MÁSTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TIC

Trabajo final de Máster

Actualización del Sistema de Gestión de Seguridad de la Información de una empresa a la norma ISO/IEC 27001:2013

Fase 5 Auditoria de cumplimiento contra ISO 27002:2013

Alexandra Ramírez Castro

UOC
Mayo 2014

Contenido

1. Descripcióndel proyecto

Considerando la reciente actualización de la norma ISO/IEC 27001 de su versión 2005 a su versión 2013, y la presencia de diferencias relevantes entre las dos versiones, así como los requerimientos de actualización a la nueva versión que tendrán que afrontar las organizaciones certificadas en la antigua versión contando como plazo máximo para esto hasta Septiembre de 2015; el presente proyecto aborda realizar la transición del sistema de gestión de seguridad de la información de una empresa dedicada al transporte de energía basado en ISO/IEC 27001:2005 (No certificado) al nuevo estándar ISO/IEC 27001:2013.

Para abordar el proyecto se realizaran las siguientes fases:

Fase 1
Situación actual: Contextualización, objetivos y análisis diferencial

La fase considera:

- Introducción al Proyecto
- Enfoque y selección de la empresa que será objeto de estudio
- Definición de los objetivos del Plan Director de Seguridad y Análisis diferencial de la empresa con respecto a la ISO/IEC 27001+ISO/IEC 27002 en su versión 2013

Los entregables de esta fase serán:

- Presentación de la empresa en estudio (objetivos, misión, visión, normatividad que la rige, procesos, esquema de red a alto nivel, estructura organizacional de la empresa)
- Alcance del SGSI ajustado para cumplir requisitos de ISO 27001:2013
- Objetivos del SGSI ajustados para cumplir requisitos de ISO 27001:2013
- Diagnóstico de seguridad frente a ISO 27001:2013 e ISO 27002:2013

Fase 2
Sistema de Gestión Documental

La fase considera:

- Alineación de la Política de Seguridad de la información frente a los requerimientos de la nueva norma

- Declaración de aplicabilidad: aseguramiento frente a la nueva norma
- Documentación del SGSI: ajuste que sean requeridos para la alineación y documentación adicional que sea requerida

Los entregables de esta fase serán:

- Política de seguridad de la información
- Roles y responsabilidades en seguridad de la información
- Proceso de revisión por la dirección
- Proceso de gestión de indicadores
- Metodología de análisis de riesgos
- Declaración de aplicabilidad
- Procedimiento de auditorías internas

Fase 3
Análisis de riesgos

La fase considera:

- Elaboración de una metodología de análisis de riesgos: Identificación y valoración de activos, amenazas, vulnerabilidades, cálculo del riesgo, nivel de riesgo aceptable y riesgo residual.

Los entregables de esta fase serán:

- Riesgos de seguridad de la información identificados a partir del análisis de vulnerabilidades y amenazas sobre los activos de información considerados críticos por la empresa.

  Nota: este entregable mostrará un bosquejo general, dado que la empresa no autorizo entregar detalles sobre el análisis de riesgos y sus resultados.

Fase 4
Propuesta de Proyectos

La fase considera:

- Evaluación de proyectos que debe llevar a cabo la Empresa para alinearse con los objetivos planteados en el Plan Director.
- Propuesta plan de tratamiento de riesgos, proyectos de cara a conseguir una adecuada gestión de la seguridad de la información.
- Cuantificación económica y temporal de los mismos.

Los entregables de esta fase serán:

- Propuestas de planes de tratamiento ante los riesgos evidenciados

Fase 5
Auditoría de Cumplimiento de la ISO/IEC 27002:2013

La fase considera:

- Evaluación de controles, madurez y nivel de cumplimiento.

Los entregables de esta fase serán:

- Informe de auditoría frente a la norma ISO 27002:2013. Este será un ajuste o segunda evaluación con respecto al realizado al inicio del proyecto en la fase de diagnóstico para ver las mejoras obtenidas en el desarrollo del proyecto.

Fase 6
Presentación de Resultados y entrega de Informes

La fase considera:

- Consolidación de los resultados obtenidos durante el proceso de análisis.
- Realización de los informes y presentación ejecutiva a la Dirección.
- Entrega del proyecto final.

Los entregables de esta fase serán:

- Informe consolidado del proyecto
- Anexos realizados durante el proyecto

2. Normas ISO 27001 e ISO 27002 del 2005 y 2007 y su actualizaciones de 2013

En el presente numeral se presentan las normas ISO 27001:2005 e ISO 27002:2007 y se realizará un breve descripción sobre los cambios que se presentaron entre estás versiones y su reciente actualización del año 2013.

La norma ISO 27001, define como organizar la seguridad de la información en cualquier tipo de organización. Está determina como gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información (SGSI). ISO 27001 especifica los requisitos necesarios para establecer, implantar, mantener y

mejorar el SGSI, esta es la norma certificable por las empresas. En la versión 2005, esto se implementaba a partir del ciclo PHVA (Planificar, Hacer, Verificar, Actuar). Para la versión 2013, no se establece este modelo como curso necesario de implementación; se da a las organizaciones la libertad de definir el modelo de mejora continua que quieran utilizar para el SGSI. La norma paso a tener 130 requisitos, la versión 2005 tenía 102.

Por su parte ISO 27002, corresponde a la guía de buenas prácticas en seguridad de la información y guarda correspondencia con los controles definidos en el Anexo A de la ISO 27001.

Uno de los cambios de ISO 27001 fue que ahora aplica, la estructura de alto nivel definidos en el Anexo SL de las directivas ISO/IEC, esto con el fin de guardar correspondencia entre las normas ISO que se han ajustado a este anexo en pro de ayudar en la implementación de sistemas integrados; esto implica que se manejan los mismos apartados y términos comunes. Los numerales o capítulos en los cuales se divide la norma son los siguientes:

0. Introducción
1. Alcance
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planeación
7. Soporte
8. Operación
9. Evaluación del desempeño
10. Mejora

A partir del numeral 4 al 10 se definen de forma específica los aspectos de cada norma, en este caso de ISO 27001 es lo siguiente:

4. Contexto de la organización: entendimiento de la organización y su contexto, expectativas de las partes interesadas, alcance del SGSI.

5. Liderazgo: Liderazgo y compromiso de la alta dirección, políticas, organización de roles, responsabilidades y autoridades.

6. Planeación: Como abordar riesgos y oportunidades

7. Soporte: Recursos, competencias, conciencia, comunicación e información documentada.

8. Operación: Evaluación de riesgos de seguridad de la información, manejo de riesgos de seguridad de la información.

9. Evaluación del desempeño: Evaluación de riesgos de seguridad de la información.

10. Mejora: Monitoreo y auditorías internas, revisión de la alta dirección.

Conrespecto al anexo A se tienen las siguientes diferencias:

	Versión 2005	Versión 2013
Dominios del anexo A	11	14
Objetivos de control	39	35
Controles	133	114

Tabla 1. Cambios Anexo A ISO 27001

La siguiente tabla presenta los controles actuales y su correspondencia con los antiguos:

Control 27001:2013	Controles	Existencia en norma anterior	Control 27001:2005
A.5	Políticas de seguridad de la información		
A.5.1	Orientación de la dirección para la gestión de la seguridad de la información		
A.5.1.1	Políticas para la seguridad de la información	SI	A.5.1.1
A.5.1.2	Revisión de las políticas para la seguridad de la información	SI	A.5.1.2
A.6	Organización de la seguridad de la información		
A.6.1	Organización interna		
A.6.1.1	Roles y responsabilidades para la seguridad de la información	SI	A.6.1.3 A.8.1.1
A.6.1.2	Separación de deberes	SI	A.10.1.3
A.6.1.3	Contacto con las autoridades	SI	A.6.1.6
A.6.1.4	Contactos con grupos de interés especial	SI	A.6.1.7
A.6.1.5	Seguridad de la información en la gestión de proyectos	NO	
A.6.2	Dispositivos móviles y teletrabajo		
A.6.2.1	Política para dispositivos móviles	SI	A.11.7.1
A.6.2.2	Teletrabajo	SI	A.11.7.2
A.7	Seguridad de los recursos humanos		
A.7.1	Antes de asumir el empleo		
A.7.1.1	Selección	SI	A.8.1.2
A.7.1.2	Términos y condiciones del empleo	SI	A.8.1.3
A.7.2	Durante la ejecución del empleo		
A.7.2.1	Responsabilidades de la dirección	SI	A.8.2.1
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	SI	A.8.2.2
A.7.2.3	Proceso disciplinario	SI	A.8.2.3
A.7.3	Terminación y cambio de empleo		
A.7.3.1	Terminación o cambio de responsabilidades de empleo	SI	A.8.3.1
A.8	Gestión de activos		
A.8.1	Responsabilidad por los activos		

Control 27001:2013	Controles	Existencia en norma anterior	Control 27001:2005
A.8.1.1	Inventario de activos	SI	A.7.1.1
A.8.1.2	Propiedad de los activos	SI	A.7.1.2
A.8.1.3	Uso aceptable de los activos	SI	A.7.1.3
A.8.1.4	Devolución de activos	SI	A.8.3.2
A.8.2	Clasificación de la información		
A.8.2.1	Clasificación de la información	SI	A.7.2.1
A.8.2.2	Etiquetado de la información	SI	A.7.2.2
A.8.2.3	Manejo de activos	SI	A.7.2.2 A.10.7.3
A.8.3	Manejo de medios		
A.8.3.1	Gestión de medios removibles	SI	A.10.7.1
A.8.3.2	Disposición de los medios	SI	A.10.7.2
A.8.3.3	Transferencia de medios físicos	SI	A.10.8.3
A.9	Control de acceso		
A.9.1	Requisitos del negocio para control de acceso		
A.9.1.1	Política de control de acceso	SI	A.11.1.1
A.9.1.2	Acceso a redes y a servicios en red	SI	A.11.4.1
A.9.2	Gestión de acceso de usuarios		
A.9.2.1	Registro y cancelación del registro de usuarios	SI	A.11.2.1 A.8.3.3
A.9.2.2	Suministro de acceso de usuarios	SI	A.11.2.2
A.9.2.3	Gestión de derechos de acceso privilegiado	SI	A.11.2.2
A.9.2.4	Gestión de información de autenticación secreta de usuarios	SI	A.11.2.3
A.9.2.5	Revisión de los derechos de acceso de los usuarios	SI	A.11.2.4
A.9.2.6	Retiro o ajuste de los derechos de acceso	SI	A.8.3.3
A.9.3	Responsabilidades de los usuarios		
A.9.3.1	Uso de información de autenticación secreta	SI	A.11.3.1
A.9.4	Control de acceso a sistemas y aplicaciones		
A.9.4.1	Restricción de acceso a la información	SI	A.11.6.1
A.9.4.2	Procedimiento de ingreso seguro	SI	A. 11.5.1 A. 11.5.5 A. 11.5.6
A.9.4.3	Sistema de gestión de contraseñas	SI	A.11.5.3
A.9.4.4	Uso de programas utilitarios privilegiados	SI	A.11.5.4
A.9.4.5	Control de acceso a códigos fuente de programas	SI	A.12.4.3
A.10	Criptografía		
A.10.1	Controles criptográficos		
A.10.1.1	Política sobre el uso de controles criptográficos	SI	A.12.3.1
A.10.1.2	Gestión de llaves	SI	A.12.3.2
A.11	Seguridad física y del entorno		

Control 27001:2013	Controles	Existencia en norma anterior	Control 27001:2005
A.11.1	Áreas seguras		
A.11.1.1	Perímetro de seguridad física	SI	A.9.1.1
A.11.1.2	Controles de acceso físico	SI	A.9.1.2
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	SI	A.9.1.3
A.11.1.4	Protección contra amenazas externas y ambientales	SI	A.9.1.4
A.11.1.5	Trabajo en áreas seguras	SI	A.9.1.5
A.11.1.6	Áreas de despacho y carga	SI	A.9.1.6
A.11.2	Equipos		
A.11.2.1	Ubicación y protección de los equipos	SI	A.9.2.1
A.11.2.2	Servicios de suministro	SI	A.9.2.2
A.11.2.3	Seguridad del cableado	SI	A.9.2.3
A.11.2.4	Mantenimiento de equipos	SI	A.9.2.4
A.11.2.5	Retiro de activos	SI	A.9.2.7
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	SI	A.9.2.5
A.11.2.7	Disposición segura o reutilización de equipos	SI	A.9.2.6
A.11.2.8	Equipos de usuarios desatendidos	SI	A.11.3.2
A.11.2.9	Política de escritorio limpio y pantalla limpia	SI	A.11.3.3
A.12	Seguridad de las operaciones		
A.12.1	Procedimientos operacionales y responsabilidades		
A.12.1.1	Procedimientos de operación documentados	SI	A.10.1.1
A.12.1.2	Gestión de cambios	SI	A.10.1.2
A.12.1.3	Gestión de capacidad	SI	A.10.3.1
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	SI	A.10.1.4
A.12.2	Protección contra códigos maliciosos		
A.12.2.1	Controles contra códigos maliciosos	SI	A.10.4.1
A.12.3	Copias de respaldo		
A.12.3.1	Respaldo de la información	SI	A.10.5.1
A.12.4	Registro y seguimiento		
A.12.4.1	Registro de eventos	SI	A.10.10.1
A.12.4.2	Protección de la información de registro	SI	A.10.10.3
A.12.4.3	Registros del administrador y del operador	SI	A.10.10.3 A.10.10.4
A.12.4.4	Sincronización de relojes	SI	A.10.10.6
A.12.5	Control de software operacional		
A.12.5.1	Instalación de software en sistemas operativos	SI	A.12.4.1
A.12.6	Gestión de la vulnerabilidad técnica		
A.12.6.1	Gestión de las vulnerabilidades técnicas	SI	A.12.6.1
A.12.6.2	Restricciones sobre la instalación de software	NO	

Control 27001:2013	Controles	Existencia en norma anterior	Control 27001:2005
A.12.7	Consideraciones sobre auditorias de sistemas de información		
A.12.7.1	Controles de auditoria de sistemas de información	SI	A.15.3.1
A.13	Seguridad de las comunicaciones		
A.13.1	Gestión de la seguridad de las redes		
A.13.1.1	Controles de redes	SI	A.10.6.1
A.13.1.2	Seguridad de los servicios de red	SI	A.10.6.2
A.13.1.3	Separación en las redes	SI	A.11.4.5
A.13.2	Transferencia de información		
A.13.2.1	Políticas y procedimientos de transferencia de información	SI	A.10.8.1
A.13.2.2	Acuerdos sobre transferencia de información	SI	A.10.8.2
A.13.2.3	Mensajería electrónica	SI	A.10.8.4
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	SI	A.6.1.5
A.14	Adquisición, desarrollo y mantenimiento de sistemas		
A.14.1	Requisitos de seguridad de los sistemas de información		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	SI	A.12.1.1
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	SI	A.10.9.1 A.10.9.3
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	SI	A.10.9.2
A.14.2	Seguridad en los procesos de desarrollo y soporte		
A.14.2.1	Política de desarrollo seguro	NO	
A.14.2.2	Procedimientos de control de cambios en sistemas	SI	A.12.5.1
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	SI	A.12.5.2
A.14.2.4	Restricciones en los cambios a los paquetes de software	SI	A.12.5.3
A.14.2.5	Principios de construcción de los sistemas seguros	NO	
A.14.2.6	Ambiente de desarrollo seguro	NO	
A.14.2.7	Desarrollo contratado externamente	SI	A.12.5.5
A.14.2.8	Pruebas de seguridad de sistemas	NO	
A.14.2.9	Prueba de aceptación de sistemas	SI	A.10.3.2
A.14.3	Datos de prueba		
A.14.3.1	Protección de datos de prueba	SI	A.12.4.2
A.15	Relaciones con los proveedores		
A.15.1	Seguridad de la información en las relaciones con los proveedores		
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	SI	A.6.2.3

Control 27001:2013	Controles	Existencia en norma anterior	Control 27001:2005
A.15.1.2	Tratamiento de seguridad dentro de los acuerdos con proveedores	SI	A.6.2.3
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	NO	
A.15.2	Gestión de la prestación de servicios de proveedores		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	SI	A.10.2.2
A.15.2.2	Gestión de cambios en los servicios de los proveedores	SI	A.10.2.3
A.16	Gestión de incidentes de seguridad de la información		
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información		
A.16.1.1	Responsabilidades y procedimientos	SI	A.13.2.1
A.16.1.2	Reporte de eventos de seguridad de la información	SI	A.13.1.1
A.16.1.3	Reporte de debilidades de seguridad de la información	SI	A.13.1.2
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	NO	
A.16.1.5	Respuesta a incidentes de seguridad de la información	NO	
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	SI	A.13.2.2
A.16.1.7	Recolección de evidencia	SI	A.13.2.3
A.17	Aspectos de seguridad de la información de la gestión de continuidad del negocio		
A.17.1	Continuidad de seguridad de la información		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	SI	A.14.1.2
A.17.1.2	Implementación de la continuidad de la seguridad de la información	NO	
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	A.14.1.5
A.17.2	Redundancias		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	NO	
A.18	Cumplimiento		
A.18.1	Cumplimiento de requisitos legales y contractuales		
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	SI	A.15.1.1
A.18.1.2	Derechos de propiedad intelectual	SI	A.15.1.2
A.18.1.3	Protección de registros	SI	A.15.1.3
A.18.1.4	Privacidad y protección de información de datos personales	SI	A.15.1.4
A.18.1.5	Reglamentación de controles criptográficos	SI	A.15.1.6
A.18.2	Revisiones de seguridad de la información		
A.18.2.1	Revisión independiente de seguridad de la información	SI	A.6.1.8
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	SI	A.15.2.1

Control 27001:2013	Controles	Existencia en norma anterior	Control 27001:2005
A.18.2.3	Revisión del cumplimiento técnico	SI	A.15.2.2

Tabla 2. Comparativo objetivos de control ISO 27001: 2005 e ISO 27001:2013

De los dominios, un aspecto relevante, es la inclusión deldominio Relaciones con el proveedor, considerando la creciente tercerización de servicios, de igual forma es importante resaltar que los controles asociados existían en su mayoría, el nuevo control es el relativo a la cadena de suministro de tecnología de información y comunicación.

De igual forma se hace énfasis en el análisis de riesgos, y no se hace exigencia el levantamiento de activos.

Como requerimientos nuevos aparecen, la definición de los dueños de riesgos (clausula 6.1.2 c) y las partes interesadas (clausula 4.2). Entre los requerimientos que ya no son considerados están las acciones preventivas (dado que estas se consideran son realizadas si se realiza gestión de riesgos).

Periodo de transición

A continuación se presenta el periodo de transición que ha sido establecido para que las organizaciones que están certificadas en ISO 27001:2005 actualicen su sistema de gestión a la versión 2013 y el momento a partir del cual, las organizaciones que desean certificarlo, deben hacerlo en la nueva versión únicamente.

Ilustración 1. Periodo de transición a ISO 27001:2013

3. Presentación de la empresa

La empresa base para el desarrollo de este proyecto es una empresa dedicada a la transmisión de energía. Esta cuenta con una gran trayectoriay ha mejoradola prestaciónde susserviciosa partir de la ampliaciónde susinstalacionesy portafolio, funciona como una sociedadanónimapor acciones.

Cuenta con aproximadamente 400 colaboradoresentre empleadosy contratistas.

La misión de la empresa está enfocada a generar valor económico, social y ambiental a sus grupos de interés a partir de buenas prácticas y un equipo humano comprometido con su labor.

La visión, considera el reconocimiento en liderazgo y generación de valor económico, social y ambiental además, ser considerada la primera empresa en transmisión energética del país.

Como valores corporativos se consideran la transparencia, el respeto, la equidad y la integridad.

La empresa en estudio, como muestra de su compromiso con las buenas prácticas internacionales, creo un sistema de gestión integrado (Salud, seguridad, medio ambiente y calidad) al cual se agregará seguridad de la información y la continuidad del negocio. El alcance definido para el sistema de gestión integrado comprende:

- El negocio de transmisión de energía eléctrica: diseño, construcción, operación y mantenimiento de sistemas de transmisión de energía eléctrica, cuyo producto asociado es la disponibilidad de la infraestructura de transmisión y sus clientes son los agentes del sector.

- El negocio de portafolio accionario: identificación, evaluación, consolidación y seguimiento de inversiones en el sector energético, cuyo producto asociado son los informes de evaluación de la gestión de las participadas y sus clientes los accionistas.

Marco Normativo

A nivel de seguridad de la información la siguiente es la legislación que debe cumplir la empresa en estudio. Esta legislación es aplicable en Colombia.

Ley / norma / reglamentación	Explicación
Ley 1273 de 2009	Ley general de delitos informáticos que clasifica y asigna penas para delitos y crímenes relacionado con tecnología e informática
Ley 594 de 2000	Ley general de archivo de la nación que dispone tiempos de retención y cuidados para documentación física de tipo público
Ley 23 de 1982	Ley de derechos de autor aplicable a propiedad intelectual

Ley / norma / reglamentación	Explicación
Ley 527 de 1999	Ley de comercio electrónico que establece lineamientos y protección para acceso y uso de mensajes de datos, comercio electrónico y firmas digitales
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones
Ley Estatutaria 1581 de 2012	Ley que establece los requerimientos para la protección de la información personal almacenada por las organizaciones y evitar la divulgación de la misma.

Tabla 3. Normatividad Colombiana aplicable a la empresa con respecto a seguridad de la información

Mapa de procesos

El mapa de procesos de la empresa está estructurado en 21 procesos, bajo lineamientos estratégicos, de cadena de valor y soporte.

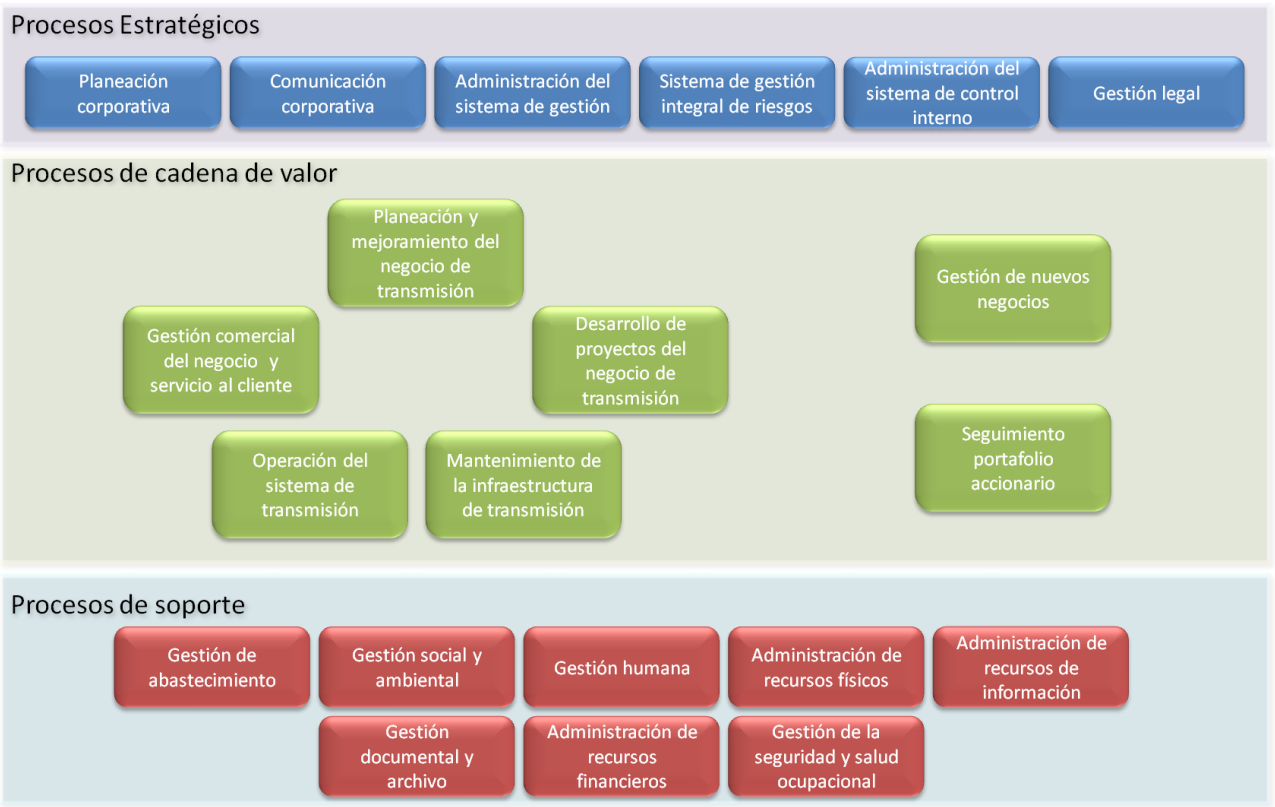

Ilustración 2. Mapa de procesos de la empresa en estudio

La descripción de los procesos es la siguiente:

Estratégicos

Se refieren a la planeación estratégica de la empresa en concordancia con las metas organizacionales, las necesidades de los clientes y al mejoramiento del servicio y del Sistema de Gestión integrado

- Planeación Corporativa: se planea la visión de la empresa, se evalúan los requerimientos del cliente, el entorno, se realizan las proyecciones financieras a mediano y largo plazo y se definen los objetivos, estrategias y proyectos del Plan Estratégico Corporativo; se establecen los mecanismos de medición del avance del logro planteado y de su gestión interna.

- Comunicación Corporativa: se gestiona las comunicaciones internas y externas de la empresa a través de los diferentes medios establecidos.

- Administración del Sistema de Gestión: se programan y evalúan las auditorías internas, se proponen acciones correctoras, correctivas, preventivas y de mejoramiento del sistema y se toman las acciones necesarias en las Revisiones del Sistema de Gestión Integrado por la Dirección.

- Sistema de Gestión Integral de Riesgos: se identifica, consolida y hace seguimiento a las acciones encaminadas a controlar los riesgos que puedan afectar el cumplimiento de los objetivos estratégicos y de gestión

- Administración del Sistema de Control Interno: se administran las Auditorías internas de control interno que contribuyen a la mejora continua de la gestión de la empresa.

- Gestión Legal: se gestiona la información de la empresa que se presenta a la Junta Directiva, a la Asamblea de Accionistas y se atienden los litigios.

De cadena de valor - Negocio de transmisión

Se refieren a la planeación y mejoramiento del negocio, el desarrollo de proyectos, la operación y mantenimiento de la infraestructura y la gestión comercial y servicio al cliente.

- Planeación y Mejoramiento del Negocio de Transmisión: se desarrollan actividades de interacción con las entidades regulatorias y del sector, se identifican y analizan alternativas de expansión y mejoramiento del negocio, se

planifican los recursos humanos, físicos, informáticos y financieros que requiere el negocio para la prestación del servicio.

- Desarrollo de Proyectos del Negocio de Transmisión: se planean y ejecutan los proyectos identificados en el Proceso Planeación y Mejoramiento del Negocio de Transmisión que contribuyen a la modernización de la infraestructura del negocio de transmisión.

- Mantenimiento de la Infraestructura de Transmisión: se planea, supervisa y se controla la ejecución de los trabajos de mantenimiento preventivo, correctivo y atención de emergencias en la infraestructura de transmisión conformada por líneas, activos en subestaciones y equipos de supervisión y control. La ejecución de los trabajos de mantenimiento es realizada por terceros.

- Operación del Sistema de Transmisión: se desarrollan actividades de supervisión, control, coordinación, estadísticas y ejecución de maniobras de los activos de transmisión en forma remota a través del Centro de Control de Transmisión y en coordinación con el CND entidad responsable de la operación del Sistema Interconectado Nacional – SIN.

- Gestión Comercial del Negocio y Servicio al Cliente: se desarrollan actividades de gestión comercial del negocio de transmisión y se atienden el servicio de conexión que requieran nuestros clientes.

De cadena de valor - Negocio de portafolio accionario

Se refieren al seguimiento de las participaciones accionarias y a las nuevas inversiones de la empresacontempladas en el Plan Estratégico Corporativo.

- Gestión Nuevos Negocios: se identifican, planean y consolidan nuevos proyectos de inversión que contribuyen a la visión de la empresa.

- Seguimiento Portafolio Accionario: se realiza el Seguimiento y evaluación de la gestión de las empresas que forman parte del portafolio accionario y se da apoyo al Distrito Capital en temas relacionados con la prestación de los servicios públicos en el sector de energía.

De soporte

Se refieren al apoyo en la contratación y compra de bienes y servicios, la gestión ambiental y la gestión de la seguridad y salud ocupacional, administración de los recursos humanos, físicos, informáticos y financieros y la gestión documental que brindan las demás áreas de la empresa.

- Gestión de abastecimiento: apoyo frente a la gestión de la adquisición de bienes y servicios

- Gestión Social y Ambiental: se define en el nivel Corporativo las herramientas de gestión ambiental y de cumplimiento normativo a partir de la responsabilidad ambiental y en el nivel operativo se asegura la viabilidad y sostenibilidad ambiental de los proyectos de construcción, operación y mantenimiento de la infraestructura de transmisión, y se ejecutan proyectos que contribuyan a afianzar las relaciones con las comunidades por donde pasa la infraestructura de transmisión de la empresa a través de la Gestión Social.

- Procesos Gestión Humana, Administración de Recursos Físicos, Administración de Recursos de Información y Gestión Documental y Archivo: se realiza la gestión humana, se administran los recursos humanos, físicos, informáticos, documentales y el archivo que contribuyen al desarrollo de las actividades propias de los procesos y a la preservación de la memoria institucional de la empresa.

- Administración de Recursos Financieros: se planea, administra y controla los recursos financieros de la empresa, garantizando su disponibilidad y oportunidad a mediano y largo plazo. Así mismo, se apoya el desarrollo del plan estratégico facilitando el acceso a fuentes de financiación locales e internacionales a través de una comunicación bidireccional con los mercados financieros.

- Gestión de la Seguridad y Salud ocupacional: se identifican los peligros ocupacionales, se valoran los riesgos y se determinan los controles para suprevención y/o control de acuerdo con los procesos, procedimientos y actividades que se realizan en la empresa.

Nota: Es importante resaltar, que como parte del proyecto de integración de seguridad de la información en el sistema de gestión integral, se busca integrar esta como uno de los procesos de soporte. Este es un proyecto en curso actualmente dentro de la empresa.

Estructura organizacional de la empresa

A continuación se presenta la estructura organizacional de la empresa en estudio

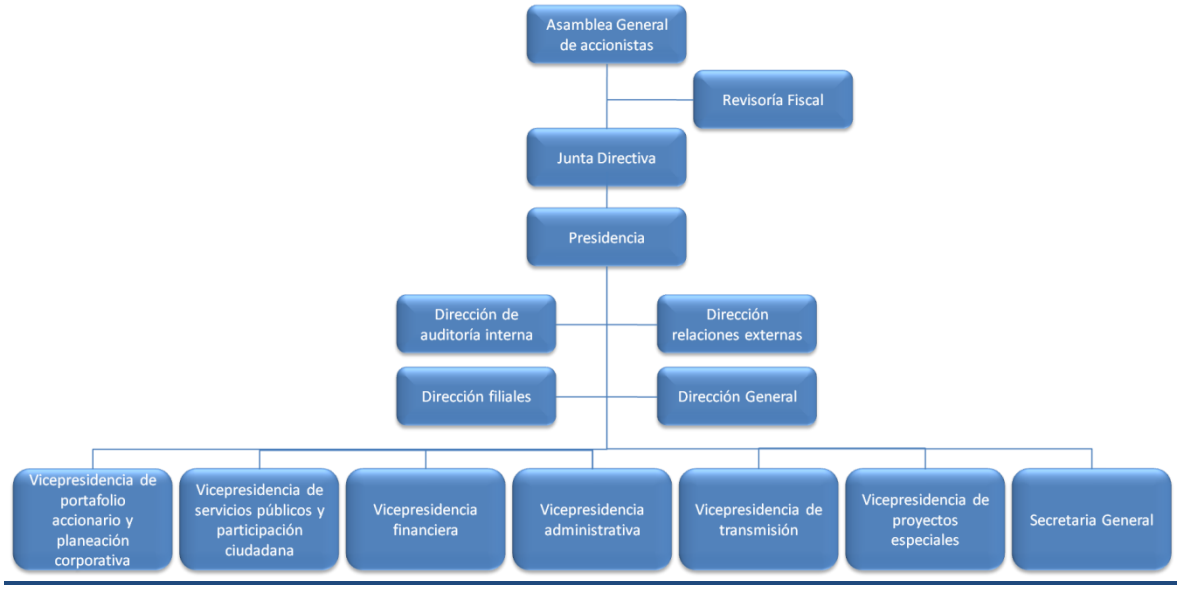

Ilustración 3. Organigrama de la empresa en estudio

4. Análisis diferencial SGSI

Con el fin de evaluar el estado actual en seguridad de la información para la empresa en estudio frente a la norma ISO 27001:2013 e ISO 27002:2013 se realizó un análisis diferencial para encontrar las brechas existentes entre lo actualmente implementado por la empresa y los requisitos de la norma.

El informe de resultados se encuentra en el documento anexo "Análisis diferencial SGSI". y el detalle de la evaluación está en las listas de chequeo "CheckList 27002_2013" y "CheckList 27001_2013".

Nota: Estos documentos se encuentran en la carpeta anexa Análisis Diferencial

5. Alcance del SGSI

La norma **ISO 27001:2013 en el numeral 4.3 Alcance del SGSI** establece los requisitos para su definición:

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance. Cuando se determina este alcance la organización debe considerar:

a) Las cuestiones externas e internas (contexto de la organización, numeral 4.1)
b) Los requisitos de las partes interesadas (numeral 4.2)
c) las interfaces y dependencias entre las actividades realizadas por la organización, y las que realizan otras organizaciones

El alcance debe estar disponible como información documentada.

Para validar su alineación con la norma, a continuación se presenta el alcance actual para el Sistema de Gestión de Seguridad de la Información (SGSI) de la empresa en estudio:

"El límite del Sistema de Gestión de Seguridad de la información está definido por los activos de información que apoyan los procesos siguientes asociados a los negocios de Transmisión de energía eléctrica y el negocio de Portafolio accionario de la Empresa

- SGSI (Proceso de soporte) –Desarrollado en la sede principal de la empresa en la dirección XXXX
- Control Interno (Proceso estratégico) - Desarrollado en la sede principal de de la empresa en la dirección XXXX
- Gestión de nuevos negocios (Proceso cadena de valor) - Desarrollado en la sede principal de de la empresa en la dirección XXXX
- Gestión documental (Proceso de soporte) - Desarrollado en la sede principal de de la empresa en la dirección XXXX
- Gestión humana (Proceso de soporte) - Desarrollado en la sede principal de de la empresa en la dirección XXXX
- Desarrollo de proyectos de transmisión (Proceso cadena de valor) - Desarrollado en la sede principal de de la empresa en la dirección XXXX"

Es importante indicar, que el SGSI de esta empresa está recién implementado y no ha completado el ciclo completo.

Nota: El proceso SGSI está en proceso está en proceso de implementación. El mapa de procesos será ajustado para Junio de 2014 para incluir este proceso como parte de los procesos de soporte.

A partir de esto se puede indicar que al alcance actual debe agregarse:

- El contexto interno y externo de la empresa y,
- Los requerimientos de las partes interesadas frente al SGSI

A continuación se determinan estos dos aspectos para dar el nuevo enfoque al alcance del SGSI

Contexto interno y externo

Para el desarrollo del contexto interno y externo de la empresa en estudio, se realizará un análisis DOFA (Debilidades, Oportunidades, Fortalezas, Amenazas), de esta forma se pueden analizar características internas (Debilidades y Fortalezas) y características externas (Oportunidades y Amenazas).

	Fortalezas	Debilidades
Análisis interno	• Cuenta con filiales a nivel nacional y fuera del país en Latinoamérica lo que le da ventaja competitiva frente a la competencia.	• Alta dependencia de terceros para la contratación de servicios. • Cerca del XXX % del personal es contratista.

	• Inversiones varias en el sector eléctrico y de gas natural que le posicionan en el mercado. • La empresa cuenta con un sistema de gestión integrado (Calidad, ambiental, salud ocupacional, eficiencia energética) que le facilita el control y mantenimiento sobre sus procesos así como el mejoramiento continuo. • Contar con procedimientos de comunicación interna y externa claramente definidos. • Equipo multidisciplinar al interior de la empresa • Bajo nivel de rotación de empleados. • Interés de la empresa por la gestión ambiental, la responsabilidad social y los riesgos ocupacionales.	• Los empleados no tienen posibilidad de crecen en la empresa y puede ser causal de renuncia. • Por tratarse de una empresa de varios años, alguna de la infraestructura es de bajo nivel de innovación y escasa presencia de nuevas tecnologías. • La cultura en seguridad de la información dentro de la empresa es incipiente, sin embargo ya se está trabajando en su fortalecimiento.
	Oportunidades	**Amenazas**
Análisis externo	• Oportunidades de expansión en el mercado nacional y latinoamericano considerando el nombre de la empresa y las relaciones con organizaciones del sector. • El tipo de servicio comercializado por la empresa es una necesidad para los ciudadanos. • Aceptación de la empresa por parte de la comunidad de influencia.	• Factores políticos considerando que la organización es una sociedad por acciones, constituida como una empresa de servicios públicos mixta. La presidencia es designada por la administración de turno así como la junta directiva. • El control por parte de entidades como la CREG (Comisión de Regulación de Energía y Gas), la SSPD (Superintendencia de servicios públicos domiciliarios), la UPME (Unidad de planeamiento minero energético), el Ministerio de minas y energía, la CND (Centro nacional de despacho) y demás entes; implican precisión y cuidado frente al cumplimiento de las leyes aplicables. • Estar sujeto a regulación en diferentes países para sus negocios de transmisión de energía y gas natural, que también implica cuidado en el cumplimiento de leyes. • Por la naturaleza de la operación de la empresa y la situación de seguridad en

		el país, está sujeta a posibles atentados por parte de grupos fuera del margen de la ley. • Cambios en la estructura organizacional que pueden impactar la organización.

Tabla 4. Análisis DOFA para determinar el contexto de la empresa

Partes interesadas y sus requerimientos frente al SGSI

Las siguientes son las partes interesadas identificadas frente al SGSI y sus requerimientos

Parte interesada	Requerimientos
Entes de control	Cumplimiento de la legislación y regulación en temas relativos a seguridad de la información referente a la actividad de la empresa.
Clientes (Empresas de distribución de energía)	Protección de la operación para que le aseguren servicio seguro sí como información.
Proveedores (Empresas de generación de energía)	Continuidad en la contratación, cumplimiento en pagos, protección de la información.
Comunidad aledaña	Seguridad física al estar cerca a instalaciones de la empresa
Filiales	Lineamientos y acompañamiento para su propio implementación.
Competencia	Mantenimiento de la operación
Alta dirección	Contar con altos estándares de seguridad para el desarrollo de la operación, para poder utilizar esto como una ventaja frente a su competencia y fortalecer la imagen de la empresa en el mercado.
Accionistas	Contar con la implementación de seguridad de la información dentro de la empresa para mejorar sus ganancias.
Colaboradores y contratistas	Contar con condiciones de seguridad física y lógica en el desarrollo de sus funciones dentro de la empresa, sin sentir vulnerados sus derechos a privacidad.
Control interno	Cumplimiento y responsabilidad social

Tabla 5. Partes interesadas y sus requerimientos frente al SGSI

Considerando lo anterior el alcance para ser ajustado a los requerimientos de ISO 27001:2013 es el siguiente:

"El límite del Sistema de Gestión de Seguridad de la información está definido por los activos de información que apoyan los procesos siguientes asociados a los negocios de Transmisión de energía eléctrica y el negocio de Portafolio accionario de la Empresa

- SGSI (Proceso de soporte) –Desarrollado en la sede principal de la empresa en la dirección XXXX
- Control Interno (Proceso estratégico) - Desarrollado en la sede principal de de la empresa en la dirección XXXX

- Gestión de nuevos negocios (Proceso cadena de valor) - Desarrollado en la sede principal de de la empresa en la dirección XXXX
- Gestión documental (Proceso de soporte) - Desarrollado en la sede principal de de la empresa en la dirección XXXX
- Gestión humana (Proceso de soporte) - Desarrollado en la sede principal de de la empresa en la dirección XXXX
- Desarrollo de proyectos de transmisión (Proceso cadena de valor) - Desarrollado en la sede principal de de la empresa en la dirección XXXX

Con respecto a estos procesos, se consideran los requerimientos y necesidades en seguridad de la información para sus grupos de interés o partes interesadas y se consideran las fortalezas, debilidades, oportunidades y amenazas a las que se enfrenta la organización para lograr la seguridad de la información."

6. Objetivos del SGSI

La norma **ISO 27001:2013 en el numeral 6.2 Objetivos de seguridad de la información y planes para lograrlos** establece los requisitos para su definición:

La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes. Los objetivos de seguridad de la información deben:

a) ser coherentes con la política de seguridad de la información
b) ser medibles (si aplica)
c) tener en cuenta requisitos de seguridad aplicables y los resultados de valoraciones y de tratamiento de riesgos
d) ser comunicados
e) ser actualizados

Se debe conservar información documentada de los objetivos. En la planificación de los objetivos, se debe determinar:

f) lo que se va a hacer
g) los recursos necesarios
h) responsables
i) cuándo se finalizará
j) cómo se evaluarán los resultados

A continuación se presentan los objetivos de seguridad de la información definidos por la empresa:

"Son objetivos de la gestión en Seguridad de la información:

I. Proteger a la infraestructura y los procesos de transmisión de energía de la empresa ante riesgos que afecten la seguridad de la información.
II. Demostrar a inversionistas e interesados que se protege adecuadamente la información y las tecnologías empleadas para los negocios de la empresa.

III. Implementar y gestionar las acciones para prevenir, mitigar y remediar los impactos de los riesgos de seguridad de la información.
IV. Dar cumplimiento a los requerimientos de privacidad y de protección de datos establecidos por las leyes Colombianas e internacionales aplicables.
V. Fomentar una cultura organizacional frente a la protección de la información donde todos reconozcan sus roles y responsabilidades en la preservación de su confidencialidad, integridad y disponibilidad."

Para cada objetivo se ha definido un plan para alcanzarlo e indicadores que permitan medir su evolución y cumplimiento. La alineación entre objetivos y la política se presenta a continuación:

POLÍTICA VS. OBJETIVOS DEL SISTEMA DE GESTIÓN		
Política (Resumen o descripción principal)	**Directriz de política (Principal compromiso extraído de la política)**	**Objetivo**
La Empresa XXX mediante esta política reconoce a la información como un activo fundamental y estratégico para el desarrollo sus actividades, en donde la protección y seguridad de esta información y el conocimiento generado tiene una importancia primordial en los objetivos de la Empresa	Identificar y reconocer los requerimientos de protección de la información y medios de procesamiento dentro de la Empresa.	Proteger a la infraestructura y los procesos de transmisión de energía ante riesgos que afecten la seguridad de la información.
	Preservar las propiedades de confidencialidad, integridad y disponibilidad de su información, protegiéndola contra amenazas internas, externas, accidentales o deliberadas, mediante la implementación de prácticas de gestión tendientes a dar tratamiento a los riesgos sobre esta y llevarlos a los niveles aceptables definidos por la Empresa.	Demostrar a inversionistas e interesados que se protege adecuadamente la información y las tecnologías empleadas para los negocios de empresa.
	Establecer, implementar y operar un modelo de gestión de seguridad de la información con un enfoque repetible, sostenible en el tiempo y de mejora continua en un marco de gestión de riesgos	Implementar y gestionar las acciones para prevenir, mitigar y remediar los impactos de los riesgos de seguridad de la información.
	Reconocer y dar cumplimiento a todos los requerimientos normativos y legales aplicables a la información empresarial, personal y de terceros	Dar cumplimiento a los requerimientos de privacidad y de protección de datos establecidos por las leyes Colombianas e internacionales aplicables.
	Establecer mecanismos de concientización en temas de seguridad para los usuarios	Fomentar una cultura organizacional frente a la protección de la información donde todos reconozcan sus roles y responsabilidades en la preservación de su confidencialidad, integridad y disponibilidad.
	Establecer los roles y responsabilidades frente a la protección de la información	

Tabla 6. Política versus objetivos del SGSI

Los objetivos han sido divulgados en la organización mediante charlas informativas y por medios de la empresa como carteleras, la intranet, fondos de pantalla.

7. Política de Seguridad de la información

La norma **ISO 27001:2013 en el numeral 5.2 Política** establece los requisitos para su definición:

La política debe ser establecida por la alta dirección y debe considerar:

1) ser adecuada al propósito de la organización

2) incluir los objetivo de seguridad de la información o proporcione un marco de referencia para que estos se establezcan

3) incluya compromiso de cumplir requisitos aplicables relativos a seguridad de la información

4) la política debe estar disponible como información documentada

5) debe ser comunicada dentro de la organización

6) debe estar disponible para las partes interesadas

A partir de esto se puede indicar lo siguiente sobre la actual política:

1) Es adecuada al propósito de la organización, aunque en la forma de su redacción puede pasar por una política genérica. En tal caso, se recomendó a la empresa, ajustarla para que sean visibles los componentes de la empresa y de forma aportar al sentido de pertenencia de los colaboradores.

2) Como parte de las definiciones del sistema integral, se maneja una matriz de políticas versus los objetivos del sistema de gestión (para el caso de seguridad, los objetivos definidos para seguridad de la información) para resaltar la relación entre la política, sus directrices y los objetivos cubiertos.

3) El compromiso de cumplimiento está redactado como parte de la política

4) Al momento de este análisis, está política no ha sido aprobada por la dirección, lo cual es el punto faltante. A partir de esta aprobación, será comunicada dentro de la empresa de manera formal y se pondrá a su disposición.

A continuación se presenta la política:

Política de seguridad de la información de la empresa en estudio

"La Empresa, mediante esta política reconoce a la información como un activo fundamental y estratégico para el desarrollo de las actividades en la empresa, en donde la protección y seguridad de esta informacióny el conocimiento generado tiene una importancia primordial en los objetivos de la Empresa; en este sentido declara su compromiso a:

- Identificar y reconocer los requerimientos de protección de la información y medios de procesamiento dentro de la Empresa.
- Preservarlas propiedades de confidencialidad, integridad y disponibilidad de su información, protegiéndola contra amenazas internas, externas, accidentales o deliberadas, mediante la implementación de prácticas de gestión tendientes a

dar tratamientoa los riesgos sobre esta, garantizando las acciones y recursos requeridos parallevarlos a los niveles aceptables definidos por la Empresa.
- Establecer, implementar y operar un modelo de gestión de seguridad de la información con un enfoque repetible, de mejora continua, sostenible en el tiempoy dentro de un marco de gestión de riesgos.
- Reconocer y dar cumplimiento a todos los requerimientos normativos y legales aplicables a la información empresarial, personal y de terceros;
- Establecer mecanismos de concientización en temas de seguridad de la información para todos los funcionarios y partes interesadas.
- Establecer los roles y responsabilidades frente a la protección de la información empresarial.

Esta política fomenta el compromiso organizacional en la protección de la información y creación de una cultura alrededor de este tema, en un marco de cumplimiento a los requisitos de protección de la información, donde esto se incorpore en la gestión del día a día de nuestro actuar y donde se entienden los roles y responsabilidades de cada uno y se actúa en consecuencia, para que la información y la seguridad de la información sean un habilitador de negocio y contribuyan al crecimiento y mejoramiento de la Empresa, permitiendo en consecuencia alcanzar los objetivos de los procesos y los objetivos corporativos establecidos en su plan estratégico."

8. Roles y responsabilidades en Seguridad de la información

La norma **ISO 27001:2013 en el numeral 5.3 Roles, Responsabilidades y Autoridades en la organización**, establece los siguientes requerimientos:

1) la alta dirección debe asegurar la asignación y comunicación de las responsabilidades y autoridades pertinentes para los roles del SGSI

2) la alta dirección debe asignar responsabilidad y autoridad para asegurar que el SGSI sea conforme con ISO 27001:2013

3) la alta dirección debe asignar responsabilidad y autoridad para tener una fuente que le reporte sobre el desempeño del SGSI

A continuación se presenta la definición de los roles y responsabilidades:

Definición de roles y responsabilidades

La empresa en estudio, frente a los temas de seguridad de la información por decisión de Gerencia reglamento las políticas informáticas y de seguridad de la información en la Empresa, en la sección “Responsabilidades” artículo PRIMERO, se establecen las diferentes responsabilidades frente a la seguridad de la información en distintos grados para los siguientes roles:

Ilustración 4. Organización de seguridad de la información definida para la empresa

Las responsabilidades se han definido con respecto a:

- Responsabilidades generales
- Gestión de normatividad y cumplimiento
- Gestión de riesgos
- Revisión y medición del SGSI
- Gestión de activos
- Gestión de incidentes
- Gestión de la cultura

El detalle de las responsabilidades definidas se encuentra en el documento anexo "Roles y Responsabilidades".

Nota: El documento se encuentra en la carpeta anexa Roles y Responsabilidades.

9. Revisión por la dirección

La norma **ISO 27001:2013 en el numeral 9.3 Revisión por la dirección** establece los siguientes requisitos:

1) la revisión debe realizarse a intervalos planificados, para asegurar su conveniencia, adecuación y eficacia continuas

2) en las revisiones se deben incluir consideraciones sobre:

- el estado de las acciones con relación a las revisiones previas
- cambios en el contexto de la empresa que sean pertinentes al SGSI

- retroalimentación sobre el desempeño de la seguridad de la información (no conformidades y acciones correctivas, seguimiento y resultados de medición, resultados de auditoría, cumplimiento de objetivos de seguridad)
- retroalimentación de partes interesadas
- resultados de valoración de riesgo y estado de planes de tratamiento
- oportunidades de mejora para el SGSI

3) como salidas deben considerarse decisiones relacionadas con oportunidades de mejora y necesidades de cambio frente al sistema.

4) se debe conservar información documentada como evidencia de la revisión

A partir de estos requisitos y revisando como es realizada la revisión por la dirección en la empresa en estudio, se puede determinar que ya se encuentran alineados a la norma, considerando todos los aspectos necesarios.

A continuación se presenta el esquema de revisión por la dirección que tiene la empresa en estudio:

Revisión por la dirección para el Sistema de gestión integrado de la empresa

"La revisión del Sistema de Gestión Integrado por la Alta Dirección la realiza la Presidencia, la Vicepresidencia de Transmisión, la Vicepresidencia de Portafolio Accionario y Planeación Corporativa y la Vicepresidencia Administrativa como responsable de la administración del sistema de gestión integrado, verificando entre otros los siguientes puntos:

- Las Políticas de Calidad, Seguridad y Salud Ocupacional, Seguridad de la información y Ambiental.
- El cumplimiento de los Objetivos de Calidad, seguridad de la información, objetivos ambientales y de seguridad y salud ocupacional.
- El desempeño de los procesos y conformidad de los productos, incluyendo la retroalimentación del cliente y partes interesadas de los sistemas de gestión.
- El desempeño en calidad, ambiental, seguridad de la información, y Seguridad y Salud Ocupacional.
- Los resultados de las auditorías internas y/o externas.
- Las acciones correctivas y/o preventivas necesarias para el mejoramiento del Sistema de Gestión, así como el estado de aquellas que se hayan identificado.
- Las acciones de seguimiento de las revisiones por la Dirección previas.
- Avance y cumplimiento de la implementación de los planes de tratamiento definidos para los riesgos identificados.
- Resultados de las mediciones de eficacia del Sistema de Gestión
- Cambios y requerimientos organizacionales que podrían afectar al Sistema de Gestión.
- Recomendaciones para la mejora.
- Resultados de la gestión de riesgos corporativos, esto incluye vulnerabilidades o amenazas no tratadas en la valoración previa de riesgos.
- Los resultados de participación y consulta.

Se ha establecido, que estas revisiones se realicen al menos una (1) vez al año o de manera extraordinaria, y se pueden realizar dentro del Comité de Presidencia, cuando así lo determine la Presidencia o lo considere necesario la Vicepresidencia Administrativa.

En cuanto a la medición del cumplimiento de los Objetivos de Calidad su revisión se realiza dentro del seguimiento al correspondiente Plan Estratégico.

Resultados de la revisión

Las decisiones y acciones tomadas en la Revisión por la Dirección quedan registradas en Actas bajo la responsabilidad de la Vicepresidencia Administrativa a través de la Gerencia del Sistema de Gestión Integrado."

A partir de este procedimiento de revisión, como información documentada que de soporte al mismo, se establecen los siguientes registros, que se encuentran como anexos:

- Formato de actas de revisión por la dirección
- Formato para informe a la dirección
- Formato para resultados revisión de la dirección

Nota: Estos documentos se encuentran en la carpeta anexa Revisión por la dirección

10. Gestión de indicadores

Como parte fundamental para validar como se está llevando a cabo la implementación de la seguridad de la información, es necesario establecer indicadores que permitan validar que requiere ser medido, como se realizará la medición, cuales son las responsabilidades frente a esta medición y el proceso de evaluación de resultados en busca de la mejora del sistema.

Para esto se ha definido un procedimiento de gestión de indicadores que indica cómo se realizaran las mediciones con respecto a 8 indicadores:

a) Tratamiento de riesgos de seguridad de la información
b) Gestión de la cultura en seguridad de la información
c) Inversión en seguridad de la información
d) Gestión de vulnerabilidades de seguridad
e) Gestión de líneas base de seguridad
f) Gestión de incidentes
g) Mejoramiento del SGSI
h) Revisiones al SGSI

El detalle del procedimiento y los formatos para realizar la medición se encuentra en los documentos anexos gestión de indicadores y Medición de indicadores.

Nota: Los documentos se encuentran en la carpeta adjunta Gestión de indicadores.

11. Metodología de análisis de riesgos

La metodología de análisis de riesgos de la empresa en estudio tiene como base estándares y buenas prácticas como ISO 27005:2008 e ISO 27001:2005. Esta metodología como estaba planteada requería algunos ajustes para estar alienada con los requisitos de ISO 27001:2013 en lo respectivo a la definición de criterios de valoración en escalas de impacto, criterios de aceptación de riesgo, tipos de impacto, riesgo base, entre otros.

La metodología definida se encuentra en el documento anexo Metodología de gestión de riesgo.

Nota: El documento se encuentra en la carpeta anexa Gestión de riesgos

12. Análisis de riesgos

Tomando como referencia la Metodología de riesgos que se presento en el numeral 11, se realizó el análisis de riesgos para la empresa en estudio. Para ello se definieron 91 riesgos base asociados a la pérdida de disponibilidad, confidencialidad o integridad de los activos de la organización. Cada riesgo tiene una descripción, una amenaza y una vulnerabilidad asociadas, un nivel de impacto y una probabilidad que dan lugar a un nivel de riesgo.

De acuerdo al criterio establecido por la empresa en estudio, los riesgos que se encuentran en nivel extremo y alto son aquellos que deben ser tratados. Los riesgos en nivel moderado y bajo son aceptables.

En el archivo Excel adjunto "Matriz Riesgos", están los resultados finales del análisis de riesgos a partir de la metodología de gestión de riesgo presentada.

Más detalle sobre el análisis de riesgos no es suministrado por restricción de la empresa en estudio

Nota: el archivo se encuentra en la carpeta anexa Gestión de riesgos

13. Declaración de aplicabilidad

La actual declaración de aplicabilidad se encuentra enmarcada contra los controles del Anexo A de la norma ISO 27001:2005.

De los 133 controles de esta norma están aplicando 130. Las exclusiones se dan sobre los controles:

- 6.2.2 Consideraciones de la seguridad cuando se trata con los clientes, dado que los clientes no tiene acceso directo a sistemas de información o recursos de la empresa.

- 10.9.1 Comercio electrónico, dado que la empresa no cuenta con este servicio

- 10.9.2 Transacciones en línea, considerando la exclusión del control anterior.

Ahora en la norma ISO 27001:2013 en su anexo A maneja 114 controles de los cuales todos se deben manejar de acuerdo al análisis realizado.

En el documento adjunto Excel Declaración de aplicabilidad se encuentra el detalle de las inclusiones.

Nota: el archivo se encuentra en la carpeta anexa Gestión de riesgos

14. Planes de tratamiento

A partir de los resultados del análisis de riesgos se tienen 91 riesgos definidos que se clasifican de la siguiente forma:

Extremos	52
Altos	24
Moderados	12
Bajos	3

De acuerdo a lo definido por la dirección, se dará tratamiento a los 76 riesgos que se encuentran en nivel extremo (52) y alto (24). Para ello se definieron unos planes de tratamiento a partir de unas líneas base de controles que permiten agrupar riesgos para su tratamiento facilitando su seguimiento y gestión.

La descripción de los controles definidos se encuentra en el documento adjunto Implementación planes de tratamiento que se encuentra en la carpeta Gestión de riesgos.

El plan de tratamiento está definido en el documento adjunto Plan tratamiento. A nivel de cada control se ha definido una etapa de diseño, implementación, revisión de implementación, revisión de operación, e indicadores de implementación e eficacia. Un ejemplo de estas definiciones se presenta en el archivo Excel Anexo tratamiento PDT - Administración de recursos físicos.

Nota: por temas de confidencialidad de la empresa, solo se presenta este archivo para un control. Sin embargo los otros controles manejan el mismo esquema.

Los controles a implementar para cada riesgo están en el archivo Excel Matriz Riesgos con controles aplicables.

Nota: Estos documentos se encuentran en la carpeta anexa Gestión de riesgos

15. Procedimiento de auditorías internas

Parte importante del mantenimiento del sistema de gestión de seguridad de la información es evaluar que los planes de tratamiento se han realizado, así como el seguimiento a la mejora del sistema mediante revisiones, y todo el proceso de mejora en la implementación inicial. Para ello se ha definido un procedimiento de auditorías internas que permita realizar este seguimiento.

Nota: El procedimiento de auditorías internas se encuentra como anexo la carpeta Procedimiento de auditoría interna. En este se detalla el paso a paso para la realización de auditorías y se hace mención a los formatos anexos que se encuentran en la misma carpeta.

16. Auditoría de cumplimiento contra ISO 27002:2013

Una vez ya están en proceso de implementación los controles definidos para mitigar los riesgos se validará la madurez de la organización frente a cada uno de los controles definidos en ISO 27002:2013.

Este estándar maneja 114 controles, 35 objetivos de control y 14 dominios. El detalle en su explicación se puede encontrar en el numeral 2 de este documento.

Para realizar la validación del nivel de madurez de la empresa frente a cada control se tomará como referencia la siguiente tabla que se basa en el modelo de madurez de la capacidad de CMM:

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	**L0**	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	**L1**	Inicial /Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	**L2**	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	**L3**	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
95%	**L4**	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	**L5**	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla 7. Matriz de madurez CMM

En el documento Excel Madurez controles ISO que está en la carpeta auditoria cumplimiento, se encuentra el detalle de las calificaciones de madurez dadas a cada uno de los 114 controles de ISO 27002:2013.

A continuación se presenta los resultados obtenidos por cada nivel de madurez:

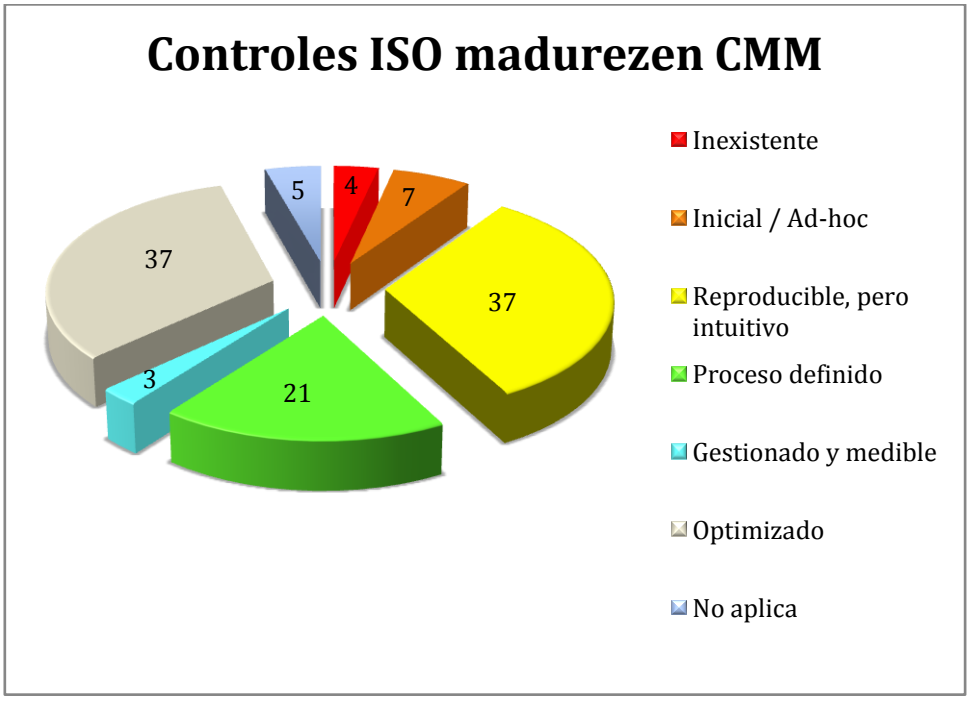

Ilustración 5. Madurez de controles ISO de acuerdo a matriz CMM

	Nivel de Madurez	Cantidad de Controles	Porcentaje
L0	Inexistente	4	4%
L1	Inicial / Ad-hoc	7	6%
L2	Reproducible, pero intuitivo	37	32%
L3	Proceso definido	21	18%
L4	Gestionado y medible	3	3%

	Nivel de Madurez	Cantidad de Controles	Porcentaje
L5	Optimizado	37	32%
N/A	No aplica	5	4%
	Total	**114**	**100%**

Tabla 8. Madurez controles ISO

A nivel de cada uno de los dominios, el nivel esperado por la organización en términos de efectividad es del 95%. A continuación se presenta a partir de esta revisión cual es su nivel de efectividad actual por dominio:

No	Dominio	Efectividad actual	Efectividad esperada
A.5	Políticas de seguridad de la información	**25%**	**95%**
A.6	Organización de la seguridad de la información	**34%**	**95%**
A.7	Seguridad de los recursos humanos	**53%**	**95%**
A.8	Gestión de activos	**67%**	**95%**
A.9	Control de acceso	**52%**	**95%**
A.10	Criptografía	**38%**	**95%**
A.11	Seguridad física y del entorno	**68%**	**95%**
A.12	Seguridad de las operaciones	**87%**	**95%**
A.13	Seguridad de las comunicaciones	**90%**	**95%**
A.14	Adquisición, desarrollo y mantenimiento de sistemas	**82%**	**95%**
A.15	Relaciones con los proveedores	**58%**	**95%**
A.16	Gestión de incidentes de seguridad de la información	**56%**	**95%**
A.17	Aspectos de seguridad de la información de la gestión de continuidad del negocio	**43%**	**95%**
A.18	Cumplimiento	**61%**	**95%**

Tabla 9. Efectividad actual por dominio

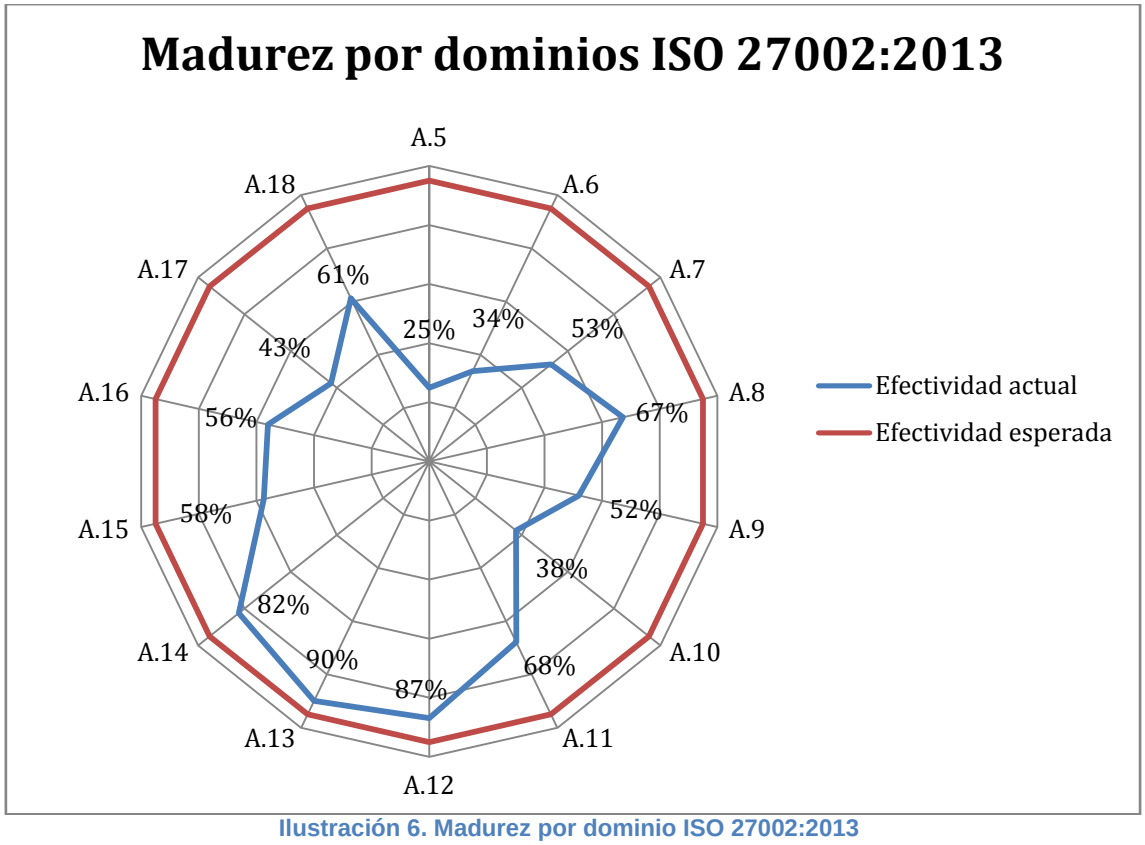

Ilustración 6. Madurez por dominio ISO 27002:2013

Glosario

Riesgo: El impacto neto considerando (1) la probabilidad de que una fuente de amenaza particular (explote accidental o intencionalmente) una vulnerabilidad particular del sistema de información y (2) el impacto resultante en caso de que esto ocurra. El riesgo relacionado con TI se deriva de la responsabilidad legal o perdida de misión debido a:

a. Divulgación no autorizada (intencional o accidental), modificación, o destrucción de información
b. Errores y omisiones no intencionales
c. Interrupciones de TI a causa de desastres naturales o causados por el hombre
d. El no ejercer el debido cuidado y diligencia en la implementación y operación de sistema de TI. [NIST02]

El potencial de que una amenaza específica explote las vulnerabilidades de un activo o grupo de activos para ocasionar pérdida y/o daño a los activos. Por lo general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia. [COB07]

Riesgo residual: Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información [MINIST06]

Criterio de riesgo: Términos de referencia con lo que el riesgo es valorado [ISO02]

Estimación del riesgo: Proceso usado para asignar valor a la probabilidad y consecuencias de un riesgo [ISO02]

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo. [ISO05]

Identificación del riesgo: Proceso para encontrar, listar e identificar los elementos de riesgo. [ISO08]

Análisis del riesgo: Uso sistemático de la información para identificar las fuentes y estimar el riesgo. [ISO05]

Valoración del riesgo: Proceso global de análisis y evaluación del riesgo. [ISO05]
Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo. [ISO05]

Análisis de impacto: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización [MINIST06]

Impacto: Consecuencia que sobre un activo tiene la materialización de una amenaza [MINIST06]

Impacto residual: Impacto remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información [MINIST06]

Incidente: Evento con consecuencias en detrimento de la seguridad del sistema de información [MINIST06]

Evento: Ocurrencia de un conjunto particular de circunstancias [NTC06]

Información: “Es un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones" [IDALBE05]

Activo: Cualquier cosa que tiene valor para la organización. [ISO05]

Degradación: Pérdida de valor de un activo como consecuencia de la materialización de una amenaza [MINIST06]

Amenaza: Eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. Las amenazas se pueden materializar y transformarse en agresiones. Pueden afectar a la integridad, confidencialidad o disponibilidad. [ARTOOL08]

Frecuencia: Tasa de ocurrencia de una amenaza [MINIST06]

Vulnerabilidad: "Una vulnerabilidad es una debilidad de seguridad en un sistema informático que suele encontrarse en programas y sistemas operativos. La presencia de vulnerabilidades conocidas en sistemas informáticos puede dejar estos sistemas expuestos a los ataques de malware. Esto se debe a que los programas que aprovechan las vulnerabilidades conocidas, normalmente llamados exploits, a menudo están disponibles públicamente como código origen, que se puede personalizar para crear una herramienta de malware o de hacking." [TRENDM08]

Consecuencia: Resultado de un evento [CNSS10]

Probabilidad: Medida de la oportunidad de ocurrencia expresada como un número entre o y 1 [NTC06]

Control: Proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo negativo o potenciar oportunidades positivas. [NTC06]

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad. [ISO05]

Dimensión de seguridad: Un aspecto, diferenciado de otros posibles aspectos, respecto del que se puede medir el valor de un activo en el sentido del perjuicio que causaría su pérdida de valor [MINIST06]

Disponibilidad: El objetivo de seguridad que genera los requerimientos para protección contra:

1. Intentos intencionales o accidentales de (1) realizar la destrucción no autorizada de datos o (2) de otra forma causar una denegación de servicios o datos
2. El uso no autorizado de recursos del sistema[NIST02]

Integridad: El objetivo de seguridad que genera requerimientos de protección contra cualquier intento intencional o accidental de violar la integridad de los datos (la propiedad que tienen cuando no han sido alterados de forma no autorizada) o la integridad de los sistemas (la calidad que un sistema tiene cuando se lleva a cabo su función prevista en una forma irreprochable, libre de manipulación no autorizada) [NIST02]

Confidencialidad: El objetivo de seguridad que genera requerimientos para protección de intentos intencionales o accidentales para realizar lectura de datos no autorizados. La confidencialidad cubre datos en almacenamiento, durante el procesamiento y en tránsito. [NIST02]

Trazabilidad: Aseguramiento de que en todo momento se podrá determinar quien hizo que y en qué momento [MINIST06]

Autenticidad: Aseguramiento de la identidad u origen [MINIST06]

Sistema de Gestión de Seguridad de la Información (SGSI): Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. [ISO05]

Continuidad del negocio: Prevenir, mitigar y recuperarse de una interrupción. Los términos "planear la reanudación del negocio", "planear la recuperación después de un desastre" y "planear contingencias" también se pueden usar en este contexto; todos se concentran en los aspectos de recuperación de la continuidad. [COB07]

Infraestructura tecnológica: La tecnología, los recursos humanos y las instalaciones que permiten el procesamiento de las aplicaciones. [COB07]

Sistema de información: "Un sistema de información es un conjunto de elementos o componentes interrelacionados para recolectar (entrada), manipular (proceso) y diseminar (salida) datos e información y para proveer un mecanismo de retroalimentación en pro del cumplimiento de un objetivo" [ISO05]

Ciclo Deming: El ciclo PDCA consiste en la secuencia encadenada de planificar, hacer, medir y actuar para mejorar, es muy conocido en el mundo de la calidad, fue explicado con cierto detalle por Shewhart en la segunda década del siglo pasado y es universalmente conocido como el ciclo o Rueda de Deming por que fue este autor quien profundizó en él, lo desarrolló y lo dio a conocer de sus escritos en los términos que se conoce hoy [CERVERA02]

Control de acceso: Consiste en controlar quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hace [SEGREDES02]

Política de seguridad de la información:Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión de la seguridad de la información [ISO11]

Bibliografía

[ARTOOL08] AR-TOOLS - Glosario de seguridad informática. AR-TOOLS, 2008

[CERVERA02] CERVERA, Josep. "*La transición a las nuevas ISO 90002000 y su implantación: Un plan sencillo y práctico con ejemplos*", Publicado por Ediciones Díaz de Santos, 2002, pág. 31

[COB07] Instituto de Gobierno de TI. COBIT 4.1. "Marco de Trabajo - Objetivos de control – Directrices Generales – Modelos de Madurez", 2007

[IDALBE05] CHIAVENATO, Idalberto. "Introducción a la Teoría General de la Administración" Séptima edición, McGraw-Hill Interamericana, 2006; Pág. 110

[ISO02] ISO (International Standard Organization).“Published Document PD ISO/IEC guide 73. Risk Management – Vocabulary - Guidelines for use in standards”, 2002.

[ISO05] ISO (International Standard Organization).“Estándar de Seguridad ISO/IEC 27001. Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos", 2005

[ISO08] ISO (International Standard Organization).“Estándar de Seguridad ISO/IEC 27005. Tecnología de la Información – Técnicas de seguridad – Gestión del Riesgo de seguridad de la información", 2008

[ISO11] ISO (International Standard Organization).“*Estándar de Seguridad ISO/IEC 31000. Gestión del riesgo – Principiosdirectrices*", 2011

[NIST02] NIST (National Institute of Standards and Technology).“NIST SP 800-30. Guía de Gestión de riesgo para sistemas de tecnología de la Información – Recomendaciones del Instituto Nacional de Estándares y Tecnología”, 2002

[NTC06] ICONTEC (Instituto Colombiano de Normas Técnicas y Certificación) NTC 5254 - Norma Técnica Colombiana. “Gestión de riesgo”, 2006

[MINIST06_3] Ministerio de administraciones públicas, "MAGERIT - Metodología de análisis y gestión de riesgos de los sistemas de información" – Guía de Técnicas. Versión 2, España, 2006

[MINIST06] Ministerio de administraciones públicas, "MAGERIT - Metodología de análisis y gestión de riesgos de los sistemas de información" – Método. Versión 2, España, 2006

[SEGREDES02] "*Manual de Seguridad en Redes*". Equipo de Seguridad en Redes. 2002; pág.24

Referencia electrónicas

[1] IS & BCA. "*Cambios en la nueva versión de ISO 27001:2013"*. {En línea} {13 de abril de 2014}. Disponible en: (http://blog.iso27001standard.com/wp-content/uploads/2013/10/Infographic_New_ISO_27001_2013_Revision2-450x2025.jpg)

[2] welivesecurity. "*Los renovados anexos de ISO/IEC 27001:2013*" {En línea} {13 de abril de 2014}. Disponible en: (http://www.welivesecurity.com/la-es/2013/10/18/renovados-anexos-iso-iec-27001-2013/)

Anexos

Anexo 1: Diagrama de red a alto nivel

El detalle del diagrama de red no puede ser entregado por solicitud de la empresa en estudio. Se presenta el siguiente diagrama general: