.10	Virus de archivo	2				60%	
A-5.17	Acceso a los sistemas / documentos por el personal de mantenimiento y aseo	1		50%			
A-5.24	Documentos dejados en la fotocopiadora, impresora, scanner, fax	3		50%			
A-6.	**Acciones No Autorizadas**						
A-6.8	Procesamiento Ilegal de los datos	1	50%		50%		
A-6.9	Uso no autorizado de datos almacenados en plantas telefónicas	1		75%			
A-6.10	Divulgación de datos o documentos	3		75%			
A-7.	**Por Operación**						
A-7.1	Deterioro de los medios de almacenamiento	2			50%	75%	

VALORACIÓN DE AMENAZAS							
DATOS		FREC.	[A]	[C]	[I]	[D]	[T]
A-7.3	Error operacional del personal	3				50%	
A-7.7	Falla para recibir información	2				25%	
A-7.12	Errores de Usuario	3		25%	25%	25%	
A-7.14	Exposición de documentos / datos	3		75%			
A-7.15	Comunicación descuidada de información a receptor no autorizado	2		50%			
A-7.16	Coacción al personal	2		25%		25%	
A-7.17	Engaño / Chantaje al personal	2		25%		25%	
A-7.18	Copia no controlada de documentos	3		25%			
A-7.19	Eliminación no controlada de documentos	3				100%	
A-8.	**Por Control**						
A-8.8	Manipulación de datos inadvertida	2			100%		
A-8.9	Eliminación negligente de datos	3				100%	
A-8.11	Degradación de documentos en papel	2			75%		
A-8.13	Corrupción de los datos (electrónicos o físicos)	3			75%		
A-8.20	Falla en los datos respaldados	3				75%	
A-8.27	Recuperación de medios de almacenamiento o procesamiento reciclados o desechados	3		75%			
A-8.28	Uso de datos de provenientes de fuente no confiables	2			50%		
A-9.	**Aspectos Generales**						
A-9.9	Usuarios desconocidos	2	50%				
A-9.11	Frustración del usuario	2				75%	

Tabla 18. Valoración de amenazas para Activos de tipo Equipamiento auxiliar. Elaboración propia.

VALORACIÓN DE AMENAZAS							
EQUIPAMIENTO AUXILIAR		FREC.	[A]	[C]	[I]	[D]	[A]
(Aux.01) Sistema de aire Acondicionado de precisión		4				100%	
(Aux.02) Sistema de detección y extinción de fuego		4				100%	
(Aux.03) Sistema de alimentación ininterrumpida de energía eléctrica		4				100%	
(Aux.04) Sistema de control de acceso al CPD		4				100%	
LISTA DE AMENAZAS							
A-1.	**Naturales**						
A-1.3	Desastre Natural - Inundación	2				25%	
A-1.4	Desastre Natural - Rayos, tormenta eléctrica (Meteorológico)	4				25%	
A-2.	**Del entorno**						
A-2.1	Ataque malicioso - Explosivos	1				100%	
A-2.2	Ataque malicioso - Aparato incendiario	1				100%	
A-2.3	Ataque malicioso - Químicos	1				50%	
A-2.4	Ataque malicioso - Daño premeditado / Vandalismo	1				50%	
A-2.14	Acceso no autorizado a la Sala - (Oficina)	2				25%	
A-3.	**Del Medio Ambiente**						
A-3.3	Daño Accidental - Material del Edificio	1				25%	
A-3.4	Daño Accidental - Incendio (Fuego)	1				100%	
A-3.5	Daño Accidental - Agua o Suciedad (Daño por agua)	2				50%	

VALORACIÓN DE AMENAZAS							
EQUIPAMIENTO AUXILIAR		FREC.	[A]	[C]	[I]	[D]	[A]
A-3.9	Daño Accidental - Roturas por personal o equipos (Destrucción del equipo o los medios)	2				25%	
A-3.12	Contaminación por polvo / polen / esporas (Corrosión, congelamiento)	1				25%	
A-4.	**Por Suministro**						
A-4.1	Falla de suministro de energía	2				100%	
A-4.3	Subidas de Voltaje / fluctuaciones	2				25%	
A-4.4	Carga electrostática	1				25%	
A-4.7	Falla / Degradación de equipo informático	2				50%	
A-6.	**Acciones No Autorizadas**						
A-6.1	Uso no autorizado de equipos	2				25%	
A-6.5	Uso no autorizado de sistemas informáticos	2				25%	
A-7.	**Por Operación**						
A-7.4	Error en la ejecución del mantenimiento	2				50%	
A-7.12	Errores de Usuario	3				25%	
A-7.17	Engaño / Chantaje al personal	1				50%	
A-8.	**Por Control**						
A-8.1	Uso no controlado de recursos	2				50%	
A-8.14	Negación de Servicios	3				100%	
A-9.	**Aspectos Generales**						
A-9.2	Dificultad para hacer verificaciones	1				15%	
A-9.5	Dificultad para encontrar fallas y/o problemas	1				15%	
A-9.11	Frustración del usuario	2				100%	

Tabla 19. Valoración de amenazas para Activos de tipo Hardware. Elaboración propia.

VALORACIÓN DE AMENAZAS							
HARDWARE		FREC.	[A]	[C]	[I]	[D]	[A]
(HW.01) Servidores físicos Win2012		4		75%	75%	100%	
(HW.02) Servidores físicos Linux Ubuntu		4		75%	75%	100%	
(HW.03) Servidores físicos host para virtualizar		4		75%	75%	100%	
(HW.04) Solución almacenamiento SAN		4		75%	75%	100%	
(HW.05) Solución backup		4		75%	75%	100%	
(HW.06) Fortigate		4		75%	75%	100%	
LISTA DE AMENAZAS							
A-1.	**Naturales**						
A-1.3	Desastre Natural - Inundación	2				25%	
A-1.4	Desastre Natural - Rayos, tormenta eléctrica (Meteorológico)	4				25%	
A-2.	**Del entorno**						
A-2.1	Ataque malicioso - Explosivos	1				100%	
A-2.2	Ataque malicioso - Aparato incendiario	1				100%	
A-2.3	Ataque malicioso - Químicos	1				50%	
A-2.4	Ataque malicioso - Daño premeditado / Vandalismo	1				50%	

VALORACIÓN DE AMENAZAS							
HARDWARE		FREC.	[A]	[C]	[I]	[D]	[A]
A-2.14	Acceso no autorizado a la Sala - (Oficina)	3				25%	
A-3.	**Del Medio Ambiente**						
A-3.3	Daño Accidental - Material del Edificio	1				25%	
A-3.4	Daño Accidental - Incendio (Fuego)	1				100%	
A-3.5	Daño Accidental - Agua o Suciedad (Daño por agua)	1				50%	
A-3.9	Daño Accidental - Roturas por personal o equipos (Destrucción del equipo o los medios)	1				25%	
A-3.12	Contaminación por polvo / polen / esporas (Corrosión, congelamiento)	1				25%	
A-4.	**Por Suministro**						
A-4.1	Falla de suministro de energía	4			50%	100%	
A-4.2	Falla de suministro de energía de respaldo (UPS)	4			50%	100%	
A-4.3	Subidas de Voltaje / fluctuaciones	3			50%	50%	
A-4.4	Carga electrostática	3			50%	50%	
A-4.5	Falla de suministro de agua o de aire acondicionado	3			75%	75%	
A-4.7	Falla / Degradación de equipo informático	2			50%	50%	
A-6.	**Acciones No Autorizadas**						
A-6.1	Uso no autorizado de equipos	1		45%		50%	
A-6.3	Uso no autorizado de medios de almacenamiento	1			50%	50%	
A-6.4	Conexión a equipo no autorizado	2				50%	
A-6.5	Uso no autorizado de sistemas informáticos	1				25%	
A-7.	**Por Operación**						
A-7.1	Deterioro de los medios de almacenamiento	2			50%	50%	
A-7.4	Error en la ejecución del mantenimiento	1				75%	
A-7.12	Errores de Usuario	2			25%	100%	
A-7.16	Coacción al personal	1		60%	50%	100%	
A-7.17	Engaño / Chantaje al personal	1			50%	100%	
A-8.	**Por Control**						
A-8.15	Robo / Pérdida de equipo / Datos del operador	2				100%	
A-8.19	Falla para usar medidas de seguridad proporcionadas	2				50%	
A-8.26	Explotación de debilidad conocida	2				100%	
A-9.	**Aspectos Generales**						
A-9.6	Registros inadecuados de cambios / modificaciones	3				75%	
A-9.7	Oportunidad para acceso a sistemas por "puertas traseras" no controladas	2				50%	
A-9.8	Rendimiento no esperado de los procesos	3				50%	
A-9.11	Frustración del usuario	2		75%		75%	

Tabla 20. Valoración de amenazas para Activos de tipo Instalaciones. Elaboración propia.

VALORACIÓN DE AMENAZAS						
INSTALACIONES	FREC.	[A]	[C]	[I]	[D]	[A]
(I.01) Centro de Procesamiento de Datos – CPD	4		50%	75%	100%	
(I.02) Cuartos de cableado	4		50%	75%	100%	

VALORACIÓN DE AMENAZAS							
INSTALACIONES		FREC.	[A]	[C]	[I]	[D]	[A]
(I.03) Oficinas directivos		4		50%	75%	100%	
(I.04) Puestos de trabajo		4		50%	75%	100%	
(I.05) Edificio principal		4		50%	75%	100%	
(I.06) Archivo central		4		50%	75%	100%	
(I.07) Recepción		4		50%	75%	100%	
LISTA DE AMENAZAS							
A-1.	**Naturales**						
A-1.1	Desastre Natural - Temblor (SÍsmicos)	4				100%	
A-1.2	Desastre Natural - Huracán, Tifón, Vendaval (Climático)	1				10%	
A-1.3	Desastre Natural - Inundación	2				25%	
A-1.4	Desastre Natural - Rayos, tormenta eléctrica (Meteorológico)	4				25%	
A-2.	**Del entorno**						
A-2.1	Ataque malicioso - Explosivos	1				100%	
A-2.2	Ataque malicioso - Aparato incendiario	1				100%	
A-2.3	Ataque malicioso - Químicos	1				50%	
A-2.4	Ataque malicioso - Daño premeditado / Vandalismo	2				50%	
A-2.13	Acceso no autorizado al Edificio	2		50%	50%		
A-2.14	Acceso no autorizado a la Sala - (Oficina)	3				50%	
A-3.	**Del Medio Ambiente**						
A-3.1	Daño Accidental - Nave Aérea (Accidente importante)	1				100%	
A-3.3	Daño Accidental - Material del Edificio	1				50%	
A-3.4	Daño Accidental - Incendio (Fuego)	4				100%	
A-3.5	Daño Accidental - Agua o Suciedad (Daño por agua)	4				100%	
A-3.6	Daño Accidental - Falla de Aire Acondicionado	2			75%	75%	
A-3.7	Daño Accidental - Extremos de temperatura / humedad	2				25%	
A-3.8	Daño Accidental - Contaminación Química (Contaminación)	1				25%	
A-3.11	Daño Accidental - durante la construcción del edificio / mantenimiento	1				25%	
A-3.13	Daño animal (roedores / insectos / bacteriológico)	2				25%	
A-4.	**Por Suministro**						
A-4.5	Falla de suministro de agua o de aire acondicionado	3				100%	
A-9.	**Aspectos Generales**						
A-9.11	Frustración del usuario	2				100%	

Tabla 21. Valoración de amenazas para Activos de tipo Red. Elaboración propia.

VALORACIÓN DE AMENAZAS						
RED	FREC.	[A]	[C]	[I]	[D]	[A]
(R.01) Switch de Core	4		100%	100%	100%	
(R.02) Switch Top of Rack	4		100%	100%	100%	
(R.03) Switch de borde	4		100%	100%	100%	
(R.04) Canales Internet	4		100%	100%	100%	

VALORACIÓN DE AMENAZAS							
RED		FREC.	[A]	[C]	[I]	[D]	[A]
LISTA DE AMENAZAS							
A-1.	**Naturales**						
A-1.3	Desastre Natural - Inundación	2				25%	
A-1.4	Desastre Natural - Rayos, tormenta eléctrica (Meteorológico)	4				25%	
A-2.	**Del entorno**						
A-2.1	Ataque malicioso - Explosivos	1				100%	
A-2.2	Ataque malicioso - Aparato incendiario	1				100%	
A-2.3	Ataque malicioso - Químicos	1				50%	
A-2.4	Ataque malicioso - Daño premeditado / Vandalismo	1				50%	
A-2.14	Acceso no autorizado a la Sala - (Oficina)	3				25%	
A-3.	**Del Medio Ambiente**						
A-3.3	Daño Accidental - Material del Edificio	1				25%	
A-3.4	Daño Accidental - Incendio (Fuego)	1				100%	
A-3.5	Daño Accidental - Agua o Suciedad (Daño por agua)	1				50%	
A-3.9	Daño Accidental - Roturas por personal o equipos (Destrucción del equipo o los medios)	1				25%	
A-3.12	Contaminación por polvo / polen / esporas (Corrosión, congelamiento)	1				25%	
A-4.	**Por Suministro**						
A-4.1	Falla de suministro de energía	4			50%	100%	
A-4.3	Subidas de Voltaje / fluctuaciones	3			50%	100%	
A-4.4	Carga electrostática	3			50%	50%	
A-4.7	Falla / Degradación de equipo informático	2			50%	50%	
A-4.8	Falla / Degradación de sistema de comunicaciones	2			75%	75%	
A-4.9	Falla de comunicaciones de largo alcance (canales dedicados, fibra óptica)	2			50%	50%	
A-5.	**Por Software**						
A-5.15	Uso inapropiado de equipo de comunicaciones	3				75%	
A-5.21	Ingeniería Social	4				75%	
A-5.23	Interrupción del servicio durante instalación / actualización al equipo	3				100%	
A-5.29	Infiltración de comunicaciones	2		100%		50%	
A-5.30	Comunicaciones a rutas equivocadas	1		100%			
A-5.32	Re - ruteo de comunicaciones	2		100%			
A-5.33	Análisis de tráfico	3		100%			
A-5.34	Engaño o suplantación de direcciones IP	2				100%	
A-5.35	Engaño de Servicios de directorio de nombres (DNS)	2				100%	
A-5.36	Análisis de flujo de mensaje	2		50%			
A-5.38	Sobrecarga deliberada de servicio	2				50%	
A-5.39	Interceptación de líneas de comunicación	1		100%			
A-5.40	Manipulación de líneas de comunicación	1			100%		
A-6.	**Acciones No Autorizadas**						
A-6.2	Uso de instalaciones de red en forma no autorizada	2				100%	
A-6.4	Conexión a equipo no autorizado	3		100%			

VALORACIÓN DE AMENAZAS							
RED		FREC.	[A]	[C]	[I]	[D]	[A]
A-6.5	Uso no autorizado de sistemas informáticos	3		100%			
A-6.7	Acceso a red por usuario no autorizado	4		100%	100%	100%	
A-7.	**Por Operación**						
A-7.2	Errores de transmisión	4			100%		
A-7.4	Error en la ejecución del mantenimiento	3				100%	
A-7.5	Falla técnica de los componentes de red	3				100%	
A-7.6	Falla de los servicios de comunicación	3				100%	
A-7.8	Daño a las líneas de comunicación	4				100%	
A-7.9	Sobrecarga de tráfico de datos en las redes	3				100%	
A-7.12	Errores de Usuario	4		100%	100%		
A-7.16	Coacción al personal	2	100%	100%	100%	100%	
A-8.	**Por Control**						
A-8.2	Uso no controlado de enlaces de comunicación	2	100%				
A-8.6	Degradación del tiempo de respuesta	2			25%		
A-8.14	Negación de Servicios	3				100%	
A-8.18	Falla para cambiar contraseñas regularmente	4		50%			
A-8.19	Falla para usar medidas de seguridad proporcionadas	4		100%		100%	
A-8.26	Explotación de debilidad conocida	2		100%	100%	100%	
A-9.	**Aspectos Generales**						
A-9.7	Oportunidad para acceso a sistemas por "puertas traseras" no controladas	2		100%	100%	100%	
A-9.11	Frustración del usuario	2				100%	

Tabla 22. Valoración de amenazas para Activos de tipo Servicios. Elaboración propia.

VALORACIÓN DE AMENAZAS							
SERVICIOS		FREC.	[A]	[C]	[I]	[D]	[A]
(S.01) Correo electrónico		4	100%	100%	100%	100%	
(S.02) Intranet		4	100%	100%	100%	100%	
(S.03) Página web		4	100%	100%	100%	100%	
(S.04) Carpetas compartidas		4	100%	100%	100%	100%	
(S.05) Directorio activo		4	100%	100%	100%	100%	
LISTA DE AMENAZAS							
A-5.	**Por Software**						
A-5.23	Interrupción del servicio durante instalación / actualización al equipo	3				75%	
A-7.	**Por Operación**						
A-7.6	Falla de los servicios de comunicación	4				100%	
A-7.9	Sobrecarga de tráfico de datos en las redes	4				50%	
A-7.12	Errores de Usuario	4		25%	25%	10%	
A-8.	**Por Control**						
A-8.8	Manipulación de datos inadvertida	2			50%		
A-8.18	Falla para cambiar contraseñas regularmente	2				10%	

VALORACIÓN DE AMENAZAS							
SERVICIOS		FREC.	[A]	[C]	[I]	[D]	[A]
A-8.19	Falla para usar medidas de seguridad proporcionadas	3				15%	
A-8.22	Mal uso de los servicios de correo	4				25%	
A-8.26	Explotación de debilidad conocida	2		100%	100%	100%	
A-9.	**Aspectos Generales**						
A-9.7	Oportunidad para acceso a sistemas por "puertas traseras" no controladas	1		100%	100%	100%	
A-9.9	Usuarios desconocidos	1	100%				
A-9.11	Frustración del usuario	2		100%	100%	100%	

Tabla 23. Valoración de amenazas para Activos de tipo Software. Elaboración propia.

VALORACIÓN DE AMENAZAS						
SOFTWARE	FREC.	[A]	[C]	[I]	[D]	[A]
(SW.01) Servidores virtuales producción	4	0%	100%	100%	100%	
(SW.02) Servidores virtuales desarrollo	4	0%	100%	100%	100%	
(SW.03) Servidores virtuales pruebas	4	0%	100%	100%	100%	
(SW.04) Sistema B.I	4	0%	100%	100%	100%	
(SW.05) Sistema ERP	4	0%	100%	100%	100%	
(SW.06) Sistema Proyectos de Obra	4	0%	100%	100%	100%	
(SW.07) CMS	4	0%	100%	100%	100%	
(SW.08) S.I. Planes de Mejoramiento	4	0%	100%	100%	100%	
(SW.09) S.I. Activos de Información	4	0%	100%	100%	100%	
(SW.10) S.I. Gestión documental	4	0%	100%	100%	100%	
(SW.11) Fortianalyzer	4	0%	100%	100%	100%	
(SW.12) Fortisandbox	4	0%	100%	100%	100%	
(SW.13) Antivirus	4	0%	100%	100%	100%	
(SW.14) Bases de datos de los SI	4	0%	100%	100%	100%	
(SW.15) RAC base de datos Oracle	4	0%	100%	100%	100%	
LISTA DE AMENAZAS						
A-5.	**Por Software**					
A-5.2	Uso de Software por usuarios no autorizados	2		100%	50%	25%	
A-5.3	Uso de Software ilegal o Software malicioso	2		100%	100%	100%	
A-5.4	Falla de software / corrupción	3			50%	50%	
A-5.5	Descuido o Falla para usar parches de software para mejorar debilidades de seguridad conocidas	4				75%	
A-5.7	Robo de Software (o aplicaciones de la organización)	2		75%			
A-5.14	Intento sistemático de uso de contraseñas	4		50%			
A-5.17	Acceso a los sistemas / documentos por el personal de mantenimiento y aseo	2		50%			
A-5.19	Abuso de derechos de usuario	3		50%			
A-5.20	Abuso de derechos de administrador	3				75%	
A-5.21	Ingeniería Social	3		100%	100%	100%	
A-5.22	Lectura / Copia / Remoción no autorizada de documentos archivados	3		100%		100%	
A-6.	**Acciones No Autorizadas**						

VALORACIÓN DE AMENAZAS							
SOFTWARE		FREC.	[A]	[C]	[I]	[D]	[A]
A-6.5	Uso no autorizado de sistemas informáticos	3		100%	100%		
A-7.	**Por Operación**						
A-7.4	Error en la ejecución del mantenimiento	3		50%		50%	
A-7.12	Errores de Usuario	4			50%		
A-7.13	Exposición de contraseña	4		75%	75%		
A-7.14	Exposición de documentos / datos	3		50%			
A-7.16	Coacción al personal	2		100%	100%	100%	
A-8.	**Por Control**						
A-8.8	Manipulación de datos inadvertida	3			100%		
A-8.9	Eliminación negligente de datos	4				100%	
A-8.12	No disponibilidad de respaldos	3			100%	100%	
A-8.18	Falla para cambiar contraseñas regularmente	4		100%			
A-8.20	Falla en los datos respaldados	2				100%	
A-8.26	Explotación de debilidad conocida	2		100%	100%	100%	
A-9.	**Aspectos Generales**						
A-9.6	Registros inadecuados de cambios / modificaciones	4				75%	
A-9.7	Oportunidad para acceso a sistemas por "puertas traseras" no controladas	3		75%		75%	
A-9.10	Improbabilidad de pruebas completas de plataformas, sistemas o procesos	3			50%		
A-9.11	Frustración del usuario	2		100%	100%	100%	

Tabla 24.Valoración de amenazas para Activos de tipo Personas. Elaboración propia.

VALORACIÓN DE AMENAZAS						
PERSONAS	FREC.	[A]	[C]	[I]	[D]	[A]
(P.01) Director	4	50%	60%	50%	50%	0%
(P.02) Subdirector de Proyectos	4	50%	60%	50%	50%	0%
(P.03) Subdirector de Infraestructura	4	50%	60%	50%	50%	0%
(P.04) Subdirector Jurídico	4	50%	60%	50%	50%	0%
(P.05) Jefe Contratación	4	50%	60%	50%	50%	0%
(P.06) Secretario General	4	50%	60%	50%	50%	0%
(P.07) Jefe Administración Financiera	4	50%	60%	50%	50%	0%
(P.08) Jefe Recursos Físicos	4	50%	60%	50%	50%	0%
(P.09) Administrador Base de Datos	4	50%	60%	50%	50%	0%
(P.10) Oficial de Seguridad	4	50%	60%	50%	50%	0%
(P.11) Arquitecto de TI	4	50%	60%	50%	50%	0%
(P.12) Operador CPD	4	50%	60%	50%	50%	0%
(P.13) Webmaster	4	50%	60%	50%	50%	0%
(P.14) Operador de Redes y Comunicaciones	4	50%	60%	50%	50%	0%
(P.15) Responsable Mesa de Servicios	4	50%	60%	50%	50%	0%
(P.16) Operador Mesa de Servicios	4	50%	60%	50%	50%	0%
LISTA DE AMENAZAS						

VALORACIÓN DE AMENAZAS							
	PERSONAS	FREC.	[A]	[C]	[I]	[D]	[A]
A-5.	Por Software						
A-5.13	Encubrimiento de identidad de usuario	1	50%	25%	25%	25%	
A-5.21	Ingeniería Social	1		25%	25%	25%	
A-6.	Acciones No Autorizadas						
A-6.10	Divulgación de datos o documentos	3		60%			
A-7.	Por Operación						
A-7.11	Déficit de personal	4				50%	
A-7.16	Coacción al personal	2		50%	50%	50%	
A-7.17	Engaño / Chantaje al personal	2		50%	50%	50%	
A-8.	Por Control						
A-8.4	Perdida de disponibilidad a usuarios autorizados	3				50%	
A-9.	Aspectos Generales						
A-9.9	Usuarios desconocidos	3		50%			

4.6. Impacto potencial

"Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza"[4].

Después de tener los valores de todos los activos, y el valor máximo del impacto, también por cada activo, se puede calcular el impacto potencial, que le puede generar a la Empresa el hecho de que se materialice una de las amenazas sobre uno de los activos.

Para calcular el impacto potencial se emplea la siguiente fórmula:

Impacto Potencial = Valor del activo x impacto mayor

Al tener los dos (2) valores necesarios para realizar este cálculo, la valoración de los activos en la tabla 12 y los impactos en las tablas 16 a 23, se procede a realizar el cálculo de este valor, como se muestra en la siguiente tabla:

[4] Tomado de: MAGERIT v. 3 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Tabla 25. Impacto potencial. Elaboración propia.

CÁLCULO DE IMPACTO POTENCIAL																	
VALORACIÓN DEL ACTIVO								% IMPACTO					IMPACTO POTENCIAL				
TIPO DE ACTIVO	COD	[A]	[C]	[I]	[D]	[T]	VALOR DEL ACTIVO	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
Datos	(D.01)	5	5	5	5	4	Muy alto	50%	75%	100%	100%	0	2,5	3.75	5	5	0
Datos	(D.02)	5	1	5	5	4	Alto	50%	75%	100%	100%	0	2,5	0,75	5	5	0
Datos	(D.03)	5	5	5	5	4	Muy alto	50%	75%	100%	100%	0	2,5	3,75	5	5	0
Datos	(D.04)	5	4	5	4	3	Muy alto	50%	75%	100%	100%		2,5	3	5	4	0
Datos	(D.05)	5	1	5	4	5	Alto	50%	75%	100%	100%		2,5	0,75	5	4	0
Datos	(D.06)	4	5	5	4	3	Muy alto	50%	75%	100%	100%		2	3,75	5	4	0
Datos	(D.07)	4	5	5	4	3	Muy alto	50%	75%	100%	100%		2	3,75	5	4	0
Datos	(D.08)	3	2	5	3	2	Medio	50%	75%	100%	100%		1,5	1,5	5	3	0
Datos	(D.09)	3	2	4	4	3	Alto	50%	75%	100%	100%		1,5	1,5	4	4	0
Datos	(D.10)	3	3	3	3	2	Medio	50%	75%	100%	100%		1,5	2,25	3	3	0
Datos	(D.11)	2	4	3	4	2	Medio	50%	75%	100%	100%		1	3	3	4	0
Datos	(D.11)	2	2	3	4	1	Medio	50%	75%	100%	100%		1	1,5	3	4	0
Datos	(D.12)	2	2	3	4	2	Medio	50%	75%	100%	100%		1	1,5	3	4	0
Datos	(D.13)	3	2	3	3	2	Medio	50%	75%	100%	100%		1,5	1,5	3	3	0
Datos	(D.14)	3	3	2	3	2	Medio	50%	75%	100%	100%		1,5	2,25	2	3	0
Datos	(D.15)	3	4	3	3	2	Medio	50%	75%	100%	100%		1,5	3	3	3	0
Equipamiento auxiliar	(Aux.02)				5		Muy bajo				100%					5	
Equipamiento auxiliar	(Aux.03)				5		Muy bajo				100%					5	
Equipamiento auxiliar	(Aux.04)				5		Muy bajo				100%					5	
Equipamiento auxiliar	(Aux.05)				3		Muy bajo				100%					3	
Hardware	(HW.01)	2	4	4	3	3	Alto		100%	100%	100%		0	4	4	3	0
Hardware	(HW.02)	2	4	4	3	3	Alto		75%	75%	100%		0	3	3	3	0
Hardware	(HW.03)	2	4	4	4	3	Alto		75%	75%	100%		0	3	3	4	0
Hardware	(HW.04)	2	4	5	3	3	Alto		75%	75%	100%		0	3	3,75	3	0
Hardware	(HW.05)	2	4	5	3	3	Alto		75%	75%	100%		0	3	3,75	3	0
Hardware	(HW.06)	2	4	5	3	3	Alto		75%	75%	100%		0	3	3,75	3	0
Instalaciones	(I.01)	2	5	5	4	4	Alto		75%	75%	100%		0	3,75	3,75	4	0
Instalaciones	(I.02)	2	4	5	4	3	Alto		50%	75%	100%		0	2	3,75	4	0
Instalaciones	(I.03)	3	3	2	4	4	Alto		50%	75%	100%		0	1,5	1,5	4	0
Instalaciones	(I.04)	2	3	3	1	4	Medio		50%	75%	100%		0	1,5	2,25	1	0
Instalaciones	(I.05)	2	2	4	4	3	Medio		50%	75%	100%		0	1	3	4	0
Instalaciones	(I.06)	3	5	5	4	3	Alto		50%	75%	100%		0	2,5	3,75	4	0

CÁLCULO DE IMPACTO POTENCIAL

VALORACIÓN DEL ACTIVO								% IMPACTO					IMPACTO POTENCIAL				
TIPO DE ACTIVO	COD	[A]	[C]	[I]	[D]	[T]	VALOR DEL ACTIVO	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
Instalaciones	(I.07)	2	3	3	4	4	Alto		50%	75%	100%		0	1,5	2,25	4	0
Red	(R.01)	4	3	3	5	5	Alto		50%	75%	100%		0	1,5	2,25	5	0
Red	(R.02)	4	3	3	5	5	Alto		100%	100%	100%		0	3	3	5	0
Red	(R.03)	4	3	3	4	5	Alto		100%	100%	100%		0	3	3	4	0
Red	(R.04)	2	2	4	5	3	Alto		100%	100%	100%		0	2	4	5	0
Servicios	(S.01)	5	4	4	4	3	Alto	100%	100%	100%	100%		5	4	4	4	0
Servicios	(S.02)	5	3	4	4	5	Muy alto	100%	100%	100%	100%		5	3	4	4	0
Servicios	(S.03)	5	3	4	4	5	Muy alto	100%	100%	100%	100%		5	3	4	4	0
Servicios	(S.04)	5	4	5	3	3	Alto	100%	100%	100%	100%		5	4	5	3	0
Servicios	(S.05)	5	5	5	5	3	Muy alto	100%	100%	100%	100%		5	5	5	5	0
Software	(SW.01)	2	4	4	4	3	Alto	0%	100%	100%	100%		0	4	4	4	0
Software	(SW.02)	2	4	4	4	3	Alto	0%	100%	100%	100%		0	4	4	4	0
Software	(SW.03)	2	4	4	4	3	Alto	0%	100%	100%	100%		0	4	4	4	0
Software	(SW.04)	2	5	4	5	2	Alto	0%	100%	100%	100%		0	5	4	5	0
Software	(SW.05)	2	5	4	4	3	Alto	0%	100%	100%	100%		0	5	4	4	0
Software	(SW.06)	2	3	4	5	3	Alto	0%	100%	100%	100%		0	3	4	5	0
Software	(SW.07)	2	3	3	4	3	Medio	0%	100%	100%	100%		0	3	3	4	0
Software	(SW.08)	2	1	4	3	3	Medio	0%	100%	100%	100%		0	1	4	3	0
Software	(SW.09)	2	3	4	2	3	Medio	0%	100%	100%	100%		0	3	4	2	0
Software	(SW.10)	3	5	4	5	3	Alto	0%	100%	100%	100%		0	5	4	5	0
Software	(SW.11)	2	2	3	1	2	Bajo	0%	100%	100%	100%		0	2	3	1	0
Software	(SW.12)	2	2	3	4	3	Medio	0%	100%	100%	100%		0	2	3	4	0
Software	(SW.13)	3	2	4	5	3	Alto	0%	100%	100%	100%		0	2	4	5	0
Software	(SW.14)	4	4	5	5	4	Muy alto	0%	100%	100%	100%		0	4	5	5	0
Software	(SW.15)	3	3	5	5	3	Alto	0%	100%	100%	100%		0	3	5	5	0
Software	(SW.16)	5	1	5	5	4	Alto	0%	100%	100%	100%		0	1	5	5	0
Software	(SW.17)	4	1	3	3	2	Medio	0%	100%	100%	100%		0	1	3	3	0
Software	(SW.18)	4	1	3	3	2	Medio	0%	100%	100%	100%		0	1	3	3	0
Software	(SW.19)	4	2	3	4	2	Medio	0%	100%	100%	100%		0	2	3	4	0
Personal	(P.01)	5			5		Bajo	50%	60%	50%	50%	0%	2,5	0	0	2,5	0
Personal	(P.02)	5			5		Bajo	50%	60%	50%	50%	0%	2,5	0	0	2,5	0
Personal	(P.03)	5			5		Bajo	50%	60%	50%	50%	0%	2,5	0	0	2,5	0
Personal	(P.04)	5			5		Bajo	50%	60%	50%	50%	0%	2,5	0	0	2,5	0
Personal	(P.05)	5			5		Bajo	50%	60%	50%	50%	0%	2,5	0	0	2,5	0

CÁLCULO DE IMPACTO POTENCIAL																	
VALORACIÓN DEL ACTIVO								% IMPACTO					IMPACTO POTENCIAL				
TIPO DE ACTIVO	COD	[A]	[C]	[I]	[D]	[T]	VALOR DEL ACTIVO	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
Personal	(P.06)	5			5		Bajo	50%	60%	50%	50%	0%	2,5	0	0	2,5	0
Personal	(P.07)	5			5		Bajo	50%	60%	50%	50%	0%	2,5	0	0	2,5	0
Personal	(P.08)	5			5		Bajo	50%	60%	50%	50%	0%	2,5	0	0	2,5	0
Personal	(P.09)	5			5		Bajo	50%	60%	50%	50%	0%	2,5	0	0	2,5	0
Personal	(P.10)	5			4		Bajo	50%	60%	50%	50%	0%	2,5	0	0	2	0
Personal	(P.11)	5			4		Bajo	50%	60%	50%	50%	0%	2,5	0	0	2	0
Personal	(P.12)	5			5		Bajo	50%	60%	50%	50%	0%	2,5	0	0	2,5	0
Personal	(P.13)	4			4		Bajo	50%	60%	50%	50%	0%	2	0	0	2	0
Personal	(P.14)	4			4		Bajo	50%	60%	50%	50%	0%	2	0	0	2	0
Personal	(P.15)	4			4		Bajo	50%	60%	50%	50%	0%	2	0	0	2	0
Personal	(P.16)	1			3		Muy bajo	50%	60%	50%	50%	0%	0,5	0	0	1,5	0

4.7. Nivel de riesgo aceptable y riesgo residual

Antes de tocar el tema del riesgo aceptable y riesgo residual, es conveniente tener presente que, de acuerdo con la metodología de la Entidad, los posibles niveles del riesgo inherente se muestran en la siguiente tabla. Este valor es el producto de la frecuencia (o probabilidad) por el impacto.

Tabla 26. Niveles de clasificación de riesgo. Fuente: Manual Administración del riesgo.

			IMPACTO				
			1	2	3	4	5
			Insignificante	Menor	Moderado	Mayor	Catastrófico
FRECUENCIA	5	Casi segura	5 MODERADO	10 ALTO	15 ALTO	20 EXTREMO	25 EXTREMO
	4	Alta	4 MODERADO	8 MODERADO	12 ALTO	16 EXTREMO	20 EXTREMO
	3	Posible	3 INFERIOR	6 MODERADO	9 MODERADO	12 ALTO	15 ALTO
	2	Baja	2 INFERIOR	4 MODERADO	6 MODERADO	8 MODERADO	10 ALTO
	1	Remota	1 INFERIOR	2 INFERIOR	3 INFERIOR	4 MODERADO	5 MODERADO

"Aceptar un riesgo es que una vez analizadas las características del riesgo, su calificación y su nivel residual, se toma la decisión de asumir el riesgo bajo esas condiciones, es decir, que se continuarán con los controles definidos e implementados. Esta decisión es importante, toda

vez que presume que no es necesario un mayor costo en la inclusión de controles, puesto que saldría más costoso dichas soluciones adicionales que el impacto que genera la ocurrencia del riesgo, y por otro lado, se entiende que la Entidad está en la capacidad de gestionar el riesgo residual que se asume"[5].

En este punto es importante tener presente el concepto de *Riesgo Residual*, que hace referencia al riesgo que se mantiene, aún después de aplicar controles o salvaguardas para tratar el riesgo inherente.

El nivel de aceptación de riesgo, para la Empresa de Manejo de Obras, estará determinado por los criterios que se muestran en el siguiente cuadro, que fue extraído del Manual de Administración del Riesgo:

Tabla 27. Criterios de aceptación del riesgo. Fuente: Manual Administración del Riesgo.

Criterios de Aceptación del Riesgo	
NIVEL DE RIESGO RESIDUAL	**DECISIÓN**
Inferior	Se asumen el riesgo residual. No requiere plan de tratamiento. Continúa con los controles existentes.
Moderado	Se asume el riesgo residual. El plan de tratamiento es opcional, a decisión del líder del proceso. Se recomienda establecer tratamiento a las causas que carezcan de controles, o mejorar los controles existentes de acuerdo a sus calificaciones más bajas.
Alto	No se asume el riesgo en estos niveles, por lo tanto se requiere establecer un Plan de Tratamiento.
Extremo	

Una vez se han recordado los conceptos, o en términos coloquiales, con las reglas claras, se procede a calcular el riesgo. En la siguiente tabla, cálculo del riesgo, se pintaron de color azul agua marina los riesgos que están en nivel moderado, en amarillo ocre los que están en nivel alto y en rojo los de nivel extremo, siguiendo los parámetros de las dos tablas previas.

[5] Tomado del Anexo 7b. Manual de Administración del Riesgo.

Tabla 28. Cálculo del riesgo. Elaboración propia.

CÁLCULO DEL RIESGO												
ACTIVO			% IMPACTO					RIESGO				
COD	NOMBRE DEL ACTIVO	FREC.	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
(D.01)	Configuración fortigate	3	2,5	3,75	5	5	0	7,5	11,25	15	15	0
(D.03)	Configuración antivirus	3	2,5	3,75	5	5	0	7,5	11,25	15	15	0
(D.04)	Código fuente de los sistemas de información	3	2,5	3	5	4	0	7,5	9	15	12	0
(D.05)	Licenciamiento software comercial	3	2,5	0,75	5	4	0	7,5	2,25	15	12	0
(D.06)	hojas de vida de los empleados	3	2	3,75	5	4	0	6	11,25	15	12	0
(D.07)	Archivo físico no digitalizado	3	2	3,75	5	4	0	6	11,25	15	12	0
(D.08)	Contratos	3	1,5	1,5	5	3	0	4,5	4,5	15	9	0
(D.09)	Correspondencia radicada	3	1,5	1,5	4	4	0	4,5	4,5	12	12	0
(D.10)	S.I. de inteligencia de negocio (BI)	3	1,5	2,25	3	3	0	4,5	6,75	9	9	0
(D.11)	Datos del sistema ERP	3	1	3	3	4	0	3	9	9	12	0
(D.11)	Datos del sistema de proyectos de obra	3	1	1,5	3	4	0	3	4,5	9	12	0
(D.12)	Datos del CMS	3	1	1,5	3	4	0	3	4,5	9	12	0
(D.13)	Datos de planes de mejoramiento	3	1,5	1,5	3	3	0	4,5	4,5	9	9	0
(D.14)	Datos del sistema de activos de información	3	1,5	2,25	2	3	0	4,5	6,75	6	9	0
(D.15)	datos del sistema de gestión documental.	3	1,5	3	3	3	0	4,5	9	9	9	0
(Aux.01)	Sistema de aire Acondicionado de precisión	4				5		0	0	0	20	0
(Aux.02)	Sistema de detección y extinción de fuego	4				5		0	0	0	20	0
(Aux.03)	Sistema de alimentación ininterrumpida de energía eléctrica	4				5		0	0	0	20	0
(Aux.04)	Sistema de Control de acceso al CPD	4				5		0	0	0	20	0

CÁLCULO DEL RIESGO												
ACTIVO			% IMPACTO					RIESGO				
COD	NOMBRE DEL ACTIVO	FREC.	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
(Aux.05)	Archivadores	4				3		0	0	0	12	0
(HW.01)	Servidores físicos Win2012	4	0	4	4	3	0	0	16	16	12	0
(HW.02)	Servidores físicos Linux Ubuntu	4	0	3	3	3	0	0	12	12	12	0
(HW.03)	Servidores físicos host para virtualizar	4	0	3	3	4	0	0	12	12	16	0
(HW.04)	Solución almacenamiento SAN	4	0	3	3,75	3	0	0	12	15	12	0
(HW.05)	Solución backup	4	0	3	3,75	3	0	0	12	15	12	0
(HW.06)	Fortigate	4	0	3	3,75	3	0	0	12	15	12	0
(I.01)	Centro de Procesamiento de Datos – CPD	4	0	3,75	3,75	4	0	0	15	15	16	0
(I.02)	Cuartos de cableado	4	0	2	3,75	4	0	0	8	15	16	0
(I.03)	Oficinas directivos	4	0	1,5	1,5	4	0	0	6	6	16	0
(I.04)	Puestos de trabajo	4	0	1,5	2,25	1	0	0	6	9	4	0
(I.05)	Edificio principal	4	0	1	3	4	0	0	4	12	16	0
(I.06)	Archívo central	4	0	2,5	3,75	4	0	0	10	15	16	0
(I.07)	Recepción	4	0	1,5	2,25	4	0	0	6	9	16	0
(R.01)	Switch de Core	4	0	1,5	2,25	5	0	0	6	9	20	0
(R.02)	Switch Top of Rack	4	0	3	3	5	0	0	12	12	20	0
(R.03)	Switch de borde	4	0	3	3	4	0	0	12	12	16	0
(R.04)	Canales Internet	4	0	2	4	5	0	0	8	16	20	0
(S.01)	Correo electrónico	4	5	4	4	4	0	20	16	16	16	0
(S.02)	Intranet	4	5	3	4	4	0	20	12	16	16	0
(S.03)	Página web	4	5	3	4	4	0	20	12	16	16	0
(S.04)	Carpetas compartidas	4	5	4	5	3	0	20	16	20	12	0

CÁLCULO DEL RIESGO												
ACTIVO			% IMPACTO					RIESGO				
COD	NOMBRE DEL ACTIVO	FREC.	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
(S.05)	Directorio activo	4	5	5	5	5	0	20	20	20	20	0
(SW.01)	Servidores virtuales producción	4	0	4	4	4	0	0	16	16	16	0
(SW.02)	Servidores virtuales desarrollo	4	0	4	4	4	0	0	16	16	16	0
(SW.03)	Servidores virtuales pruebas	4	0	4	4	4	0	0	16	16	16	0
(SW.04)	Sistema B.I	4	0	5	4	5	0	0	20	16	20	0
(SW.05)	Sistema ERP	4	0	5	4	4	0	0	20	16	16	0
(SW.06)	Sistema Proyectos de Obra	4	0	3	4	5	0	0	12	16	20	0
(SW.07)	CMS	4	0	3	3	4	0	0	12	12	16	0
(SW.08)	S.I. Planes de Mejoramiento	4	0	1	4	3	0	0	4	16	12	0
(SW.09)	S.I. Activos de Infromación	4	0	3	4	2	0	0	12	16	8	0
(SW.10)	S.I. Gestión documental	4	0	5	4	5	0	0	20	16	20	0
(SW.11)	Fortianalyzer	4	0	2	3	1	0	0	8	12	4	0
(SW.12)	Fortisandbox	4	0	2	3	4	0	0	8	12	16	0
(SW.13)	Antivirus	4	0	2	4	5	0	0	8	16	20	0
(SW.14)	Bases de datos de los SI	4	0	4	5	5	0	0	16	20	20	0
(SW.15)	RAC base de datos Oracle	4	0	3	5	5	0	0	12	20	20	0
(SW.16)	Firmware fortigate	4	0	1	5	5	0	0	4	20	20	0
(SW.17)	Sistema Operativo Ubuntu	4	0	1	3	3	0	0	4	12	12	0
(SW.18)	Sistema Operativo Windows	4	0	1	3	3	0	0	4	12	12	0
(SW.19)	Hipervisor	4	0	2	3	4	0	0	8	12	16	0
(P.01)	Director	4	2,5	0	0	2,5	0	10	0	0	10	0
(P.02)	Subdirector de Proyectos	4	2,5	0	0	2,5	0	10	0	0	10	0

CÁLCULO DEL RIESGO												
ACTIVO			% IMPACTO					RIESGO				
COD	NOMBRE DEL ACTIVO	FREC.	[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
(P.03)	Subdirector de Infraestructura	4	2,5	0	0	2,5	0	10	0	0	10	0
(P.04)	Subdirector Jurídico	4	2,5	0	0	2,5	0	10	0	0	10	0
(P.05)	Jefe Contratación	4	2,5	0	0	2,5	0	10	0	0	10	0
(P.06)	Secretario General	4	2,5	0	0	2,5	0	10	0	0	10	0
(P.07)	Jefe Administración Financiera	4	2,5	0	0	2,5	0	10	0	0	10	0
(P.08)	Jefe Recursos Físicos	4	2,5	0	0	2,5	0	10	0	0	10	0
(P.09)	Administrador Base de Datos	4	2,5	0	0	2,5	0	10	0	0	10	0
(P.10)	Oficial de Seguridad	4	2,5	0	0	2	0	10	0	0	8	0
(P.11)	Arquitecto de TI	4	2,5	0	0	2	0	10	0	0	8	0
(P.12)	Operador CPD	4	2,5	0	0	2,5	0	10	0	0	10	0
(P.13)	Webmaster	4	2	0	0	2	0	8	0	0	8	0
(P.14)	Operador de Redes y Comunicaciones	4	2	0	0	2	0	8	0	0	8	0
(P.15)	Responsable Mesa de Servicios	4	2	0	0	2	0	8	0	0	8	0
(P.16)	Operador Mesa de Servicios	4	0,5	0	0	1,5	0	2	0	0	6	0

4.8. Conclusiones

Los activos más críticos son Servicios y Software, seguidos por los Equipos Auxiliares, Redes y Hardware, en esta última específicamente los servidores físicos con Windows.

Las amenazas que mayor afectación pueden causar a los activos son las del grupo A-8 Por Control y A-5 Por Software.

En los activos de tipo personal, la dimensión que mayor criticidad presenta es la confidencialidad.

5. Propuestas de Proyectos

Después de tener un análisis de riesgos detallado, como el presentado en el capítulo anterior, se precisa plantear unos proyectos que le permitan a la Empresa de Manejo de Obras, mitigar los riesgos más críticos, y a su vez, cerrar la brecha frente al cumplimiento de la norma de referencia.

Teniendo en cuenta el nivel de cumplimiento inicial que demarcó el avance en la implementación de la norma, los proyectos que se planearán en seguida, se deberán desarrollar en un término no mayor a dos (2) años calendario.

Las Amenazas con mayor probabilidad de materialización, después de analizar la frecuencia y el impacto potencial son las siguientes 15:

- A-1.1 Desastre Natural - Temblor (Sísmicos)
- A-3.4 Daño Accidental - Incendio (Fuego)
- A-3.5 Daño Accidental - Agua o Suciedad (Daño por agua)
- A-4.1 Falla de suministro de energía
- A-4.2 Falla de suministro de energía de respaldo (UPS)
- A-6.7 Acceso a red por usuario no autorizado
- A-7.2 Errores de transmisión
- A-7.6 Falla de los servicios de comunicación
- A-7.8 Daño a las líneas de comunicación
- A-7.11 Déficit de personal
- A-7.12 Errores de Usuario
- A-8.9 Eliminación negligente de datos
- A-8.14 Negación de Servicios
- A-8.18 Falla para cambiar contraseñas regularmente
- A-8.19 Falla para usar medidas de seguridad proporcionadas

De la misma manera, al analizar los tipos de activo con mayor afectación por los riesgos, encontramos que en nivel extremo están: Equipamiento auxiliar, Instalaciones, Redes, Servicios y Software, mientras que en nivel alto están Datos, Hardware y Personal.

De otra parte, si se retoma el análisis diferencial frente a la implementación de los controles de la guía técnica colombiana GTC-ISO/IEC 27002:2015, y se identifican los dominios de menor cumplimiento, se pueden mencionar los siguientes cinco (5):

Tabla 29. Dominios con menor grado de implementación. Fuente propia.

DOMINIOS DE MENOR IMPLEMENTACIÓN		
NUMERAL	DOMINIO	% CUMPL
A.17	Aspectos de seguridad de la información de la gestión de continuidad de negocio	7%
A.16	Gestión de incidentes de seguridad de la información	23%
A.15	Relación con los proveedores	29%
A.7	Seguridad de los recursos humanos	38%
A.14	Adquisición, desarrollo y mantenimiento de sistemas	41%

Con estos tres insumos mencionados previamente, se plantean los siguientes proyectos integrales.

5.1. Propuestas

Con los riesgos identificados y calificados, y los dominios de menor implementación en la Empresa, se plantean los siguientes proyectos, que se espera permitan a la empresa de Manejo de Obras y en particular a su SGSI, mitigar los riegos encontrados. Se proponen en total nueve (9) proyectos, que se resumen en la siguiente tabla, y se amplían en seguida:

PROYECTOS PROPUESTOS		
Cod	Nombre	Costo
PR.01	Sensibilización y entrenamiento en seguridad de la información	COP$ 28.000.000
PR.02	Plan de Recuperación de Desastres	COP$ 1.800.000.000
PR.03	Modernización de las UPS	COP$ 376.000.000
PR.04	Modernización del cableado estructurado	COP$ 600.000.000
PR.05	Adquisición e implantación de un sistema DLP	COP$ 25.000.000
PR.06	Gestión de incidentes de seguridad	COP$ 0
PR.07	Hacer parte de un CSIRT de gobierno	COP$ 0
PR.08	Actualizar la documentación operativa (políticas y procedimientos)	COP$ 0
PR.09	Definir una metodología de desarrollo de software seguro	COP$ 0
	TOTAL	COP$ 2.829.000.000
		USD$ 1.000.000

Código del proyecto: PR.01
Nombre del proyecto: Sensibilización y entrenamiento en seguridad de la información
Responsable: Oficial de seguridad de la Información
Dominios afectados: A.7 Seguridad de los recursos humanos

Duración: 1 año. Esta duración es la inicial, pues este tipo de proyecto es permanente y se debe renovar año a año.
Costos: COP$ 28.000.000
Riesgo (s) a mitigar:

- A-7.12 Errores de Usuario
- A-8.18 Falla para cambiar contraseñas regularmente
- A-8.19 Falla para usar medidas de seguridad proporcionadas

Impacto sobre los dominios de la seguridad: Ver sección 5.2. Resultados

Código del proyecto: PR.02
Nombre del proyecto: Plan de Recuperación de Desastres
Responsable: Jefe Oficina Asesora de Tecnología
Dominios afectados: A.17.1 Continuidad de seguridad de la información
Duración: 6 meses (el plan y los servicios se contratarán a 3 años)
Costos: COP$ 1.800.000.000
Riesgo (s) a mitigar:

- A-1.1 Desastre Natural - Temblor (Sísmicos)
- A-3.4 Daño Accidental - Incendio (Fuego)
- A-3.5 Daño Accidental - Agua o Suciedad (Daño por agua)
- A-4.1 Falla de suministro de energía)

Impacto sobre los dominios de la seguridad: Ver sección 5.2. Resultados

Código del proyecto: PR.03
Nombre del proyecto: Modernización de las UPS
Responsable: Jefe Oficina Asesora de Tecnología
Dominios afectados: A.17.1 Continuidad de seguridad de la información
Duración: 10 meses
Costos: COP$ 376.000.000
Riesgo (s) a mitigar:

- A-4.1 Falla de suministro de energía)
- A-4.2 Falla de suministro de energía de respaldo (UPS)
- A-8.14 Negación de Servicios

Impacto sobre los dominios de la seguridad: Ver sección 5.2. Resultados

Código del proyecto: PR.04
Nombre del proyecto: Modernización del cableado estructurado
Responsable: Jefe Oficina Asesora de Tecnología
Dominios afectados:

- A.16 Gestión de incidentes de seguridad de la información
- A.17.1 Continuidad de seguridad de la información

Duración: 10 meses
Costos: COP$600.000.000
Riesgo (s) a mitigar:

- A-7.2 Errores de transmisión
- A-7.6 Falla de los servicios de comunicación

- A-7.8 Daño a las líneas de comunicación

Impacto sobre los dominios de la seguridad: Ver sección 5.2. Resultados

Código del proyecto: PR.05
Nombre del proyecto: Adquisición e implantación de un sistema DLP
Responsable: Jefe Oficina de Seguridad de la Información
Dominios afectados: A.8. Gestión de activos
Duración: 8 meses
Costos: COP$ 25.000.000
Riesgo (s) a mitigar:

- A-7.12 Errores de Usuario
- A-8.9 Eliminación negligente de datos

Impacto sobre los dominios de la seguridad: Ver sección 5.2. Resultados

Código del proyecto: PR.06
Nombre del proyecto: Gestión de incidentes de seguridad
Responsable: Oficial de Seguridad de la Información
Dominios afectados: A.16. Gestión de incidentes de seguridad de la información
Duración: 3 meses
Costos: COP$ 0
Riesgo (s) a mitigar:

- A-8.14 Negación de Servicios

Impacto sobre los dominios de la seguridad: Ver sección 5.2. Resultados

Código del proyecto: PR.07
Nombre del proyecto: Hacer parte de un CSIRT de gobierno
Dominios afectados: A.16. Gestión de incidentes de seguridad de la información
Duración: 2 meses
Costos: COP$ 0
Riesgo (s) a mitigar:

- A-8.9 Eliminación negligente de datos
- A-8.14 Negación de Servicios

Impacto sobre los dominios de la seguridad: Ver sección 5.2. Resultados

Código del proyecto: PR.08
Nombre del proyecto: Actualizar la documentación operativa (políticas y procedimientos)
Responsable: Oficial de Seguridad de la Información
Dominios afectados:

- 7.5. Información documentada
- A.6 Organización de la seguridad de la información
- A.15. Relaciones con los proveedores (en la medida en que se puede documentar la forma de proteger la información, en la relación contractual)

Duración: 6 meses
Costos: COP$ 0
Riesgo (s) a mitigar:

- A-8.19 Falla para usar medidas de seguridad proporcionadas

Impacto sobre los dominios de la seguridad: Ver sección 5.2. Resultados

Código del proyecto: PR.09
Nombre del proyecto: Definir una metodología de desarrollo de software seguro
Responsable: Jefe Oficina Asesora de Tecnología – Jefe Oficina de Seguridad de la Información
Dominios afectados:

- A.12.1.4. Separación de los ambientes de desarrollo, prueba y operación
- A.14 Adquisición, desarrollo y mantenimiento de sistemas

Duración: 2 meses
Costos: COP$ 0
Riesgo (s) a mitigar:

- A-8.14 Negación de Servicios

Impacto sobre los dominios de la seguridad: Ver sección 5.2. Resultados

Diagramas de planificación de los proyectos en el tiempo

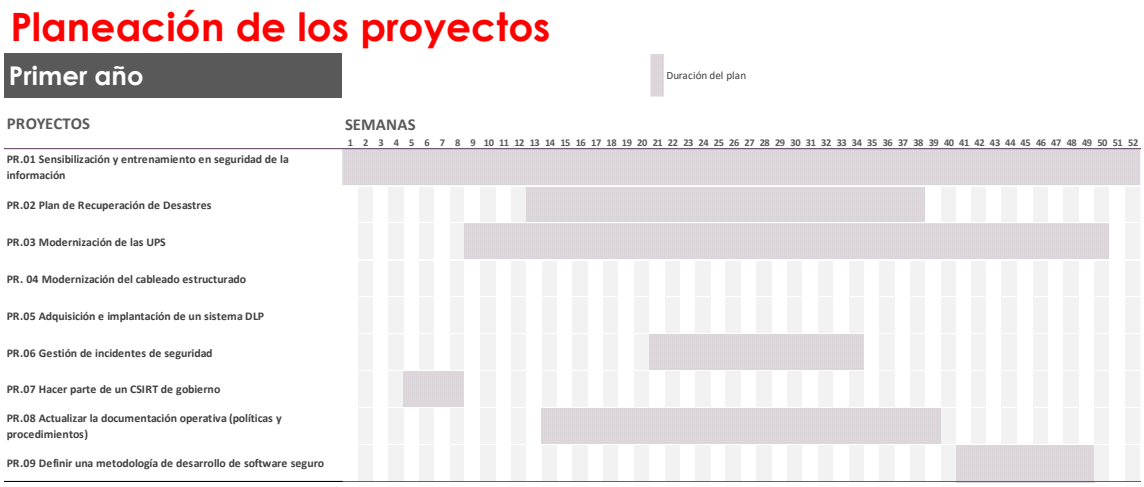


Ilustración 8. Planeación temporal de los proyectos propuestos para el primer año. Fuente propia

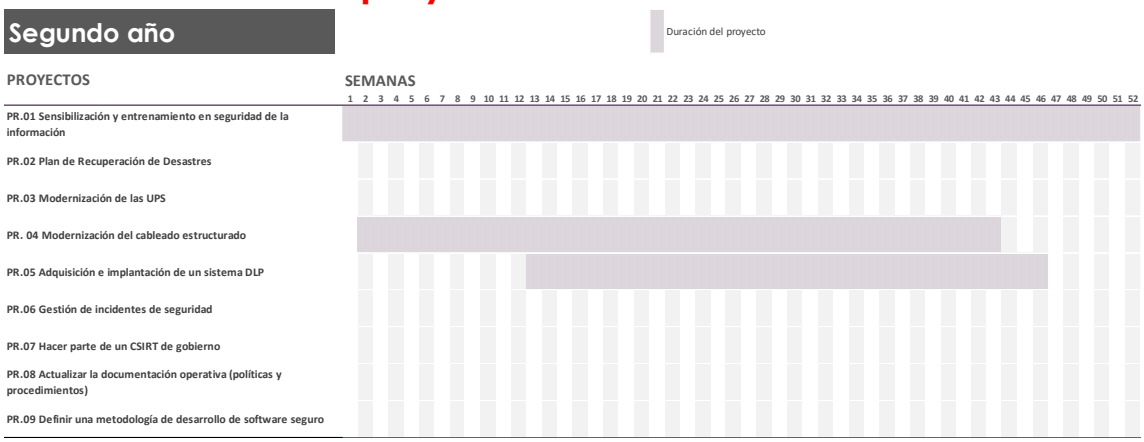


Ilustración 9. Planeación temporal de los proyectos propuestos para el segundo año. Fuente propia

5.2. Resultados

Una vez que los proyectos planteados se finalicen, se espera tener el siguiente estado de cumplimiento frente a la guía técnica GTC-ISO-IEC 27002:2015

Tabla 30. Estado esperado de los controles luego de los proyectos. Fuente propia.

EVOLUCIÓN EN EL CUMPLIMIENTO DE CONTROLES LUEGO DE FINALIZAR LOS PROYECTOS			
Nombre dominios	Cumplimiento actual	Primer año	Segundo año
A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	100%	100%	100%
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	48%	75%	80%
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	38%	65%	85%
A.8 GESTIÓN DE ACTIVOS	68%	72%	90%
A.9 CONTROL DE ACCESO	73%	75%	80%
A.10 CRIPTOGRAFÍA	60%	62%	65%
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	87%	90%	92%
A.12 SEGURIDAD DE LAS OPERACIONES	62%	75%	95%
A.13 SEGURIDAD DE LAS COMUNICACIONES	69%	70%	73%
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	41%	85%	90%
A.15 RELACIÓN CON LOS PROVEEDORES	29%	60%	65%
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	23%	65%	92%
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	7%	70%	94%
A.18 SEGURIDAD DE LAS COMUNICACIONES	72%	73%	75%

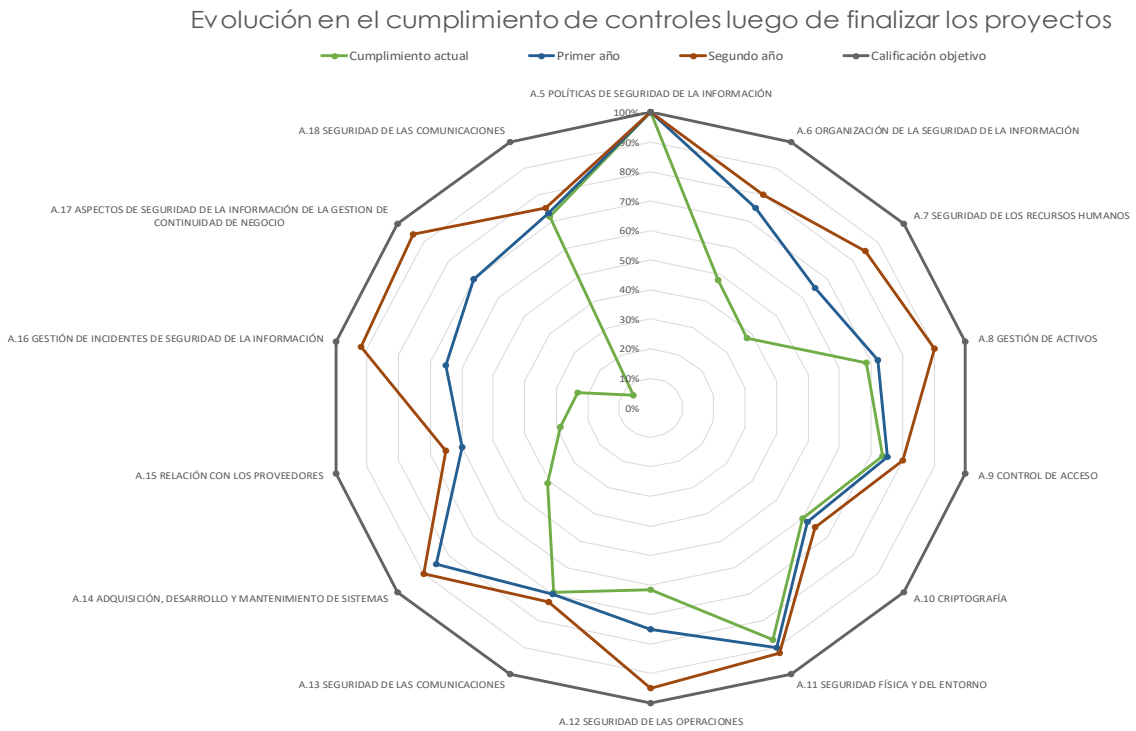


Ilustración 10. Evolución de los controles luego de finalizar los proyectos. Fuente propia.

6. Auditoría de Cumplimiento

Una vez que se han desarrollado los proyectos planteados para mitigar los riesgos encontrados, se presume que la Empresa de Manejo de Obras tiene la madurez necesaria para certificar su SGSI, en este sentido se parte del hecho de que el proceso de auditoría ocurre después de finalizar la implementación de los proyectos propuestos en el capítulo anterior.

De esta manera, el primer paso es adelantar una auditoría interna que permita evaluar el estado de la implementación del sistema de gestión, contra la norma de referencia, NTC-ISO/IEC-27001:2013, específicamente los controles del anexo A de la citada norma.

6.1. Metodología

La auditoría se basará en la evaluación de cumplimiento o capacidad y madurez de los controles del Anexo A de la norma NTC-ISO/IEC 27001:2013. Para ello, se empleará el modelo CMM, o Modelo de Capacidad y Madurez, con base en la siguiente escala de valoración:

Tabla 31. Modelo de Madurez de la Capacidad. Descripción tomada de https://es.wikipedia.org/wiki/Modelo_de_Capacidad_y_Madurez

MODELO DE CAPACIDAD Y MADUREZ			
EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	L0	Inexistente	Carencia completa de cualquier control reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10% - 49%	L1	Inicial / Ad-hoc	Aunque se utilicen técnicas correctas, los esfuerzos se ven minados por falta de planificación. El éxito de los controles se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. La efectividad de los controles es impredecible.
50% - 69%	L2	Reproducible, pero intuitivo	En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión de los controles, existen unas métricas básicas y un razonable seguimiento de la calidad. La relación con subcontratistas y clientes está gestionada sistemáticamente. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
70% - 85%	L3	Definido	Además de una buena gestión de los controles, a este nivel las organizaciones disponen de correctos procedimientos de coordinación entre grupos, formación del personal, técnicas de ingeniería más detalladas y un nivel más avanzado de métricas en los procesos. Se implementan técnicas de revisión por pares.

MODELO DE CAPACIDAD Y MADUREZ			
EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
86% - 99%	L4	Gestionado y medible	Se caracteriza porque las organizaciones disponen de un conjunto de métricas significativas de calidad y productividad, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. La efectividad de los controles es alta.
100%	L5	Optimizado	La organización completa está volcada en la mejora continua de los procesos, incluyendo los controles de la seguridad de la información. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

La evaluación de los controles se realizará mediante un análisis de los recursos disponibles: documentación existente dentro de la Empresa, reportes de evidencias, reportes de incidentes, reportes de funcionamiento, reportes de evaluaciones, informes de auditorías pasadas, reportes de entrevistas y observaciones realizadas in situ.

6.2. Evaluación de la Madurez

Para realizar la evaluación se empleará la siguiente tabla, que cita cada uno de los 114 controles. Se incluye una casilla para indicar si cumple o no, en caso de ser positivo, el nivel de cumplimiento y una casilla más para incluir una observación del equipo auditor.

Tabla 32. Evaluación de la Madurez de los Controles

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			L5	
A.5.1. ORIENTACION DE LA DIRECCION PARA LA GESTION DE LA SEGURIDAD DE LA INFORMACION	Brindar orientación y soporte, por parte de la Dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.		L5	
A.5.1.1. Políticas para la seguridad de la información	DEBE definir un conjunto de políticas para la Seguridad de la Información, aprobadas por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.	Sí	L5	En la Empresa de Manejo de Obras se cuenta con 2 documentos de políticas, uno aprobado mediante la resolución 34217 de 2015, que incluye unas políticas obligatorias y de alto nivel. Y un Documento de Políticas Operacionales de Seguridad de la Información.
A.5.1.2. Revisión de las políticas para la seguridad de la información	Las políticas para la seguridad de la información se DEBEN revisar a intervalos planificados o si ocurren cambios significativos para asegurar su conveniencia, adecuación y eficacias continúas.	Sí	L5	Existe un plan de revisión de las políticas de manera periódica, al menos una vez al año, o cada vez que se presente un cambio significativo. Sin embargo, no hay registro de revisiones de las políticas hasta ahora.
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			L4	
A.6.1. ORGANIZACIÓN INTERNA	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la Seguridad de la Información dentro de la organización.		L4	

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.6.1.1. Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar TODAS las responsabilidades de la Seguridad de la Información.	Sí	L4	Los roles y las responsabilidades están claramente asignadas. La Oficina de Seguridad de la Información depende directamente de la dirección. Los responsables de los activos están claramente identificados. Existe un documento en el que figuran los diferentes roles y responsabilidades.
A.6.1.2. Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación No Autorizada o No Intencional, o el uso indebido de los activos de la organización.	Sí	L4	Se tiene definido un solo propietario para cada activo crítico. Ningún funcionario tiene autorización para cambiar o modificar activos sin el lleno de los requisitos.
A.6.1.3. Contacto con las autoridades	Se deben mantener contactos apropiados con las autoridades pertinentes.	Sí	L5	Luego de la implementación del proyecto PR.07 Hacer parte de un CSIRT de gobierno le ha permitido a La Empresa mantenerse en contacto permanente con las autoridades.
A.6.1.4. Contacto Con Grupos De Interés Especiales	Se deben mantener contactos apropiados con los grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	Sí	L4	Se crearon dos grupos de distribución para mantenerse en contacto permanente, uno a través de correo electrónico, a través del cual se reciben boletines de actualidad en temas de seguridad de la información. Y un segundo grupo a través de Whatsapp, mediante el cual se comparten noticias más rápidas sobe seguridad de la información, así como alertas de posibles incidentes o vulnerabilidades. En los 2 grupos hay 8 funcionarios, entre personas de la oficina de seguridad y de la de tecnología.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.6.1.5. Seguridad de la información en la gestión de proyectos	La seguridad de la Información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	Sí	L3	La Empresa cuenta con un profesional de proyectos que orienta la aplicación de la metodología PMI. Asimismo, se tiene un formato a manera de lista de verificación, para comprobar la seguridad de la información en los proyectos. Sin embargo, este último no se utiliza masivamente.
A.6.2. DISPOSITIVOS MÓVILES Y TELETRABAJO	Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.		L4	
A.6.2.1. Política para dispositivos móviles.	Se DEBE adoptar una POLÍTICA y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Sí	L4	Se encuentra adoptada la política correspondiente, mediante la resolución 34217 de 2015.
A.6.2.2. Teletrabajo.	Se DEBE implementar una POLÍTICA y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza el teletrabajo.	Sí	L4	Se encuentra adoptada la política correspondiente, mediante la resolución 34217 de 2015.
A.7. SEGURIDAD DE LOS RECURSOS HUMANOS			L4	
A.7.1. ANTES DE ASUMIR EL EMPLEO	Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.		L3	
A.7.1.1. Selección	Las verificaciones de los antecedentes de TODOS los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben proporcionales a los requisitos del negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	Sí	L3	Por ser una empresa de orden gubernamental, se deben seguir unos controles de ley en la vinculación de los funcionarios de carrera administrativa, quienes se vinculan al ganarse el derecho por un concurso de méritos. Por otra parte, en la vinculación de contratistas, se tienen algunos vacíos, pues la selección no es estándar.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.7.1.2. Términos y condiciones del empleo	Los acuerdos contractuales con los empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	Sí	L3	Se publicó una guía de roles y responsabilidades, en la que se especifican estas.
A.7.2. DURANTE LA EJECUCION DEL EMPLEO	Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.		L4	
A.7.2.1. Responsabilidades de la dirección	La dirección DEBE exigir a todos los empleados y contratistas la aplicación de la Seguridad de la Información de acuerdo con las políticas y procedimientos establecidos por la organización.	Sí	L4	La Empresa ha dado las directivas sobre la importancia de la seguridad de la información y las consecuencias de no respetar las políticas definidas. Los funcionarios y contratistas tienen definido un programa de formación / información / concienciación sobre políticas y procedimientos y sus responsabilidades
A.7.2.2. Toma de conciencia, educación y formación en la seguridad de la información	TODOS los empleados de la organización, y en donde sea pertinente, los contratistas, DEBEN recibir la educación y formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	Sí	L4	Las entidades deben formular el Plan Institucional de Capacitación, sin embargo en este no pueden participar los contratistas. También se realizaron sesiones de inducción y reinducción (para personal de carrera) y otras de presentación de la empresa para contratistas de apoyo.
A.7.2.3. Proceso disciplinario	Se DEBE contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la Seguridad de la Información.	Sí	L4	Se cuenta con un procedimiento documentado y aprobado sobre el proceso disciplinario.
A.7.3. TERMINACION Y CAMBIO DE EMPLEO	Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.		L4	

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.7.3.1. Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de Seguridad de la Información que permanecen válidos después de la terminación o cambio de empleo se DEBEN definir, comunicar al empleado o contratista y se deben hacer cumplir.	Sí	L4	Se incluyen estas responsabilidades en los manuales de funciones del personal de carrera administrativa y en las cláusulas de los contratos.
A.8. GESTION DE ACTIVOS			L5	
A.8.1. RESPONSABILIDAD POR LOS ACTIVOS	Identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.		L5	
A.8.1.1. Inventario de activos	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información y se debe elaborar y mantener un inventario de estos activos	Sí	L5	Se cuenta con un sistema de información que permite la toma y actualización de los inventarios de activos de información. Se tiene un procedimiento formalizado y se hace la actualización mínimo una vez al año.
A.8.1.2. Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.	Sí	L5	Todos los activos de información identificados tienen un propietario asignado.
A.8.1.3. Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de la INFORMACION y de los ACTIVOS asociados con información e instalaciones de procesamiento de información.	Sí	L4	Se cuenta con el instructivo IN-TI-06 Uso adecuado de los recursos de TI, el cual fue divulgado a través de los medios internos.
A.8.1.4. Devolución de activos	TODOS los empleados y usuarios de partes externas DEBEN devolver todos los activos de la organización que se encuentren a su cargo. Al terminar su empleo, contrato o acuerdo.	Sí	L4	El proceso Gestión del Talento Humano tiene dentro del procedimiento de desvinculación, el requerimiento de diligenciar el formato FO-TH-22 Paz y salvo para el retiro de funcionarios de planta y contratistas.
A.8.2. CLASIFICACION DE LA INFORMACION	Asegurar que la información recibe un NIVEL apropiado de PROTECCION, de acuerdo con su importancia para la organización.		L3	

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.8.2.1. Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o modificación no autorizada.	Sí	L2	Se tiene un lineamiento sobre la clasificación de la información, pero hace falta divulgación de la misma.
A.8.2.2. Etiquetado y manejo de información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Sí	L2	Se tiene un lineamiento sobre el etiquetado de la información, pero hace falta divulgación de la misma.
A.8.2.3. Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación adoptado por la organización.	Sí	L4	Se tienen un procedimiento y un instructivo para el manejo de los activos de información. Se han realizado jornadas de divulgación y sensibilización sobre el tema, en cada una de las dependencias durante los dos últimos años.
A.8.3. MANEJO DE MEDIOS	Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.		L3	
A.8.3.1. Gestión de medios removibles	Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Sí	L3	Se tiene el instructivo IN-TI-05 Uso adecuado de los dispositivos de almacenamiento de información, aunque falta mayor divulgación para masificar su utilización.
A.8.3.2. Disposición de los medios	Se debe disponer en forma segura del os medios cuando ya no se requieran, usando procedimientos formales.	Sí	L4	Se tiene el instructivo IN-TI-15 Borrado seguro y formateo final de equipos, el cual es aplicado por el personal de la mesa de servicios, ante la solicitud de baja de los bienes.
A.8.3.3. Transferencia de medios físicos	Los medios que contienen información, se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Sí	L3	Se tiene el Instructivo IN-TI-05 uso adecuado de los dispositivos de almacenamiento de información, aunque falta mayor divulgación para masificar su utilización.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.9. CONTROL DE ACCESO			L4	
A.9.1. REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO.	Limitar acceso a información y a instalaciones de procesamiento de información.		L4	
A.9.1.1. Política de control de acceso	Se DEBE establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Sí	L4	Se tienen las políticas de seguridad de la información de alto nivel, adoptadas con la resolución 34217 de 2015, y el Manual de seguridad y vigilancia (MG-RF-03)en los que se definen los lineamientos sobre el acceso a la información y a las instalaciones restringidas.
A.9.1.2. Acceso a redes y a servicios de red	Se DEBE permitir acceso de los usuarios a la red para los que hayan sido autorizados específicamente.	Sí	L4	Se tiene el procedimiento PR-TI-23 Gestión de telecomunicaciones, que es aplicado en los casos que se han necesitado.
A.9.2. GESTIÓN DE ACCESO A USUARIOS.	Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.		L4	
A.9.2.1. Registro y cancelación del registro de usuarios.	Se DEBE implementar un proceso FORMAL de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Sí	L5	El procedimiento PR-TI-02 Gestionar usuarios tecnológicos se emplea con frecuencia. Se ha implementado un sistema de apoyo para facilitar el registro y cancelación del registro de usuarios. Ver Sistema de Información CHIE módulo Gestión TIC.
A.9.2.2. Suministro de acceso a usuarios.	Se DEBE implementar un proceso de suministro de acceso formal de usuario para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	Sí	L4	Se tiene el procedimiento PR-TI-02 Gestionar usuarios tecnológicos, el cual es aplicado continuamente por las personas que tienen el rol apropiado para crear nuevos usuarios.
A.9.2.3. Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Sí	L3	Se cuenta con el instructivo IN-TI-16 Revisión de los Derechos de Acceso de los Usuarios, sin embargo no se utiliza regularmente.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.9.2.4. Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	Sí	L4	Se tiene el procedimiento PR-TI-02 Gestionar usuarios tecnológicos, el cual es aplicado continuamente por las personas que tienen el rol apropiado para crear nuevos usuarios.
A.9.2.5. Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Sí	L3	Se cuenta con el instructivo IN-TI-16 Revisión de los Derechos de Acceso de los Usuarios, sin embargo no se utiliza regularmente.
A.9.2.6. Retiro o ajuste de los derechos de acceso	Los derechos de acceso de TODOS los empleados y de los usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Sí	L4	El procedimiento PR-TI-02 Gestionar usuarios tecnológicos se emplea con frecuencia. Se ha implementado un sistema de apoyo para facilitar el registro y cancelación del registro de usuarios. Ver Sistema de Información CHIE módulo Gestión TIC.
A.9.3. RESPONSABILIDADES DE LOS USUARIOS.	Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.		L4	
A.9.3.1. Uso de información de autenticación secreta.	Se debe EXIGIR a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Sí	L4	Existen directivas dentro de la organización sobre las prácticas en materia de manejo de claves, como el procedimiento PR-TI-02 Gestionar usuarios tecnológicos. Este asunto forma parte del temario de la formación en seguridad que los empleados siguen. Estas directivas se encuentran definidas dentro de las políticas de seguridad de la empresa.
A.9.4. CONTROL DE ACCESO A SISTEMAS Y APLICACIONES.	Evitar el acceso no autorizado a sistemas y aplicaciones.		L3	
A.9.4.1. Restricción de acceso a la información.	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Sí	L3	Instructivo IN-TI-22 uso adecuado de las carpetas compartidas. Se tiene control de los roles y perfiles de los usuarios que acceden a las aplicaciones.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.9.4.2. Procedimiento de ingreso seguro.	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	Sí	L4	Con el procedimiento PR-TI-02 Gestionar usuarios tecnológicos se controlan los requerimientos de acceso a los sistemas. Se ha implementado un sistema de apoyo para facilitar el registro y cancelación del registro de usuarios. Ver Sistema de Información CHIE módulo Gestión TIC.
A.9.4.3. Sistemas de gestión de contraseñas.	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Sí	L4	Procedimiento PR-TI-02 Gestionar usuarios tecnológicos. Instructivo IN-TI-07 Administración del directorio activo. Guía GU-TI-02 Manejo de credenciales TIC en contingencia. A través del Directorio Activo se realiza la gestión de las contraseñas y se controlan las políticas de robustez de las mismas.
A.9.4.4. Uso de programas utilitarios privilegiados.	Se debe restringir y controlar ESTRICTAMENTE el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	Sí	L2	Se cuenta con el Instructivo IN-TI-35 Uso de herramientas de la mesa de servicios. Con este documento se identifica y delimita el uso las herramientas especializadas de software para la prestación de soporte informático.
A.9.4.5. Control de acceso a códigos fuente de programas.	Se debe restringir el acceso a los códigos fuente de los programas.	Sí	L3	Se cuenta con el instructivo IN-TI-36 Gestión de la Configuración de Software. Sin embargo, por su reciente publicación, aún no está suficientemente apropiado.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.10. CRIPTOGRAFIA			L3	
A.10.1. CONTROLES CRIPTOGRAFICOS	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.		L3	
A.10.1.1. Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una POLITICA sobre el uso de controles criptográficos para la protección de la información.	Sí	L3	Se encuentra adoptada la política correspondiente, mediante la resolución 34217 de 2015. Instructivo IN-TI-08 Protección de la información digital. Instructivo IN-TI-19 Aplicación de cifrado.
A.10.1.2. Gestión de llaves	Se debe desarrollar e implementar una POLITICA sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	Sí	L3	Se encuentra adoptada la política correspondiente, mediante la resolución 34217 de 2015. Instructivo IN-TI-08 Protección de la información digital. Instructivo IN-TI-19 Aplicación de cifrado. Se cuenta con los documentos mencionados, sin embargo se evidencia que hace falta apropiación por parte de los usuarios.
A.11. SEGURIDAD FÍSICA Y DEL ENTORNO			L5	
A.11.1. ÁREAS SEGURAS.	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.		L5	

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.11.1.1. Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	Sí	L5	Manual MG-RF-03 Seguridad y vigilancia. Los perímetros de seguridad están claramente definidos y son respetados por los funcionarios y contratistas.
A.11.1.2. Controles de acceso físicos	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	Sí	L5	Manual MG-RF-03 Seguridad y vigilancia. Los perímetros de seguridad están claramente definidos y están protegidos por controles de acceso biométricos o mediante tarjeta de acceso.
A.11.1.3. Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	Sí	L5	Manual MG-RF-03 Seguridad y vigilancia. Los perímetros de seguridad están claramente definidos y están protegidos por controles de acceso biométricos o mediante tarjeta de acceso.
A.11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Sí	L4	Se cuenta con un Plan Institucional de Respuesta a Emergencias. Manual MG-RF-03 Seguridad y vigilancia.
A.11.1.5. Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	Sí	L5	Manual MG-RF-03 Seguridad y vigilancia. A las áreas seguras sólo se puede acceder con autorización y acompañamiento de un funcionario del área.
A.11.1.6. Áreas de despacho y carga	Se deben controlar puntos de acceso tales como áreas de despacho y de carga y otros puntos donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	Sí	L5	Manual MG-RF-03 Seguridad y vigilancia. Las áreas de carga y descarga son de acceso público y se encuentran físicamente aisladas de las áreas de trabajo del personal y de las áreas de tratamiento de la información. Para ingresar y salir de estas áreas se necesita de autorización.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.11.2. EQUIPOS.	Prevenir pérdida, daño, robo o compromiso de activos, y la interceptación de operaciones de la organización.		L4	
A.11.2.1. Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Sí	L4	Instructivo IN-TI-06 Uso adecuado de los recursos de TI. El CPD se encuentra dentro de un área ya protegida. Se cuenta con vigilancia privada para proteger las áreas.
A.11.2.2. Servicios de suministro.	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Sí	L5	Se tiene un sistema de Ups en alta disponibilidad para los equipos del CPD
A.11.2.3. Seguridad del cableado.	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	Sí	L5	El cableado estructurado cumple con la norma TIA/EIA-568-B. Se tiene adoptado y se cumple el procedimiento PR-TI-23 Gestión de telecomunicaciones.
A.11.2.4. Mantenimiento de equipos.	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Sí	L5	El mantenimiento de los equipos se contrata para todo el año con un proveedor externo.
A.11.2.5. Retiro de activos.	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	Sí	L4	En el Manual MG-RF-03 Seguridad y vigilancia se incluyen los lineamientos al respecto, sin embargo se han presentado incidentes relacionados con la pérdida de equipos de usuario final.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones.	Se deben aplicar medidas se seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones. (Incluir actividades de Teletrabajo y de salidas en comisión a sitios diferentes al puesto natural de trabajo).	Sí	L4	Manual administración del programa de seguros para los bienes de la Empresa de Manejo de Obras (MG-RF-002) Instructivo de Uso adecuado de los dispositivos de almacenamiento de información (IN-TI-05). En la práctica, los equipos que se retiran de la entidad, van acompañados de un cable de seguridad para ser "amarrados" en el sitio de destino.
A.11.2.7. Disposición segura o reutilización de equipos.	Se deben verificar TODOS los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.	Sí	L5	Se tiene el instructivo IN-TI-15 Borrado seguro y formateo final de equipos, el cual es aplicado por el personal de la mesa de servicios, ante la solicitud de baja.
A.11.2.8. Equipos de usuario desatendidos.	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección adecuada.	Sí	L4	Instructivo de administración del directorio activo (IN-TI-07) Documento DU-TI-06 Políticas Operacionales de Seguridad de la Información. Políticas de directorio activo sobre cierre de sesiones.
A.11.2.9. Política de escritorio limpio y pantalla limpia.	Se DEBE adoptar una POLÍTICA de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	Sí	L4	Se tienen las políticas de seguridad de la información de alto nivel, adoptadas con la resolución 34217 de 2015. Sin embargo, algunos usuarios aún no la aplican.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.12. SEGURIDAD DE LAS OPERACIONES			L4	
A.12.1. PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.		L4	
A.12.1.1. Procedimientos de operación documentados	Los procedimientos de operación SE DEBEN DOCUMENTAR y poner a disposición de todos los usuarios que los necesitan.	Sí	L4	Se tiene el 100% de los documentos requeridos por la norma y un 90% de los planeados por elaborar.
A.12.1.2. Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamientos de información que afectan la seguridad de la información.	Sí	L4	Con base en el procedimiento PR-TI-08 Gestión de cambios que se aplican únicamente a temas tecnológicos, se realiza una mesa de trabajo semanal para presentar y discutir los cambios del siguiente periodo.
A.12.1.3. Gestión de capacidad	Se debe hacer seguimiento al uso de los recursos, hacer los ajustes y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	Sí	L3	Se aplica el procedimiento PR-TI-16 Gestión de capacidad y disponibilidad en forma periódica, cada 3 meses.
A.12.1.4. Separación de los ambientes de desarrollo, prueba y operación	Se deben separar los ambientes de desarrollo, pruebas y operación (producción), para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	Sí	L3	Los ambientes de producción, pruebas y desarrollo de software están separados formalmente mediante el instructivo IN-TI-37 Definición y uso de los ambientes de trabajo para desarrollo de software
A.12.2. PROTECCION CONTRA CODIGO MALICIOSO	Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.		L4	
A.12.2.1. Controles contra códigos maliciosos	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Sí	L4	Se tiene un software antivirus de tipo corporativo, y se complementa con el instructivo IN-TI-21 Uso del antivirus en los equipos de usuario final.
A.12.3. COPIAS DE RESPALDO	Proteger contra la pérdida de la información.		L4	

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.12.3.1. Respaldo de la información	Se DEBEN hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Sí	L4	Se evidencia que para este control se cuenta con varios documentos que apoyan el quehacer del mismo. Esta actividad en particular es muy robusta en la Empresa. Manual MG-TI-16 Copias seguridad Procedimiento PR-TI-11 Generación de copias de seguridad Procedimiento PR-TI-12 Restauración de copias de seguridad Formato FO-TI-185 Solicitud de restauración de backup Formato FO-TI-218 Solicitud realización de backup
A.12.4. REGISTRO Y SEGUIMIENTO	Registrar eventos y generar evidencia.		L4	
A.12.4.1. Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Sí	L3	Se han definido aspectos básicos para tener en cuenta en la tarea de revisar los registros de eventos, de los elementos de tecnología, mediante el instructivo IN-TI-38 Revisión de registros automáticos de la plataforma de TI.
A.12.4.2. Protección de la información del registro	Las instalaciones y la información de registro se deben proteger contra la alteración y acceso no autorizado.	Sí	L3	Los registros de los sistemas operativos y de los sistemas de información son protegidos de modificación, de acuerdo con lo mencionado por el instructivo IN-TI-38 Revisión de registros automáticos de la plataforma de TI.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.12.4.3. Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, los registros se deben proteger y revisar con seguridad.	Sí	L2	Aunque hay un instructivo de Revisión de registros automáticos de la plataforma de TI (IN-TI-38), no hay evidencia de que se hayan revisado recientemente las acciones de los administradores.
A.12.4.4. Sincronización de relojes	Los relojes de TODOS los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	Sí	L4	Con base en el instructivo IN-TI-28 Configuración de la hora legal colombiana en la plataforma de TI, se sincronizaron todos los servidores contra el servicio NTP del Gobierno colombiano.
A.12.5. CONTROL DE SOFTWARE OPERACIONAL	Asegurar la integridad de los sistemas operacionales.		L4	
A.12.5.1. Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Sí	L4	Con base en el instructivo IN-TI-14 Preparación de un equipo de cómputo para usuario final, el personal de mesa de servicios realiza la instalación inicial del software en una máquina de usuario final. Cuando se requiere la instalación de un software adicional, se hace a través de la herramienta de autogestión de soporte y se valida la existencia de licenciamiento disponible antes de autorizar la instalación.
A.12.6. GESTION DE LA VULNERABILIDAD TECNICA	Prevenir el aprovechamiento de las vulnerabilidades técnicas.		L4	
A.12.6.1. Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a esas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Sí	L4	Se evidenció que durante la vigencia anterior se realizó un análisis de vulnerabilidades y hacking ético

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.12.6.2. Restricciones sobre la instalación de software	Se DEBE establecer e implementar las reglas para la instalación de software por parte de los usuarios.	Sí	L3	Existen restricciones para que los usuarios no puedan instalar software, Procedimiento Revisión a la plataforma de tecnología de información (PR-TI-18)
A.12.7. CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS DE INFORMACION	Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.		L4	
A.12.7.1. Controles de auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos de negocio.	Sí	L4	La Oficina de Control Interno publica anualmente el programa de auditoría, en el cual se incluye el SGSI de la Empresa.
A.13. SEGURIDAD DE LAS COMUNICACIONES			L4	
A.13.1. GESTION DE LA SEGURIDAD DE LAS REDES	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.		L4	

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.13.1.1. Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Sí	L3	Con el Documento de gestión de las telecomunicaciones se centralizan las actividades que se realizan para administrar la conectividad de los usuarios a la red de datos. Hace falta divulgarlo más, pues es muy nuevo. También se tiene el procedimiento PR-TI-23 Gestión de telecomunicaciones, y el documento DU-TI-06 Políticas Operacionales de Seguridad de la Información. Operacionalmente, se cuenta con unos equipos de seguridad de la red que permiten una gestión y monitorización apropiados.
A.13.1.2. Seguridad en los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten extremamente.	Sí	L3	Se tienen acuerdos con los proveedores de los canales de comunicación sobre la calidad y auditoría a los servicios de red. Por parte de la empresa se tienen equipos de seguridad de red, tales como un firewall Fortinet en alta disponibilidad, con los módulos fortigate, fortianalyzer y fortisandbox.
A.13.1.3. Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	Sí	L5	Se tienen subredes con distintos niveles de seguridad y acceso a los servicios de TI, según las necesidades identificadas de cada dependencia. Para el caso de la red de Tesorería, donde se maneja la banca electrónica, las restricciones son mayores. Se tiene por ejemplo una subred exclusiva para las impresoras y otra para los equipos del CPD. El enrutamiento entre las redes se hace a nivel de capa 3 de acuerdo con el modelo OSI.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.13.2. TRANSFERENCIA DE INFORMACION	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		L4	
A.13.2.1. Políticas y procedimientos de transferencia de información	Se debe contar con POLITICAS, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	Sí	L4	Se tienen los siguientes documentos: Resolución 34217 de 2015, de políticas obligatorias o de alto nivel. DU-TI-06 Políticas Operacionales de Seguridad de la Información. Procedimiento PR-TI-23 Gestión de telecomunicaciones. Instructivo IN-TI-05 Uso adecuado de los dispositivos de almacenamiento de información. Instructivo IN-TI-20 intercambio de información
A.13.2.2. Acuerdos sobre transferencia de información	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	Sí	L3	Se tienen adoptados los siguientes documentos: Instructivo IN-TI-19 aplicación de cifrado Instructivo intercambio de información (INTI20) Formato FO-TI-04 acuerdo de confidencialidad con terceros. Sin embargo, no se tienen evidencias de su uso.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.13.2.3. Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	Sí	L4	Se cuenta con los siguientes documentos: Instructivo IN-TI-12 Uso del servicio de correo electrónico institucional. Instructivo IN-TI-11 uso del servicio de mensajería instantánea. Se adquirió un sistema DLP que está empezando a arrojar sus primeros resultados.
A.13.2.4. Acuerdos de confidencialidad o de no divulgación	Se debe identificar, revisar y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	Sí	L4	Se tiene el formato FO-TI-04 Acuerdo de confidencialidad con terceros. Adicional, se está incluyendo en todos los contratos, una cláusula de confidencialidad.
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			L3	
A.14.1. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	Asegurar que la seguridad de la información sea parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.		L4	
A.14.1.1. Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras de sistemas de información existentes.	Sí	L3	Aunque se tienen los siguientes documentos, no siempre se especifican los requerimientos de seguridad para el nuevo desarrollo: Procedimiento PR-TI-04 Gestión de desarrollo de tecnologías de información Formato FO-TI-06 Solicitud de requerimientos para aplicaciones. Formato FO-TI-12 Diseño de alto nivel. Formato FO-TI-13 Especificación de requerimientos. Formato FO-TI-14 Análisis de actividades

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de las aplicaciones que pasan por las redes públicas se debe proteger de actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizadas.	Sí	L4	Las aplicaciones que se tienen expuestas en redes públicas están protegidas mediante certificados digitales SSL. Cuando se requiere utilizar desde una red pública, una aplicación que no soporta las protecciones antes mencionadas, se exige que se realice una conexión segura de tipo VPN, para proteger la información.
A.14.1.3. Protección de transacciones de los servicios de las aplicaciones	La información involucrada en los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	Sí	L4	Se han implantado mecanismos de protección de transacciones. Técnicas como el cifrado de los datos, protocolos para la transmisión segura (HTTPS), certificados de seguridad, los cuales están descritos en los instructivos IN-TI-19 aplicación de cifrado, IN-TI-20 intercambio de información e IN-TI-08 protección de la información digital.
A.14.2. Seguridad en los procesos de desarrollo y de soporte	Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.		L3	
A.14.2.1. Política de desarrollo seguro	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	Sí	L4	Se encuentra adoptada la política correspondiente, mediante la resolución 34217 de 2015. Procedimiento PR-TI-04 Gestión de desarrollo de tecnologías de información

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.14.2.2. Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	Sí	L4	Como se mencionó en el numeral A.12.1.2, Con base en el procedimiento PR-TI-08 Gestión de cambios que se aplican únicamente a temas tecnológicos, se realiza una mesa de trabajo semanal para presentar y discutir los cambios del siguiente periodo. También se tienen los siguientes documentos que fortalecen el control: Procedimiento Gestión de desarrollo de tecnologías de información (PR-TI-04) Procedimiento Gestión de sistemas de información (PR-TI-15)
A.14.2.3. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas de negocio, y someter a pruebas para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	Sí	L4	Como se mencionó en el numeral A.12.1.2, Con base en el procedimiento PR-TI-08 Gestión de cambios que se aplican únicamente a temas tecnológicos, se realiza una mesa de trabajo semanal para presentar y discutir los cambios del siguiente periodo. Para cambios de gran magnitud, se realizan planes de trabajo detallados, se informa a todas las partes interesadas y se realizan las pruebas correspondientes antes de activar la entrada en producción formalmente.
A.14.2.4. Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	Sí	L4	Los cambios son controlados desde la mesa de trabajo semanal ya mencionada. Los cambios sobre el software, solamente los pueden realizar las personas autorizadas y pasan a producción después de ser aprobados.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.14.2.5. Principios de construcción de los sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	Sí	L2	Se tienen procedimientos que adoptan una metodología de desarrollo, sin embargo, no se evidencia la aplicación de dicha metodología en todos los proyectos de desarrollo de software
A.14.2.6. Ambiente seguro de desarrollo	Las organizaciones se deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de software.	Sí	L3	Los ambientes de desarrollo están segregados y protegidos y solo tienen acceso los desarrolladores, según lo indica el instructivo IN-TI-37 Definición y uso de los ambientes de trabajo para desarrollo de software.
A.14.2.7. Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	Sí	L4	Existen procedimientos relacionados con la supervisión contractual, que están basados en lo indicado por las normas de orden nacional que rigen la contratación estatal.
A.14.2.8. Pruebas de seguridad de sistemas	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad.	Sí	L3	Se tiene publicado el Instructivo IN-TI-10 Realización de pruebas a los desarrollos de software, sin embargo, hace falta mayor apropiación del mismo.
A.14.2.9. Pruebas de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	Sí	L3	Se tiene publicado el Instructivo IN-TI-10 Realización de pruebas a los desarrollos de software, sin embargo, hace falta mayor apropiación del mismo.
A.14.3. DATOS DE PRUEBA	Asegurar la protección de los datos usados para pruebas.		L3	
A.14.3.1. Protección de datos de prueba	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	Sí	L3	Se tiene publicado el Instructivo IN-TI-10 Realización de pruebas a los desarrollos de software, sin embargo, hace falta mayor apropiación del mismo.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.15. RELACIONES CON LOS PROVEEDORES			L4	
A.15.1. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.		L3	
A.15.1.1. Política de seguridad de la información para las relaciones con los proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.	Sí	L4	Se encuentra adoptada la política correspondiente, mediante la resolución 34217 de 2015.
A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con los proveedores	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación NO Autorizada o No Intencional, o el uso indebido de los activos de la organización.	Sí	L3	Se está incluyendo en todos los contratos, una cláusula de confidencialidad. Se establecen y se acuerdan con los proveedores los requisitos relacionados a la seguridad de la información. El respeto de los mismos está especificado en todos los contratos con los proveedores. Sin embargo en los acuerdos no se especifica que los acuerdos se deban respetar por parte de los subcontratistas
A.15.1.3. Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	Sí	L3	De acuerdo con el procedimiento PR-TI-21 Gestión de compras de productos y/o servicios de tecnología de información, los proveedores críticos deben tener un SGSI implementado y en operación.
A.15.2. GESTIÓN DE LA PRESTACIÓN DE LOS SERVICIOS DE PROVEEDORES	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.		L4	
A.15.2.1. Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	Sí	L3	Se realizan seguimientos periódicos, previos a cada pago, relacionados con la calidad del servicio o producto.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.15.2.2.Gestión de cambios en los servicios de los proveedores	Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.	Sí	L4	Como se mencionó en el numeral A.12.1.2, Con base en el procedimiento PR-TI-08 Gestión de cambios que se aplican únicamente a temas tecnológicos, se realiza una mesa de trabajo semanal para presentar y discutir los cambios del siguiente periodo, incluyendo los cambios que se presenten en los servicios prestados por los proveedores.
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			L3	
A.16.1. GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.		L3	
A.16.1.1. Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Sí	L3	Aunque se tienen estos documentos, procedimiento PR-TI-22 Gestión de Incidentes de Seguridad de la Información y formato FO-TI-28 condiciones para validación de eventos de seguridad de la información, el personal de la Empresa aún no los tiene apropiados y el nivel de registro de eventos de seguridad es muy bajo.
A.16.1.2. Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	Sí	L3	De acuerdo con lo indicado en el procedimiento PR-TI-22 Gestión de Incidentes de Seguridad de la Información, los pocos eventos atendidos son informados mediante la intranet de la Empresa.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.16.1.3.Reporte de debilidades de seguridad de la información	Se debe EXIGIR a los TODOS los empleados y contratistas que usan servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	Sí	L3	En las jornadas de sensibilización, inducción y reinducción del personal de la Empresa, así como a través de campañas de divulgación, se ha abordado el tema de la necesidad de reportar oportunamente los posibles eventos de seguridad de la información. Sin embargo, como se mencionó el nivel de reporte es bajo.
A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	Sí	L3	Se tienen los siguientes documentos: procedimiento PR-TI-22 Gestión de Incidentes de Seguridad de la Información y formato FO-TI-28 condiciones para validación de eventos de seguridad de la información.
A.16.1.5. Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.	Sí	L3	De acuerdo con lo mencionado en el procedimiento PR-TI-22 Gestión de Incidentes de Seguridad de la Información, se han atendido los incidentes de seguridad reportados.
A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	Sí	L3	Las conclusiones de las investigaciones sobre los incidentes de seguridad son compartidas en el comité de seguridad y guardadas en una base de datos de conocimiento que posee el sistema de gestión de casos de soporte.
A.16.1.7. Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Sí	L2	En la Empresa de manejo de Obras esta labor la debe realizar un externo autorizado, como el cuerpo Técnico de Investigación de la Fiscalía.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO			L4	
A.17.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACION	La continuidad de seguridad de la información se DEBE incluir en los sistemas de gestión de la continuidad del negocio de la organización.		L3	
A.17.1.1. Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	Sí	L3	En el documento DU-TI-07 Plan de recuperación de desastres se abordan los temas requeridos por este control.
A.17.1.2. Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Sí	L3	Lo requerido por el control está incorporado en el documento DU-TI-07 Plan de recuperación de desastres. Se evidencias actas de reuniones y de pruebas de los instructivos de restauración de los aplicativos críticos.
A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	Sí	L3	En el documento DU-TI-07 Plan de recuperación de desastres se incluye un plan de pruebas, el cual se ha desplegado una vez.
A.17.2. REDUNDANCIAS	Asegurar la disponibilidad de las instalaciones de procedimiento de información.		L4	
A.17.2.1. Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de procesamiento de la información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Sí	L4	Se tiene un centro de procesamiento de datos alterno, para contingencias. En conjunto con el proveedor se han realizado 2 pruebas por año desde su implementación.

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.18. CUMPLIMIENTOS			L4	
A.18.1. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.		L3	
A.18.1.1. Identificación de la legislación aplicable y los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información de la organización.	Sí	L4	Se Actualiza dos (2) veces por año el Formato FO-GI-02 Actualización y evaluación del normograma institucional. Luego de la evaluación, se publica en la web de la Entidad.
A.18.1.2. Derechos de propiedad intelectual (DPI)	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	Sí	L4	Anualmente la Empresa debe presentar el informe de derechos de autor ante la Dirección Nacional de Derechos de Autor.
A.18.1.3. Protección de registros	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Sí	L2	Se terminó y aprobó recientemente el Instructivo de revisión de registros automáticos de la plataforma de TI. Se debe hacerle promoción, para fortalecerlo.
A.18.1.4. Privacidad y protección de información de datos personales	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	Sí	L3	Manual Operativo para la Protección de Datos Personales (MG-TI-17) Documento Condiciones de uso y políticas de privacidad de la página web (DU-TI-03)

DOMINIO	OBJETIVO/CONTROL	CUMPLE	NIVEL	OBSERVACIÓN
A.18.1.5. Reglamentación de controles criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	Sí	L3	Se tienen implementados los siguientes controles, aunque falta la divulgación y promoción: Instructivo IN-TI-08 protección de la información digital Instructivo aplicación de cifrado (INTI19)
A.18.2. REVISIONES DE SEGURIDAD DE LA INFORMACION	Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.		L4	
A.18.2.1. Revisión independiente de la seguridad de información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	Sí	L5	La oficina de Control Interno debe realizar un programa anual e auditoría, que incluye al SGSI. La auditoría más reciente fue el año anterior.
A.18.2.2. Cumplimiento con las políticas y normas de seguridad	Los Directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	Sí	L4	Se realizan campañas de divulgación sobre las responsabilidades con el SGSI. Esto da pie para que cada jefe de dependencia coordine la formulación de las acciones correctivas y la suscripción de los planes de mejoramiento producto de la auditoría.
A.18.2.3. Revisión del cumplimiento técnico	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	Sí	L3	Se han realizado pruebas de penetración controladas, acompañadas de análisis de vulnerabilidades e ingeniería social. Sobre los resultados, se elabora un plan de acción para la mitigación de las vulnerabilidades encontradas.

6.3. Presentación de Resultados

Luego de realizar la evaluación de la madurez de los controles, se puede determinar que solamente el **6%** de los controles están en un nivel de madurez **L2 Reproducible, pero intuitivo**. El **34%** están en nivel **L3 Definido**. Una mayor parte de ellos, el **45%** están en nivel **L4 Gestionado y medible.** Finalmente, el **15%** se encuentran en nivel **L5 Optimizado**. Para mayor facilidad, se presentan estos resultados en la tabla 33, a continuación.

Tabla 33. Nivel de madurez de los controles del SGSI, según el modelo CMM. Fuente propia

NIVEL DE MADUREZ DE LOS CONTROLES		
Nivel	Cantidad	Porcentaje
L0 Inexistente	0	0%
L1 Inicial / Ad-hoc	0	0%
L2 Reproducible, pero intuitivo	7	6%
L3 Definido	39	34%
L4 Gestionado y medible	51	45%
L5 Optimizado	17	15%
TOTAL	114	100%

Si la anterior tabla se grafica, el resultado es el siguiente:

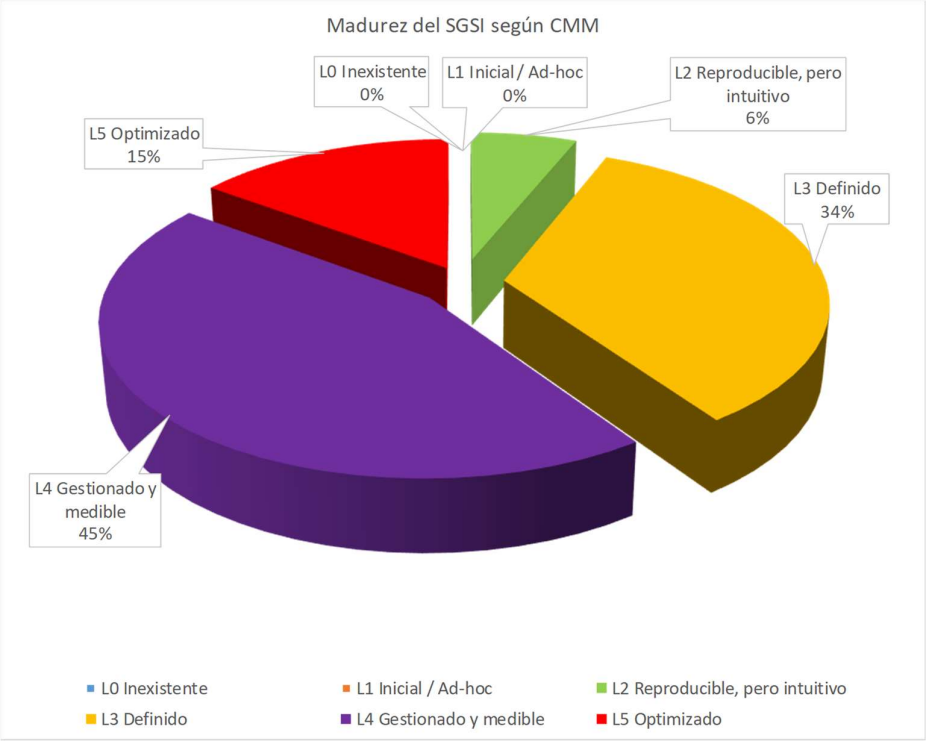


Ilustración 11. Nivel de madurez de los controles del SGSI, según el modelo CMM. Fuente propia

Ahora, si se compara el estado de los controles en su estado inicial, con el análisis diferencial, se puede apreciar el gran avance en la madurez de todos los controles, para ello se presenta la siguiente ilustración:

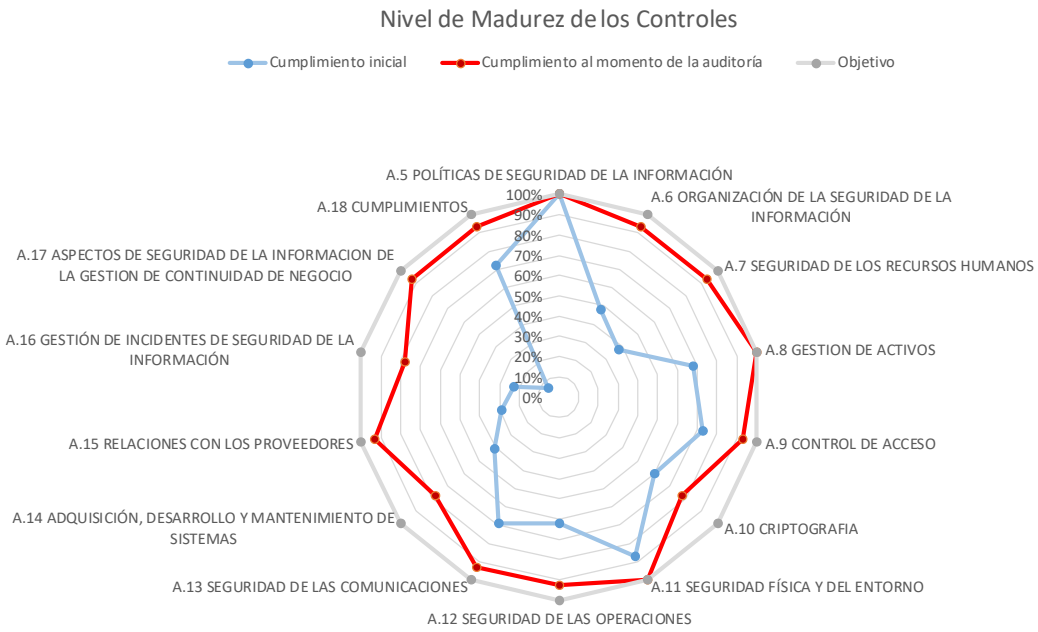


Ilustración 12. Comparativo del nivel de madurez de los controles. Fuente propia

6.4. Auditoría de Cumplimiento

En la formalidad de un sistema de gestión de seguridad de la información, los requisitos auditables están definidos en la norma NTC–ISO/IEC 27.001, versión 2013, para nuestro caso. Es así como se realizó un ejercicio de auditoría interno, previo al de certificación, para evaluar el estado de implementación del SGSI en la Empresa de Manejo de Obras. En el Anexo 9. Informe de auditoría, se puede encontrar el detalle de esta.

6.4.1. Plan de auditoría

Objetivo: Evaluar el grado de conformidad del Sistema frente a los requisitos del estándar ISO 27001:2013.

Alcance: Activos de información críticos para la financiación, diseño y ejecución de proyectos de infraestructura en la ciudad.

EXTRACTO DEL FORMATO PLAN DE AUDITORÍA							
Id	Actividad	Equipo Auditor		Horas	Auditado	Lugar	Fecha/Hora
		Responsable	Acompañante				
1	REUNIÓN DE APERTURA	Todos	Todos	30 min	Todos	Sala de juntas Gerencia	Mayo 3 de 2021 - 7:00 am
2	AUDITORIA DE PROCESO: PLANEACIÓN ESTRATÉGICA	Hernán Salazar	Víctor Sosa	2 horas	Líder de proceso	Sala juntas piso 10	Mayo 5 de 2021 - 7:00 am
3	AUDITORIA DE PROCESO: INNOVACIÓN Y GESTIÓN DE CONOCIMIENTO	Hernán Salazar	Hugo Arias	2 horas	Líder de proceso	Sala juntas piso 5	Mayo 6 de 2021 - 7:00 am
4	AUDITORIA DE PROCESO: GESTIÓN SOCIAL Y PARTICIPACIÓN CIUDADANA	Roberto Carlos Suarez	Víctor Sosa	2 horas	Líder de proceso	Sala juntas piso 1	Mayo 7 de 2021 - 7:00 am
5	AUDITORIA DE PROCESO: GESTIÓN INTERINSTITUCIONAL	María Fernanda Cuellar	Hugo Arias	2 horas	Líder de proceso	Sala juntas piso 6	Mayo 11 de 2021 - 7:00 am
6	AUDITORIA DE PROCESO: COMUNICACIONES	Hernán Salazar	Víctor Sosa	2 horas	Líder de proceso	Sala juntas piso 10	Mayo 12 de 2021 - 7:00 am
7	AUDITORIA DE PROCESO: FACTIBILIDAD DE PROYECTOS	Roberto Carlos Suarez	Hugo Arias	2 horas	Líder de proceso	Sala juntas piso 3	Mayo 4 de 2021 - 7:00 am

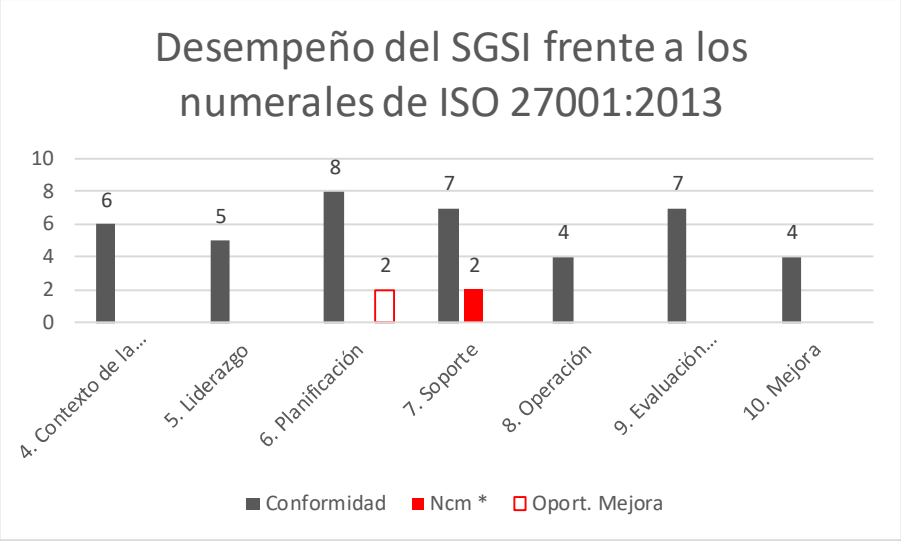
EXTRACTO DEL FORMATO PLAN DE AUDITORÍA							
Id	Actividad	Equipo Auditor		Horas	Auditado	Lugar	Fecha/Hora
		Responsable	Acompañante				
8	AUDITORIA DE PROCESO: GESTIÓN DE LA FINANCIACIÓN Y VALORIZACIÓN	María Fernanda Cuellar	Víctor Sosa	2 horas	Líder de proceso	Sala juntas piso 4	Mayo 12 de 2021 - 9:00 am
9	AUDITORIA DE PROCESO: DISEÑO DE PROYECTOS	Roberto Carlos Suarez	Hugo Arias	2 horas	Líder de proceso	Sala juntas piso 3	Mayo 4 de 2021 - 9:00 am
10	AUDITORIA DE PROCESO: GESTIÓN PREDIAL	Roberto Carlos Suarez	Hugo Arias	2 horas	Líder de proceso	Sala juntas piso 7	Mayo 4 de 2021 - 1:00 pm
11	AUDITORIA DE PROCESO: EJECUCIÓN DE OBRAS	María Fernanda Cuellar	Víctor Sosa	2 horas	Líder de proceso	Sala juntas piso 8	Mayo 13 de 2021 - 9:00 am
12	AUDITORIA DE PROCESO: CONSERVACIÓN DE INFRAESTRUCTURA	María Fernanda Cuellar	Hugo Arias	2 horas	Líder de proceso	Sala juntas piso 6	Mayo 4 de 2021 - 3:00
13	AUDITORIA DE PROCESO: GESTIÓN CONTRACTUAL	María Fernanda Cuellar	Víctor Sosa	2 horas	Líder de proceso	Sala juntas piso 9	Mayo 5 de 2021 - 9:00 am
14	AUDITORIA DE PROCESO: GESTIÓN LEGAL	Roberto Carlos Suarez	Hugo Arias	2 horas	Líder de proceso	Sala juntas piso 9	Mayo 5 de 2021 - 11:00 am
15	AUDITORIA DE PROCESO: GESTIÓN AMBIENTAL, CALIDAD Y SST	Roberto Carlos Suarez	Víctor Sosa	3 horas	Líder de proceso	Sala juntas piso 10	Mayo 3 de 2021 - 9:30 am

EXTRACTO DEL FORMATO PLAN DE AUDITORÍA							
Id	Actividad	Equipo Auditor		Horas	Auditado	Lugar	Fecha/Hora
		Responsable	Acompañante				
16	AUDITORIA DE PROCESO: GESTIÓN FINANCIERA	Roberto Carlos Suarez	Hugo Arias	2 horas	Líder de proceso	Sala juntas piso 4	Mayo 5 de 2021 - 2:00 pm
17	AUDITORIA DE PROCESO: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	Roberto Carlos Suarez	Víctor Sosa	5 horas	Líder de proceso	Oficina de Tecnología	Mayo 3 de 2021 - 1 pm a 5 pm
18	AUDITORIA DE PROCESO: GESTIÓN DE RECURSOS FÍSICOS	Hernán Salazar	Hugo Arias	2 horas	Líder de proceso	Sala juntas piso 4	Mayo 6 de 2021 - 9:00 am
19	AUDITORIA DE PROCESO: GESTIÓN DEL TALENTO HUMANO	Roberto Carlos Suarez	Víctor Sosa	2 horas	Líder de proceso	Sala juntas piso 2	Mayo 6 de 2021 - 11:00 am
20	AUDITORIA DE PROCESO: GESTIÓN DOCUMENTAL	Hernán Salazar	Hugo Arias	2 horas	Líder de proceso	Sala juntas piso 1	Mayo 6 de 2021 - 2:00 pm
21	AUDITORIA DE PROCESO: GESTIÓN INTEGRAL DE PROYECTOS	Roberto Carlos Suarez	Víctor Sosa	2 horas	Líder de proceso	Sala juntas piso 10	Mayo 7 de 2021 - 9:00 am
22	AUDITORIA DE PROCESO: EVALUACIÓN Y CONTROL	Hernán Salazar	Hugo Arias	2 horas	Líder de proceso	Sala juntas piso 8	Mayo 7 de 2021 - 1:00 pm
23	Reunión de cierre y entrega de informe final de Auditoría	Todos	Todos	1 hora	Líder de proceso	Sala de juntas Gerencia	Mayo 7 de 2021 - 3:00 pm

6.5. Resultados

El resultado de la auditoría es muy satisfactorio para la Empresa de Manejo de Obras y refleja el tiempo que se lleva en la implementación del Sistema de Gestión de Seguridad de la Información.

En cuanto a los requerimientos de gestión, se encontraron 2 no conformidades menores, relacionadas con el manejo de documentos obsoletos y con la divulgación hacia las partes interesadas externas; ambas relacionadas con el numeral 7 Soporte; y 2 oportunidades de mejora, relacionadas con el numeral 6 planificación. En la siguiente gráfica se puede observar el desempeño del SGSI frente a la norma ISO 27001:2013.



* Ncm: Se refiere a No conformidad menor

Como se pudo observar en los apartados previos, el nivel de madurez de los controles es excelente, salvo siete (7) casos particulares que se encuentran en nivel L2 Reproducible, pero intuitivo.

A lo largo del análisis de auditoría se pudo determinar que en la Empresa de Manejo de Obras se tienen todos los controles recomendados por el anexo A de la norma técnica, sin embargo la debilidad se presenta en la aplicación de los mismos, básicamente por falta de apropiación.

En este sentido, la recomendación que se eleva a las directivas de la Empresa es que se fortalezca el proceso de divulgación y apropiación del SGSI, incluyendo sus controles.

Asimismo, se puede concluir que el SGSI de la Empresa de Manejo de Obras está preparado para la certificación.

6.6. Fichas de no conformidades

A continuación, se presentan las dos fichas correspondientes a las no conformidades encontradas durante el proceso de auditoría:

Formato Solicitud de acción correctiva o preventiva	

Fecha: Día [1][5] Mes [5][ ] Año [2][0][2][1]

Tipo de proceso generador de la No conformidad: _____

Proceso generador de la No conformidad: _____

Hallazgo

Durante la auditoría del SGSI en el área de tecnología se solicitó el formato de creación de usuarios FO-TH-02, la versión entregada por el auditado corresponde a la 02, sin embargo, al auditar el proceso se verificó que en el portal de intranet la versión vigente es la 03, evidenciando una falla de controles sobre el manejo de versiones de los formatos, incumpliendo el requisito 7.5.3 Control de la información documentada, literal e), en el cual se establece la necesidad de tener controles sobre el control de cambios.

Acción Preventiva [ ] **Acción Correctiva** [X] **Correcci**

Áreas Involucradas

Oficina Asesora de Planeación- Oficina Asesora de Tecnologías de Información

Responsable por ejecutar la acción preventiva, correctiva o corrección.

Nombres y Apellidos Carlos Fernando Campos- Erika Aristizabal

Personal que debe ser enterado de la disposición:

Nombres y Apellidos, cargo

Mauro Quiñonez Jefe Oficina Asesora de Tecnologías de Información	

_____

Firma del responsable de ejecutar la acción preventiva, correctiva o corrección.

Formato

Solicitud de acción correctiva o preventiva

Fecha: Día 15 Mes 5 Año 2021

Tipo de proceso generador de la No conformidad: _____

Proceso generador de la No conformidad: _____

Hallazgo

Al solicitar los mecanismos de comunicación sobre el SGSI al exterior, el profesional Pablo Rosas expreso que el plan existente es de indolé interno, razón por la cual no incluye a los grupos de interés externo, al preguntarle al oficial de seguridad, manifesto que las comunicaciones son administradas por Rosas, situación que genera un inclumplimiento al numeral 7.4 Comunicaciones de la norma ISO 270001, donde se establece que la organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al SGSI

Acción Preventiva [ ] **Acción Correctiva** [X] **Corrección** [X]

Áreas Involucradas

Oficina de Comunicaciones - Oficina Asesora de Tecnologías de Información

Responsable por ejecutar la acción preventiva, correctiva o corrección.

Nombres y Apellidos Pablo Rosas - Erika Aristizabal

Personal que debe ser enterado de la disposición:

Nombres y Apellidos, cargo

Mauro Quiñonez	

_____

Firma del responsable de ejecutar la acción preventiva, correctiva o corrección.

7. CONCLUSIONES

1. La importancia de realizar un diagnóstico al iniciar el proceso de implementación, radica en que se convierte en un punto de partida, para la elaboración de una hoja de ruta que facilite el cumplimiento de los objetivos.
2. Del mismo análisis diferencial inicial, se puede concluir que hay controles como el A.5. Políticas de seguridad y el A.11. Seguridad física y del entorno que tienen un nivel alto de implementación; mientras que el A.16. Gestión de incidentes de seguridad de la información y el A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio tienen los niveles más bajos en la implementación con un 23% y un 7% respectivamente, por lo cual en estos últimos se deberá trabajar con mayor énfasis para mejorar su desempeño.
3. Un sistema de Gestión está definido por los documentos que lo enmarcan y los describen, de ahí la importancia de definir de forma clara y concisa los documentos del SGSI.
4. Una de las etapas más importantes, sino la más, es la gestión de los riesgos. Gracias a ella se puede dar mayor claridad a la definición de los proyectos que se van a implementar en torno al SGSI.
5. Un análisis de riesgos permitirá conocer las amenazas e impacto de ellas sobre los activos institucionales, para de esta forma tomar las medidas de protección o inclusive, medidas de acción (planes) para protegerlos (a los activos).
6. Es bien conocida una frase que dice: "que una cadena es tan fuerte como su eslabón más débil". Si la extrapolamos al ámbito del SGSI de la Empresa de Manejo de Obras, podemos decir que ese eslabón son los empleados apáticos, que no se apropian de los conceptos, las políticas y recomendaciones, es por ello que los proyectos de divulgación, socialización, apropiación o en términos generales, de formación, deben ser permanentes.
7. Es muy importante saber definir las acciones de tratamiento de los riesgos, o como en nuestro caso, los proyectos que van a permitir mitigar el riesgo identificado; pues una mala decisión puede hacer que se pierda la inversión, pero sobre todo, la confianza de la alta dirección en el SGSI.
8. El SGSI está basado en el modelo PHVA de mejoramiento continuo, y por ello la importancia de los ciclos permanentes y periódicos de auditoría, pues permiten que por cada nuevo ciclo o iteración, el sistema vaya mejorando. Una muestra de ello es el nivel de madurez mostrado por el sistema en la última auditoría Interna.
9. El apoyo de la alta dirección, además de ser un requerimiento normativo, en la práctica se convierte en un punto altamente crítico para el éxito del SGSI en la Empresa.

8. BIBLIOGRAFÍA Y REFERENCIAS

- Introducción a la seguridad de la información, Silvia Garre Gui. UOC
- https://www.timetoast.com/timelines/evolucion-de-la-norma-iso-iec-27000.
- Norma Técnica Colombiana NTC-ISO/IEC 27001:2013. Icontec. 2013.
- Guía Técnica Colombiana GTC-ISO/IEC 27002:2015. Icontec. 2015.
- DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA – BANCO MUNDIAL Propuesta metodológica: Identificación de riesgos de corrupción, Bogotá D.C., 1999.
- DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Guía para la administración del riesgo. Bogotá, D.C., septiembre de 2011. Cuarta Edición
- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la Información (SGSI). Requisitos. NTC-ISO 27001. Bogotá D.C., 2006. (esta norma es una adopción idéntica por traducción de la norma ISO/IEC 27001).
- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del Riesgo, Principios y Directrices. NTC-ISO 31000. Bogotá D.C., 2011. (esta norma es una adopción idéntica por traducción de la norma ISO 31000:2009).
- COLOMBIA COMPRA EFICIENTE. Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación. Bogotá D.C., 2013.
- ISO 27001: Revisión por la dirección y mejora del SGSI: http://www.pmg-ssi.com/2014/12/iso-27001-revision-por-la-direccion-y-mejora-del-sgsi/

- DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA – BANCO MUNDIAL Propuesta metodológica: Identificación de riesgos de corrupción, Bogotá D.C., 1999.
- DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Guía para la administración del riesgo. Bogotá, D.C., septiembre de 2011. Cuarta Edición
- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la Información (SGSI). Requisitos. NTC-ISO 27001. Bogotá D.C., 2006. (esta norma es una adopción idéntica por traducción de la norma ISO/IEC 27001).
- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del Riesgo, Principios y Directrices. NTC-ISO 31000. Bogotá D.C., 2011. (esta norma es una adopción idéntica por traducción de la norma ISO 31000:2009).
- COLOMBIA COMPRA EFICIENTE. Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación. Bogotá D.C., 2013.