DISEÑO E IMPLEMENTACIÓN DE UN SGSI PARA EL ÁREA DE INFORMÁTICA DE LA CURADURÍA URBANA SEGUNDA DE PASTO BAJO LA NORMA ISO/IEC 27001

ALBA ELISA CÓRDOBA SUÁREZ

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA "UNAD"
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO, COLOMBIA
2015

DISEÑO E IMPLEMENTACIÓN DE UN SGSI PARA EL ÁREA DE INFORMÁTICA DE LA CURADURÍA URBANA SEGUNDA DE PASTO BAJO LA NORMA ISO/IEC 27001

ALBA ELISA CORDOBA SUAREZ

Proyecto de Grado para optar al título de:
Especialista en Seguridad Informática

Director de Proyecto
Ingeniero de Sistemas, Especialista en Seguridad Informática
Martin Cancelado
Tutor UNAD

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA "UNAD"
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO, COLOMBIA
2015

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

San Juan de Pasto, Mayo de 2015

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

El gobierno nacional dispone mediante leyes y decretos que en las ciudades para el desarrollo urbano sean las curadurías urbanas o la oficina de planeación municipal las encargadas de otorgar licencias urbanísticas en todas sus modalidades.

Por lo tanto el Curador Urbano es un particular con función pública encargado de estudiar, tramitar y expedir licencias urbanísticas a todos los interesados que presenten solicitud de obtención de licencia. Su función es verificar el cumplimiento de las normas urbanísticas y de edificaciones vigentes, con autonomía en el ejercicio de sus funciones y responsable conforme a la ley.

Este proyecto se lleva a cabo para la Curaduría Urbana Segunda de Pasto la cual pretende cada día implementar políticas y controles de seguridad para proteger la información; mejorar la atención a sus clientes, brindándoles eficiencia y calidad en la prestación de su servicio y asegurar la continuidad del negocio.

Este trabajo tiene como objetivo fundamental, diseñar un SGSI para el área de informática de la Curaduría Urbana Segunda de Pasto bajo la Norma ISO/IEC 27001 con el fin de clasificar la información, identificar vulnerabilidades y amenazas en el área de informática; valorar los riesgos y con base en estos definir controles y políticas de seguridad que deben ser de conocimiento de la empresa, instrucciones de los procedimientos a realizarse y la documentación que se debe desarrollar en todo el proceso para la posterior implementación del SGSI, aplicando el modelo PHVA (Planificar, hacer, verificar y actuar).

Como primera medida se recolecta información de la curaduría a través de la observación, la técnica de la encuesta y una prueba de tráfico de red que permiten tener una idea general del manejo de la seguridad en la organización.

Seguidamente se realiza un análisis de riesgos paso a paso desarrollando el inventario de activos, la valoración cualitativa de los activos, identificación de amenazas, identificación de salvaguardas para los activos, valoración y evaluación del riesgo y el informe de calificación del riesgo, que permiten identificar los riesgos más apremiantes a los que está expuesta la empresa.

Posteriormente se definen las políticas y controles de seguridad, que tienen como finalidad contribuir a la disminución de riesgos de los elementos del área de informática y fortalecer la seguridad con medidas que se ven reflejadas en la empresa y a sus clientes en la prestación de un servicio ágil, eficiente, eficaz y con calidad. Finalmente se realiza la primera fase de la implementación que es el plan de gestión del riesgo donde se concreta de forma clara cómo se va a actuar en el control de los riesgos, se identifica los controles seleccionados, los responsables y el tiempo. Listo para ser adoptado por la Curaduría Segunda cuando el Curador lo desee.

ABSTRACT

The national government has through laws and decrees that in cities for urban development are the urban curator or the municipal planning office responsible for granting planning permission in all its forms.

Therefore the Urban Curator is a particular public service in charge of studying, processing and issue planning permission for all interested parties to submit application for licensing. It will check compliance with planning regulations and existing buildings, with autonomy in the exercise of their duties and accountable under the law.

This project is carried out for the urban curator Second Pasto which seeks every day to implement policies and security controls to protect information; improve service to its customers, providing efficiency and quality in the provision of service and ensure business continuity.

This work has as main objective, to design an ISMS for the computer field of urban curator Second Pasto under ISO / IEC 27001 standard in order to classify information, identify threats and vulnerabilities in the computer field; assess the risks and based on these controls and define security policies that should be known to the company, instructions for procedures to be performed and the documentation that must be developed throughout the process for the subsequent implementation of the ISMS, using the model PDCA (plan, do, check and act).

As a first step curated information through observation, survey technique and test network traffic that provide a general idea of the management of security in the organization is collected.

Following a risk analysis step by step developing the asset inventory, qualitative valuation of assets, identifying threats, safeguards for identifying assets, valuation and risk assessment and risk rating report that identify performed the most pressing risks to which the company is exposed.

Subsequently policies and security checks, which aim to contribute to the reduction of risks of the elements of informatics and strengthen security measures that are reflected in the company and its customers in providing an agile defined , efficient, effective and quality.

Finally, the first phase of implementation is the risk management plan where concrete clearly how it will act in the control of risks, selected controls are identified, those responsible and the time is done. Ready to be adopted by the Second Curator Curator when desired

GLOSARIO

Amenaza. Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

Confidencialidad: La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

Contraseñas: Una contraseña o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se les permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

Datos: El dato es una representación simbólica (numérica, alfabética, algorítmica, etc.) de un atributo o variable cuantitativa. Los datos describen hechos empíricos, sucesos y entidades. Es un valor o referente que recibe el computador por diferentes medios, los datos representan la información que el programador manipula en la construcción de una solución o en el desarrollo de un algoritmo.

Debilidad: Las debilidades se refieren a todos aquellos elementos, recursos, habilidades y actitudes que la empresa ya tiene y que constituyen barreras para lograr la buena marcha de la organización. (en este caso un sistema).

Disponibilidad: La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

Fallos: Es un estado o situación en la que se encuentra un sistema formado por dispositivos, equipos, aparatos y/o personas en el momento que deja de cumplir la función para el cual había sido diseñado.” Hay que evitar ésta situación siempre que queramos diseñar un sistema altamente fiable, competitivo y fuerte. Para ello hay que adelantarse a dicho estado o situación mediante métodos matemáticos y científicos.

Integridad: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) A groso modo, la integridad es el mantener con exactitud la información tal

cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

ISO/IEC 27000: Publicada el 1 de Mayo de 2009, revisada con una segunda edición de 01 de Diciembre de 2012 y una tercera edición de 14 de Enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua).

ISO/IEC 27001: Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones.

Política de seguridad: Toda intención y directriz expresada formalmente por la Dirección, Su objetivo es proporcionar a la gerencia la dirección y soporte para la seguridad de la información, en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes. Esto por supuesto debe ser creado de forma particular por cada organización. Se debe redactar un "Documento de la política de seguridad de la información".

Procedimientos: Es un conjunto de acciones u operaciones que tienen que realizarse de la misma forma, para obtener siempre el mismo resultado bajo las mismas circunstancias (por ejemplo, procedimiento de emergencia).

Recursos: Un recurso es una fuente o suministro del cual se produce un beneficio

Riesgo. Combinación de la probabilidad de un evento y sus consecuencias

Sistema de detección de intrusos: (o **IDS** de sus siglas en inglés *Intrusion Detection System*) es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos crackers, o de Script Kiddies que usan herramientas automáticas.

SGSI: Es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Información Security Management System.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

Vulnerabilidad. Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

INTRODUCCIÓN

En la actualidad la información se ha denominado dentro de una empresa como uno de los activos más importantes, de allí la necesidad de proteger la información de los diferentes riesgos a los que se encuentra expuesta.

El estar a la vanguardia de la tecnología, el compartir información a diario a través de los diferentes sistemas tecnológicos y electrónicos es una necesidad pero también convierte la información en una activo vulnerable por lo tanto cada organización asume el reto de proteger su activo más preciado.

La implementación de un SGSI es una opción fundamental cuando se trata de proteger la información, ya que este tiene como objetivo esencial proteger dicho activo a través de controles y políticas de seguridad que deben ser aplicadas en una organización en cabeza de la gerencia.

La curaduría urbana segunda de Pasto, a través del diseño e implementación de un SGSI busca minimizar los riesgos a los que se encuentra expuesta la información de la organización desarrollo que se documenta paso a paso.

Para el desarrollo de la primera fase se aplica la metodología Magerit con la cual se realiza el análisis de riesgos que es uno de los procesos más importantes que se debe realizar dentro de la empresa ya que permite identificar y analizar cada uno de los procesos y determinar los riesgos a los cuales esta expuestos cada uno de ellos. Además permite identificar amenazas y vulnerabilidades.

Para el análisis de riesgos se realiza un inventario de activos, valoración cualitativa de dichos activos, identificación de amenazas, definición de salvaguardas. Una vez realizado este procesos y analizado las pruebas realizadas a la red de la Curaduría con herramientas de análisis de trafico de red se procede a realizar una evaluación de los riesgos el cual permite determinar que activos se encuentran en peligro.

Una vez identificado claramente los activos que se encuentran en riesgo y que generarían mayor impacto en caso de sufrir un ataque, se procede a definir políticas de seguridad, la declaración y aplicabilidad de los controles y el plan de gestión del riesgo, para cada uno de estos activos teniendo en cuenta lo expuesto por la Norma ISO/IEC 27002. Dichas políticas y controles deben ser implementadas en la organización por parte de la gerencia, en este caso por Curador urbano junto al comité de seguridad para cumplir el objetivo fundamental del SGSI que es proteger la información y disminuir los riesgos, garantizando la continuidad del negocio.

1. ELEMENTOS DE IDENTIFICACIÓN

1.1 TEMA

Dentro de las líneas de investigación de la UNAD el proyecto de grado está enfocado hacia la seguridad informática, la gestión e implementación de políticas de seguridad, el buen uso de los recursos informáticos que involucran la parte administrativa y operativa de la empresa, especialmente en:

- Medidas de seguridad lógicas con respecto a los equipos y a los usuarios
- Prevención de amenazas y riesgos.
- Diseño e implementación de políticas de seguridad
- Uso adecuado de archivos y recursos
- Medidas de seguridad física y controles de acceso
- Herramientas y prácticas de seguridad
- Implantación de un SGSI que ofrece seguridad y protección en la información para el Registros de proyectos, Control de proyectos, reportes, consultas etc.

1.2 TÍTULO

Diseño e implementación de un SGSI para el área de informática de la Curaduría Urbana Segunda de Pasto bajo la Norma ISO/IEC 27001

1.3 LÍNEA DE INVESTIGACIÓN

La propuesta presentada se enmarca dentro de la línea de investigación de gestión de sistemas específicamente dentro de la auditoría de sistemas que hacen referencia a:

1.3.1 Gestión de sistemas: Se ocupa de integrar, planificar y controlar los aspectos técnicos, humanos, organizativos, comerciales y sociales del proceso completo empezando con el análisis del dominio del problema, continuando con el diseño de alternativas de solución y finalizando con la operatividad de un sistema. La gestión de sistema incluye también procesos que abarcan la planificación de actividades, metas, responsables, indicadores de eficiencia eficacia y efectividad.

1.3.2 Auditoría de sistemas: Incluye control de información, calidad de procesos, seguridad informática, que son vitales para asegurar la validez y veracidad de la información.

1.4 PLANTEAMIENTO DEL PROBLEMA.

1.4.1 Descripción del problema. La Curaduría Urbana Segunda de Pasto es una entidad privada con función pública que se encarga de tramitar y aprobar solicitudes de licencias urbanísticas en el municipio de Pasto, actualmente maneja un volumen considerablemente alto de información, cuenta con una base de datos que alberga aproximadamente de 15.000 registros de proyectos urbanísticos aprobados y en trámite, en cada registro se almacenan los datos de cada proyecto como numero catastral, matricula inmobiliaria, dirección, barrio, estrato etc.

La Curaduría funciona en el segundo piso de un edificio, cuenta con 5 oficinas con 10 estaciones de trabajo conectadas a través de una red inalámbrica. Los archivos de licencias urbanísticas, recursos, memorandos, descripciones, oficios, reportes, informes y la base de datos pueden ser accedidos, consultados y modificados por todos los empleados de la Curaduría desde su estación de trabajo, estos cuentan con privilegios para instalar, descargar software, navegar en internet, y pueden acceder a sus correos electrónicos, además pueden utilizar memorias usb, copiar cd, acceder a redes sociales teniendo a su disposición toda la información histórica y actual de la Curaduría Urbana Segunda de Pasto etc. donde es evidente la inseguridad a la que está expuesta la información.

1.4.2 Formulación del problema. ¿Cómo proteger de manera efectiva la información relacionada con licencias y proyectos urbanísticos en trámite en la curaduría urbana segunda de Pasto?

1.5 OBJETIVOS

1.5.1 Objetivo general. Diseñar e implementar un sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001 en la curaduría urbana segunda de Pasto para el área de informática, que permita establecer políticas de seguridad y disminuir el riesgo de la información ante un eventual ataque.

1.5.2 Objetivos específicos

- Identificar riesgos de seguridad en el área de informática a los que está expuesta la Curaduría Urbana Segunda de Pasto.
- Describir los principales problemas de seguridad que presenta la entidad en el área de informática.
- Definir las medidas de seguridad más apropiadas a aplicarse en este caso.

- Definir políticas de seguridad encaminadas a minimizar los riesgos a los que está expuesta la información.

- Plantear un SGSI para el área de informática bajo la norma ISO/IEC 27001 para la Curaduría Urbana Segunda de Pasto que permita obtener confidencialidad, integridad y disponibilidad de la información.

- Implementar un SGSI para el área de informática que permita proteger los recursos informáticos más valiosos para la CU como la información, el hardware y el software.

1.6 JUSTIFICACIÓN

Proteger la información de una empresa consiste en poner barreras de protección para bloquear posibles ataques, es necesario proteger todos los medios de acceso a la empresa debido a que las últimas décadas el uso del internet y los sistemas de información es más común lo que convierte a una empresa en vulnerable frente a los atacantes.

La Curaduría Urbana Segunda de Pasto como cualquier empresa exitosa busca mejorar día a día prestando un mejor servicio a todo el municipio de Pasto adoptando herramientas de optimización, basadas en nuevas tecnologías y estableciendo políticas de seguridad de la información a fin de alcanzar el éxito a corto, mediano y largo plazo, con el propósito de establecerse metas, que permitan aumentar las ganancias y aporten al desarrollo social con la participación y colaboración tanto de directivos como de empleados.

La información se ha denominado como uno de los activos más valiosos en una empresa por lo tanto definir políticas de seguridad en el manejo de la información y en el uso de herramientas tecnológicas es vital, porque permite evitar problemas e incidentes que afectan el buen funcionamiento de la empresa.

Por lo tanto se hace un análisis general de los principales objetivos y necesidades más apremiantes que se tienen en este momento, donde es evidente que carece de políticas de seguridad para la protección de la información a nivel general.

Hasta el momento no se han presentado dificultades referentes a ataques, pero el riesgo es inminente y estas falencias pueden traer inconvenientes desastrosos, puesto que la Curaduría es una empresa con función pública que se encarga de expedir licencias Urbanísticas para todo el municipio de Pasto, se puede decir que la información puede ser robada, manipulada, o modificada para fines delictivos.

Por lo anteriormente expuesto es de suma importancia el diseño de un SGSI para el área de informática bajo la norma ISO/IEC 27001 que permita obtener una visión global del estado de los sistemas de información y observar claramente las medidas de seguridad a aplicar para prevenir futuros incidentes.

1.7 DELIMITACIÓN

El proceso se viene adelantando desde hace nueve (9) meses y se pretende terminar en un período de (2) dos meses.

Para optar por el título de Especialista en Informática, se hace el diseño e implementación de un SGSI para el área de Informática de la Curaduría Urbana Segunda de Pasto bajo la Norma ISO/IEC 27001, realizando un inventario de los activos, identificando riesgos e implementado políticas de seguridad que deben ser aplicadas por los empleados de esta organización para mejorar la seguridad de información sensible como lo es el registro y control de proyectos urbanísticos.

Este proyecto se realizará en San Juan de Pasto (Nariño – Colombia), y está dirigido a curaduría urbana segunda de Pasto, ubicada en la Calle 18 # 19-95 barrio, el Centro.

1.8 ALCANCES

Este proyecto puede adaptarse a empresas de la misma naturaleza prestadoras de servicios como la curaduría urbana primera de Pasto y curadurías de otras ciudades, atendiendo a nuevos requerimientos.

2. MARCO REFERENCIAL

Para desarrollar el presente proyecto es importante conocer conceptos que están relacionados directamente con el tema, tener un soporte teórico que permita clarificar definiciones con la finalidad de dar respuesta a los requerimientos del proyecto; cada uno de los procesos en el desarrollo del proyecto significa la búsqueda de resultados y está acompañada de una buena investigación necesaria para alcanzar los objetivos propuestos

2.1 MARCO TEÓRICO

2.1.1 Sistema de Gestión de la Seguridad de la Información SGSI

2.1.1.1 ¿Qué es un SGSI?: SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Información Security Management System.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la

organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI[1].

Figura 1. SGSI

Fuente: www.iso27000.es

2.1.1.2 ¿Para qué sirve un SGSI? La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

[1] [1] ISO 27001. (2005). El portal de ISO 27001 en Español. Obtenido de http://www.iso27000.es/iso27000.html

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones[2].

Figura 2. Utilidad de un SGSI

Fuente: www.iso27000.es

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

[2] IBID., ISO 27001.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

2.1.1.3 ¿Qué incluye un SGSI?. En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma[3]:

Figura 3. Qué incluye un SGSI

Fuente: www.iso27000.es

Documentos de Nivel 1:

Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

Documentos de Nivel 2:

Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

Documentos de Nivel 3:

Instrucciones, *checklists* y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

[3] IBID., ISO 27001.

Documentos de Nivel 4

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como *output* que demuestra que se ha cumplido lo indicado en los mismos.

De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

Alcance del SGSI: Ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas)[4].

Política y objetivos de seguridad: Documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Procedimientos y mecanismos de control que soportan al SGSI: Aquellos procedimientos que regulan el propio funcionamiento del SGSI.

Enfoque de evaluación de riesgos: Descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables .

Informe de evaluación de riesgos: Estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

Plan de tratamiento de riesgos: Documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

Procedimientos documentados: Todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

Registros: Documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

Declaración de aplicabilidad: (SOA -*Statement of Applicability*-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el

[4] IBID., ISO 27001.

SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

Control de la documentación

Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

- Aprobar documentos apropiados antes de su emisión[5].
- Revisar y actualizar documentos cuando sea necesario y renovar su validez
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponible en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos.
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

2.1.1.4 ¿Cómo implementar un SGSI?. Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

Figura 4. Ciclo PDCA

Fuente: www.iso27000.es

[5] IBID., ISO 27001.

- **Plan (planificar):** establecer el SGSI.
- **Do (hacer):** implementar y utilizar el SGSI.
- **Check (verificar):** monitorizar y revisar el SGSI.
- **Act (actuar):** mantener y mejorar el SGSI[6].

2.1.1.4.1 Plan: Establecer el SGSI

- Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
- Definir una política de seguridad que: Incluya el marco general y los objetivos de seguridad de la información de la organización; considere requerimientos legales o contractuales relativos a la seguridad de la información; esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI; establezca los criterios con los que se va a evaluar el riesgo; esté aprobada por la dirección.
- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia).
- Identificar los riesgos: Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios; identificar las amenazas en relación a los activos; identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas; identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.
- Analizar y evaluar los riesgos: Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información; evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados; estimar los niveles de riesgo; determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.
- Identificar y evaluar las distintas opciones de tratamiento de los riesgos para: Aplicar controles adecuados; aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos; evitar el riesgo, p. ej., mediante el cese de las actividades que lo

[6] IBID., ISO 27001.

originan; transferir el riesgo a terceros, p. ej., compañías aseguradoras o proveedores de *outsourcing*[7].

Figura 5. Gestión de Riesgos[8]

Fuente: www.iso27000.es

- Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.
- Definir una declaración de aplicabilidad que incluya: Los objetivos de control y controles seleccionados y los motivos para su elección; los objetivos de control y controles que actualmente ya están implantados; los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

En relación a los controles de seguridad, el estándar ISO 27002 (antigua ISO 17799) proporciona una completa guía de implantación que contiene 133 controles, según 39 objetivos de control agrupados en 11 dominios. Esta norma es

[7] IBID., ISO 27001.

[8] ISO / IEC 2700 (2009) Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la Información – Medición. Obtenido de http://www.iso27001security.com/html/27004.html

referenciada en ISO 27001, en su segunda cláusula, en términos de “documento indispensable para la aplicación de este documento” y deja abierta la posibilidad de incluir controles adicionales en el caso de que la guía no contemplase todas las necesidades particulares.

2.1.1.4.2 Do: Implementar y utilizar el SGSI

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información[9].

- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

2.1.1.4.3 Check: Monitorizar y revisar el SGSI

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para: Detectar a tiempo los errores en los resultados generados por el procesamiento de la información; identificar brechas e incidentes de seguridad; ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto; detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores; determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.
- Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad,

[9] IBID., ISO 27001.

incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.
- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.
- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

2.1.1.4.4 Act: Mantener y mejorar el SGSI

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.
- PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de *Plan* para iniciar un nuevo ciclo de las cuatro fases. Téngase en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, p. ej., puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

2.1.1.5 ¿Qué tareas tiene la gerencia en un SGSI?[10]. Uno de los componentes primordiales en la implantación exitosa de un Sistema de Gestión de Seguridad de la Información es la implicación de la dirección. No se trata de una expresión retórica, sino que debe asumirse desde un principio que un SGSI afecta fundamentalmente a la gestión del negocio y requiere, por tanto, de decisiones y acciones que sólo puede tomar la gerencia de la organización. No se debe caer en el error de considerar un SGSI una mera cuestión técnica o tecnológica relegada a niveles inferiores del organigrama; se están gestionando riesgos e impactos de negocio que son responsabilidad y decisión de la dirección.

El término Dirección debe contemplarse siempre desde el punto de vista del alcance del SGSI. Es decir, se refiere al nivel más alto de gerencia de la parte de la organización afectada por el SGSI (recuérdese que el alcance no tiene por qué ser toda la organización).
Algunas de las tareas fundamentales del SGSI que ISO 27001 asigna a la dirección se detallan en los siguientes puntos:

2.1.1.5.1 Compromiso de la dirección. La dirección de la organización debe comprometerse con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. Para ello, debe tomar las siguientes iniciativas:

- Establecer una política de seguridad de la información.
- Asegurarse de que se establecen objetivos y planes del SGSI.
- Establecer roles y responsabilidades de seguridad de la información.
- Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.
- Asignar suficientes recursos al SGSI en todas sus fases.
- Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.
- Asegurar que se realizan auditorías internas.
- Realizar revisiones del SGSI, como se detalla más adelante.

2.1.1.5.2 Asignación de Recursos. Para el correcto desarrollo de todas las actividades relacionadas con el SGSI, es imprescindible la asignación de recursos. Es responsabilidad de la dirección garantizar que se asignan los suficientes para:

- Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI.
- Garantizar que los procedimientos de seguridad de la información apoyan los requerimientos de negocio.

[10] IBID., ISO 27001.

- Identificar y tratar todos los requerimientos legales y normativos, así como las obligaciones contractuales de seguridad.
- Aplicar correctamente todos los controles implementados, manteniendo de esa forma la seguridad adecuada.
- Realizar revisiones cuando sea necesario y actuar adecuadamente según los resultados de las mismas.
- Mejorar la eficacia del SGSI donde sea necesario.

2.1.1.5.3 Formación y concienciación[11]. La formación y la concienciación en seguridad de la información son elementos básicos para el éxito de un SGSI. Por ello, la dirección debe asegurar que todo el personal de la organización al que se le asignen responsabilidades definidas en el SGSI esté suficientemente capacitado. Se deberá:

- Determinar las competencias necesarias para el personal que realiza tareas en aplicación del SGSI.
- Satisfacer dichas necesidades por medio de formación o de otras acciones como, p. ej., contratación de personal ya formado.
- Evaluar la eficacia de las acciones realizadas.
- Mantener registros de estudios, formación, habilidades, experiencia y cualificación.

Además, la dirección debe asegurar que todo el personal relevante esté concienciado de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del SGSI.

2.1.1.5.4 Revisión del SGSI. La dirección de la organización se le asigna también la tarea de, al menos una vez al año, revisar el SGSI, para asegurar que continúe siendo adecuado y eficaz. Para ello, debe recibir una serie de informaciones, que le ayuden a tomar decisiones, entre las que se pueden enumerar:

- Resultados de auditorías y revisiones del SGSI.
- Observaciones de todas las partes interesadas.
- Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.
- Información sobre el estado de acciones preventivas y correctivas.
- Vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.
- Resultados de las mediciones de eficacia.
- Estado de las acciones iniciadas a raíz de revisiones anteriores de la dirección.
- Cualquier cambio que pueda afectar al SGSI.

[11] IBID., ISO 27001.

- Recomendaciones de mejora.

Basándose en todas estas informaciones, la dirección debe revisar el SGSI y tomar decisiones y acciones relativas a:

- Mejora de la eficacia del SGSI.
- Actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.
- Modificación de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.
- Necesidades de recursos.
- Mejora de la forma de medir la efectividad de los controles[12].

2.1.2 Conceptos Básicos

2.1.2.1 ¿Qué es la seguridad de la información?. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada. Esto es especialmente importante en el entorno de negocios cada vez más interconectado. Como resultado de esta interconexión creciente, la información se expone a un gran número y variedad de amenazas y vulnerabilidades (véase también OECD Guía para la seguridad redes sistemas de información).

La información puede existir en diversas formas. Se puede imprimir o escribir en papel, almacenar electrónicamente, transmitir por correo o por medios electrónicos, presentar en películas, o expresarse en la conversación. Cualquiera sea su forma o medio por el cual se comparte o almacena, siempre debería tener protección adecuada.

La seguridad de la información es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo para el negocio y maximizar el retorno de inversiones y oportunidades de negocio.

La seguridad de la información se logra implementando un conjunto apropiado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Los controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados, donde sea necesario, para asegurar que se cumplen los objetivos específicos de seguridad y

[12] IBID., ISO 27001.

del negocio de la organización. Esto debería hacerse en conjunto con otros procesos de gestión de negocio.

2.1.2.2 ¿Por qué es necesaria la seguridad de la información?. La seguridad de la información es importante tanto para los negocios del sector público como del privado y para proteger la infraestructura critica. En ambos sectores, la seguridad de la información actuara como un elemento facilitador para lograr, por ejemplo, gobierno en línea (e government) o negocios electrónicos (e-Business) y evitar o reducir los riesgos pertinentes. La interconexión de las redes públicas y privadas y compartir los recursos de información incrementan la dificultad para lograr el control del acceso. La tendencia hacia la computación distribuida también ha debilitado la eficacia del control central y especializado.

Muchos sistemas de información no se han diseñado para ser seguros. La seguridad que se puede lograr a través de los medios técnicos es limitada y debería estar soportada por una buena gestión y por procedimientos apropiados. La identificación de los controles que se deberían establecer requiere planificación y atención cuidadosa a los detalles. La gestión de la seguridad de la información requiere, como mínimo, la participación de todos los empleados de la organización[13].

También puede requerir la participación de accionistas, proveedores, terceras partes, clientes u otras partes externas. De igual modo puede ser necesaria la asesoría especializada de organizaciones externas.

2.1.2.3 ¿Cómo establecer los requisitos de seguridad? Es esencial que la organización identifique sus requisitos de seguridad. Existen tres fuentes principales de requisitos de seguridad:

- Una fuente se deriva de la evaluación de los riesgos para la organización, teniendo en cuenta la estrategia y los objetivos globales del negocio. A través de la evaluación de riesgos, se identifican las amenazas para los activos, se evalúan la vulnerabilidad y la probabilidad de ocurrencia y se estima el impacto potencial.
- Otra fuente son los requisitos legales, estatutarios, reglamentarios y contractuales que debe cumplir la organización, sus socios comerciales, los contratistas y los proveedores de servicios, así como su entorno socio-cultural.
- Una fuente adicional es el conjunto particular de principios, objetivos y requisitos del negocio para el procesamiento de la información que la organización ha desarrollado para apoyar sus operaciones.

[13] IBID., ISO 27001.

2.1.2.4 Confidencialidad: La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

2.1.2.5 Integridad: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) A groso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

2.1.2.6 Disponibilidad: La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

2.1.2.7 Evaluación de los riesgos de seguridad: La reducción de riesgos no puede ser un proceso arbitrario y regido por la voluntad de los dueños o administradores de la empresa, sino que además de seguir medidas adecuadas y eficientes, se deben tener en cuenta los requerimientos y restricciones de la legislación y las regulaciones nacionales e internacionales, objetivos organizacionales, bienestar de clientes y trabajadores, costos de implementación y operación (pues existen medidas de seguridad de gran calidad pero excesivamente caras, tanto que es más cara la seguridad que la propia ganancia de una empresa, afectando la rentabilidad)[14].

Se debe saber que ningún conjunto de controles puede lograr la seguridad completa, pero que sí es posible reducir al máximo los riesgos que amenacen con afectar la seguridad en una organización.

2.1.2.8 Evento de seguridad de la información. Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

2.1.2.9 Incidente de seguridad de la información. Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

[14] IBID., ISO 27001.

2.1.2.10 Política de seguridad: Toda intención y directriz expresada formalmente por la Dirección, Su objetivo es proporcionar a la gerencia la dirección y soporte para la seguridad de la información, en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes. Esto por supuesto debe ser creado de forma particular por cada organización. Se debe redactar un "Documento de la política de seguridad de la información".

2.1.2.11 Riesgo. Combinación de la probabilidad de un evento y sus consecuencias

2.1.2.12 Análisis de riesgos. Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

2.1.2.13 Evaluación de riesgos. Todo proceso de análisis y valoración del riesgo.

2.1.2.14 Valoración del riesgo. Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.

2.1.2.15 Gestión del riesgo. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

2.1.2.16 Amenaza. Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

2.1.2.17 Vulnerabilidad. Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

2.1.3 Sobre la Norma ISO/IEC 27000

2.1.3.1 ISO/IEC 27000[15]: Publicada el 1 de Mayo de 2009, revisada con una segunda edición de 01 de Diciembre de 2012 y una tercera edición de 14 de Enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua).

2.1.3.2 ISO/IEC 27001: Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del

[15] IBID., ISO 27001.

sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones.

2.1.3.3 ISO/IEC 27002: Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005.

2.1.3.4 ISO/IEC 27003: Publicada el 01 de Febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.

2.1.3.5 ISO/IEC 27004: Publicada el 15 de Diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

2.1.3.6 ISO/IEC 27005: Publicada en segunda edición el 1 de Junio de 2011 (primera edición del 15 de Junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Su primera publicación revisó y retiró las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000[16].

2.1.3.7 ISO/IEC 27006: Publicada en segunda edición el 1 de Diciembre de 2011 (primera edición del 1 de Marzo de 2007). Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001:2005 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

[16] IBID., ISO 27001.

2.1.3.8 ISO/IEC 27007: Publica da el 14 de Noviembre de 2011. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011. En España, esta norma no está traducida.

2.1.3.9 ISO/IEC TR 27008: Publicada el 15 de Octubre de 2011. No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI. En España, esta norma no está traducida.

2.1.4 Conceptos sobre Curadurías

2.1.4.1 Que son las curadurías urbanas: Son oficinas independientes de la Administración Municipal, que operan bajo la responsabilidad de particulares llamados Curadores Urbanos y en las cuales los interesados deben realizar los trámites relacionados con la obtención de licencias urbanísticas y reconocimientos de edificaciones y otras actividades complementarias a éstas.

2.1.4.2 Qué es el curador urbano: El Curador Urbano es un particular con funciones públicas; encargado de estudiar, tramitar y expedir licencias de parcelación, urbanización, construcción, y subdivisión de predios, a petición del interesado en adelantar proyectos de esta índole en las distintas zonas de la ciudad que la administración municipal le haya determinado como su jurisdicción.
Igualmente, resolverán las solicitudes de prorroga y modificación de dichas licencias así como otras actuaciones como aprobación de los planos de propiedad horizontal y movimiento de tierras. El Curador Urbano ejerce una función pública para la verificación del cumplimiento de las normas urbanísticas y de edificaciones vigentes y es autónomo en el ejercicio de sus funciones y responsable conforme a la Ley[17].

2.1.4.3 Quién designa al curador urbano: El alcalde municipal designa a los Curadores Urbanos para períodos individuales de cinco (5) años, previo concurso de méritos y puede ser designado previa evaluación de su desempeño.

2.1.4.4 Qué es una licencia urbanística: Es la autorización previa, expedida por el cual el Curador Urbano a solicitud del interesado para adelantar obras de urbanización, parcelación, loteo o subdivisión de predios; de construcción, ampliación, adecuación, reforzamiento estructural, modificación y demolición de edificaciones.

2.1.4.5 Qué es una licencia de urbanización: Es la autorización previa para ejecutar en uno o varios predios localizados en suelo urbano, la creación de espacios públicos y privados y la construcción de las obras de infraestructura que permitan la adecuación y dotación de estos terrenos para la futura construcción de

[17] Decreto1469. (2010). Ministerio de Vivienda Ciudad y Territorio. Obtenido de http://www.minvivienda.gov.co.

edificaciones con destino a usos urbanos acordes con el plan de ordenamiento territorial del municipio.

2.1.4.6 Qué es una licencia de parcelación: Es la autorización previa para ejecutar en uno o varios predios localizados en suelo rural y suburbano, la creación de espacios públicos y privados y la ejecución de obras para vías e infraestructura que garanticen la autoprestación de los servicios domiciliarios que permitan destinar los predios resultantes a los usos permitidos por el plan de ordenamiento territorial del municipio y la normatividad agraria y ambiental aplicable**.**

2.1.4.7 Qué es una licencia de subdivisión: Es la autorización previa para dividir uno o varios predios localizados en suelo rural, urbano o de expansión de conformidad con el plan de ordenamiento territorial del municipio. Son modalidades de la Licencia de Subdivisión en suelo rural y de expansión; la Subdivisión Rural y en suelo urbano; la Subdivisión Urbana y Reloteo. La Licencia de Subdivisión no implica autorización alguna para urbanizar, parcelar, o construir sobre los lotes resultantes, para cuyo efecto, en todos los casos, deberá adelantar el trámite de solicitud de licencia de parcelación, urbanización o construcción.

2.1.4.8 Qué es una licencia de construcción: Es la autorización previa para desarrollar edificaciones en uno o varios predios de conformidad con el plan de ordenamiento territorial del municipio. Son modalidades de la licencia de construcción las autorizaciones para Obra nueva, Ampliación, Adecuación, Modificación, Restauración, Reforzamiento estructural, Demolición y Cerramiento.

2.1.4.9 Cuál es el término de tiempo que tiene un curador urbano para expedir una licencia: Cuarenta y cinco (45) días hábiles. Este plazo podrá prorrogarse hasta en la mitad del mismo[18].

2.1.4.10 Quienes pueden solicitar una licencia urbanística: Los titulares de derechos reales principales, los propietarios del derecho de dominio a título de fiducia y los fideicomitentes de las mismas fiducias, de los inmuebles objeto de la solicitud. Los poseedores solo podrán ser titulares de las licencias de construcción.

2.1.4.11 Que documentos se deben adjuntar para obtener una licencia urbanística. Toda solicitud de licencia debe acompañarse de los siguientes documentos:

- Formulario único nacional de solicitud de licencia, completamente diligenciado.
- Copia del certificado de libertad y tradición del inmueble o inmuebles objeto de la solicitud, cuya fecha de expedición no sea superior a un (1) mes antes de la fecha de solicitud.

[18] IBID., Decreto1469.

- Plano de localización e identificación del predio o predios objeto de la solicitud, mediante carta catastral del Codazzi – IGAC.
- Certificado de demarcación urbanística y arquitectónica de la oficina de Planeación Municipal.
- Copia del documento que acredite el pago o declaración privada con pago del impuesto predial de los últimos cinco (5) años, donde figure la nomenclatura alfanumérica o identificación del predio.
- Si el solicitante de la licencia fuera una persona jurídica, deberá acreditarse la existencia y representación de la misma mediante el documento legal idóneo, cuya fecha de expedición no sea superior a un (1) mes.
- Poder debidamente otorgado, cuando se actúe mediante apoderado.
- La relación de la dirección de los vecinos de los predios colindantes objeto de la solicitud y si fuere posible el nombre de ellos.
- La manifestación bajo la gravedad del juramento de si el proyecto sometido a consideración se destinará o no a vivienda de interés social, de lo cual se dejará constancia en el acto que resuelva la solicitud de licencia.
- Los documentos o planos que el proyecto requiera en forma específica.

2.1.4.12 Cuál es la vigencia y prórroga de una licencia: Las licencias de urbanización, parcelación y construcción tendrán una vigencia máxima de veinticuatro (24) meses, prorrogables por una sola vez por un plazo adicional de doce (12) meses.

Cuando en la misma licencia se conceda licencia de urbanización y construcción, estas tendrán una vigencia máxima de treinta y seis (36) meses prorrogables por un periodo adicional de doce (12) meses.

La prórroga deberá formularse dentro de los treinta (30) días calendario, anteriores al vencimiento de la respectiva licencia, siempre y cuando se haya iniciado la obra[19].

Las licencias de subdivisión tendrán una vigencia improrrogable de seis (6) meses.

Las Licencias de Reconocimiento, cuando fuere necesario adecuar la edificación al cumplimiento de las normas, tendrán un plazo máximo de veinticuatro (24) meses improrrogables, para que el interesado ejecute dichas actuaciones.

2.2. MARCO CONTEXTUAL

La Curaduría Urbana Segunda de Pasto inicia labores el 18 de Julio del 2002 la sede de la curaduría urbana segunda está ubicada en el centro de la ciudad, contigua a la plaza del carnaval y la cultura, en la Calle 18 No 19 – 95 oficina 208, 209, 210, 211, conmutador 7204488 telefax 7330203.

[19] IBID., Decreto1469.

En la actualidad la curaduría segunda de Pasto cuenta con 12 empleados que se encargan de elaborar diferentes trabajos así:

La curaduría cuenta con una recepción encargada de radicación, liquidaciones y atención al público, un área técnica dividida en una parte legal revisada por una abogada con especialización en derecho administrativo, quien es la persona encargada de revisar la legalidad de la documentación recibida; y en cuanto a la parte estructural revisada por un ingeniero especializado en estructuras quien es el encargado de cotejar los planos y memorias a la luz de la Norma de Sismo-resistencia Colombiana NSR 10.

En cuanto a la revisión arquitectónica es realizada por el curador urbano quien al contar con un postgrado en urbanismo se encarga de revisar los planos arquitectónicos y atender consultas en cuanto al cumplimiento del Plan de Ordenamiento Territorial POT.

Por otra parte existen personas que se encargan de realizar la parte operativa como, ingreso de proyectos al sistema actual, comunicación de vecinos, ubicación de proyectos, transcripción de memos, elaboración de licencias, citación de vecinos y organización de archivo.

2.3. MARCO LEGAL

Las Curadurías por ser oficinas independientes de la Administración Municipal, que operan bajo la responsabilidad de particulares llamados Curadores Urbanos que ejercen la función pública están reglamentadas por las siguientes normas y Decretos nacionales y locales.
Normas Nacionales y locales[20]

- Ley 388 del 18 de Julio de 1997 – Ley de ordenamiento territorial
- Decreto 4397-2006 - Modifica Decreto 564/06 y Decreto 96/06
- Decreto 2181_290606- planes parciales
- Ley 810 de 2003 – sanciones urbanísticas
- Ley 675 - propiedad horizontal
- Ley 361 de 1997 - minusválidos
- Decreto1504-1998- espacio público
- Decreto 1538 DE 2005 - accesibilidad
- Decreto 96 2006 - decreto 3600_20-09 de 2007 – suelo rural
- Ley 9 de 1989 – ley de reforma urbana

[20] MINVIVIENDA. (2010). Decreto 1469. Obtenido de http://www.minvivienda.gov.co/Decretos%20Vivienda/1469%20-%202010.pdf#search=1469

- Decreto 975-2004 subsidio de vivienda
- Decreto 1469 de 2010
- Plan de ordenamiento territorial de Pasto – POT.

2.3.1 Normas Nacionales:

2.3.1.1 Ley 388 del 18 de Julio de 1997 – Ley de ordenamiento territorial: "Por la cual se modifica la Ley 9ª de 1989, y la Ley 3ª de 1991 y se dictan otras disposiciones. El Congreso de Colombia.

DECRETA: CAPITULO I Objetivos y principios generales Artículo 1º. Objetivos. La presente ley tiene por objetivos:

1. Armonizar y actualizar las disposiciones contenidas en la Ley 9ª de 1989 con las nuevas normas establecidas en la Constitución Política, la Ley Orgánica del Plan de Desarrollo, la Ley Orgánica de Áreas Metropolitanas y la Ley por la que se crea el Sistema Nacional Ambiental.
2. El establecimiento de los mecanismos que permitan al municipio, en ejercicio de su autonomía, promover el ordenamiento de su territorio, el uso equitativo y racional del suelo, la preservación y defensa del patrimonio ecológico y cultural localizado en su ámbito territorial y la prevención de desastres en asentamientos de alto riesgo, así como la ejecución de acciones urbanísticas eficientes.
3. Garantizar que la utilización del suelo por parte de sus propietarios se ajuste a la función social de la propiedad y permita hacer efectivos los derechos constitucionales a la vivienda y a los servicios públicos domiciliarios, y velar por la creación y la defensa del espacio público, así como por la protección del medio ambiente y la prevención de desastres.
4. Promover la armoniosa concurrencia de la Nación, las entidades territoriales, las autoridades ambientales y las instancias y autoridades administrativas y de planificación, en el cumplimiento de las obligaciones constitucionales y legales que prescriben al Estado el ordenamiento del territorio, para lograr el mejoramiento de la calidad de vida de sus habitantes.

5. Facilitar la ejecución de actuaciones urbanas integrales, en las cuales confluyan en forma coordinada la iniciativa, la organización y la gestión municipales con la política urbana nacional, así como con los esfuerzos y recursos de las entidades encargadas del desarrollo de dicha política[21].

[21] MINVIVIENDA. (1997). Ley 388. Obtenido de http://www.minvivienda.gov.co/LeyesMinvivienda/0388%20-%201997.pdf#search=ley%20388%20de%201997

Artículo 2º. Principios. El ordenamiento del territorio se fundamenta en los siguientes principios:
1. La función social y ecológica de la propiedad.
2. La prevalencia del interés general sobre el particular.
3. La distribución equitativa de las cargas y los beneficios.

Artículo 3º. Función pública del urbanismo. El ordenamiento del territorio constituye en su conjunto una función pública, para el cumplimiento de los siguientes fines:

1. Posibilitar a los habitantes el acceso a las vías públicas, infraestructuras de transporte y demás espacios públicos, y su destinación al uso común, y hacer efectivos los derechos constitucionales de la vivienda y los servicios públicos domiciliarios.
2. Atender los procesos de cambio en el uso del suelo y adecuarlo en aras del interés común, procurando su utilización racional en armonía con la función social de la propiedad a la cual le es inherente una función ecológica, buscando el desarrollo sostenible.
3. Propender por el mejoramiento de la calidad de vida de los habitantes, la distribución equitativa de las oportunidades y los beneficios del desarrollo y la preservación del patrimonio cultural y natural.
4. Mejorar la seguridad de los asentamientos humanos ante los riesgos naturales.

Artículo 4º. Participación democrática. En ejercicio de las diferentes actividades que conforman la acción urbanística, las administraciones municipales, distritales y metropolitanas deberán fomentar la concertación entre los intereses sociales, económicos y urbanísticos, mediante la participación de los pobladores y sus organizaciones. Esta concertación tendrá por objeto asegurar la eficacia de las políticas públicas respecto de las necesidades y aspiraciones de los diversos sectores de la vida económica y social relacionados con el ordenamiento del territorio municipal, teniendo en cuenta los principios señalados en el artículo 2º de la presente ley. La participación ciudadana podrá desarrollarse mediante el derecho de petición, la celebración de audiencias públicas, el ejercicio de la acción de cumplimiento, la intervención en la formulación, discusión y ejecución de los planes de ordenamiento y en los procesos de otorgamiento, modificación, suspensión o revocatoria de las licencias urbanísticas, en los términos establecidos en la ley y sus reglamentos...

---

[21] MINVIVIENDA. (1997). Ley 388. Obtenido de http://www.minvivienda.gov.co/LeyesMinvivienda/0388%20-%201997.pdf#search=ley%20388%20de%201997

2.3.1.2 Decreto 1469 del 2010 del Ministerio de Ambiente, Vivienda y Desarrollo Territorial: "Por el cual se reglamentan las disposiciones relativas a las licencias urbanísticas; al reconocimiento de edificaciones; a la función pública que desempeñan los curadores urbanos; a la legalización de asentamientos humanos constituidos por viviendas de interés social, y se expiden otras disposiciones.

2.3.2 Normas Locales

2.3.2.1 Decreto número 0026 del 13 de octubre de 2009: Por medio del cual se realiza la revisión ordinaria y ajustes del Plan de Ordenamiento Territorial del Municipio de Pasto, adoptado mediante Decreto Municipal 0084 de 2003 y se dictan otras disposiciones.

2.4 MARCO HISTÓRICO

LA CURADURIA URBANA SEGUNDA DE PASTO inicia labores el 18 de Julio del 2002 una vez toma posesión del cargo de curador urbano segundo de Pasto; el arquitecto Germán Vela Luna, ante el alcalde del municipio de Pasto, Dr. Eduardo Alvarado Santander, por designación realizada después de haber logrado obtener el puntaje necesario en el concurso de méritos, realizado por la alcaldía municipal por convocatoria pública.

Actualmente el ingeniero Hernando Castillo Bravo ejerce el cargo de curador urbano segundo de Pasto, tras ser designado mediante Decreto expedido por la Administración Municipal como Curador Urbano Segundo Provisional desde el 19 de Julio 2012 hasta la fecha

La sede de la curaduría urbana segunda está ubicada en el centro de la ciudad, contigua a la plaza del carnaval y la cultura, en la Calle 18 No 19 – 95 oficina 208, 209, 210, 211, conmutador 7204488 telefax 7330203.

En la actualidad la curaduría segunda de Pasto cuenta con 12 empleados que se encargan de elaborar diferentes trabajos así:

La curaduría cuenta con una recepción encargada de radicación, liquidaciones y atención al público, un área técnica dividida en una parte legal revisada por una abogada con especialización en derecho administrativo, quien es la persona encargada de revisar la legalidad de la documentación recibida; y en cuanto a la parte estructural revisada por un ingeniero especializado en estructuras quien es el encargado de cotejar los planos y memorias a la luz de la Norma de Sismo-resistencia Colombiana NSR 98.

En cuanto a la revisión arquitectónica es realizada por el curador urbano quien al contar con un postgrado en urbanismo se encarga de revisar los planos arquitectónicos y atender consultas en cuanto al cumplimiento del Plan de Ordenamiento Territorial POT.

Por otra parte existen personas que se encargan de realizar la parte operativa como, ingreso de proyectos al sistema actual, comunicación de vecinos, ubicación de proyectos, transcripción de memos, elaboración de licencias, citación de vecinos y organización de archivo.

3. DISEÑO METODOLÓGICO

El proyecto está encaminado al diseño de un SGSI bajo la norma ISO/IEC 27001 que permita definir políticas de seguridad orientadas a la disminución de riesgos para la información de la Curaduría Urbana Segunda de Pasto y a satisfacer los requerimientos necesarios para la prestación de un buen servicio con eficiencia y calidad.

Con los diferentes métodos de recolección de información como la encuestas a empleados de los diferentes departamentos de la Curaduría Urbana Segunda de Pasto y la observación directa de los procesos se pretende realizar una investigación analítica y descriptiva donde se identifiquen los componentes necesarios a tener en cuenta en el diseño del SGSI.

Se analizará paso a paso cuales son las necesidades en el área de informática en cuanto a seguridad física, seguridad interna, seguridad externa, seguridad lógica, seguridad perimetral, elementos de control para la seguridad del hardware y software, alcances, análisis de riesgos, amenazas, posibles ataques, plan de contingencia y políticas de seguridad.

Este proceso se lo realiza mediante observación directa y encuestas a empleados.

La encuesta aplicada a los empleados de la curaduría, pretende medir las buenas prácticas de ellos para el manejo de la información, el conocimiento de los riesgos y el conocimiento sobre la seguridad de la información.

Tanto la observación directa como la aplicación de la encuesta están encaminadas a medir el grado de conocimiento sobre la importancia de seguridad en el manejo de la información y la importancia del seguimiento y aplicación de políticas de seguridad.

Una vez analizada la información se propondrá políticas de seguridad a implementar teniendo en cuanta la Norma ISO/IEC 27001 para disminuir los riesgos en cuanto a la seguridad de la información.

3.1 TIPO DE INVESTIGACIÓN

Este proyecto se enmarca dentro del tipo de investigación descriptiva y analítica porque abarca la recolección, descripción, registro, análisis e interpretación de la información, y la comprensión de procesos y fenómenos de la realidad estudiada. El análisis se hace sobre el funcionamiento y manejo actual de

la información, sobre el cual se pretende detectar falencias, plantear soluciones y resolver problemas[22].

3.1.1 Descriptiva: se efectúa cuando se desea describir, en todos sus componentes principales, una realidad; se refiere a la etapa preparatoria del trabajo científico que permita ordenar el resultado de las observaciones de las conductas, las características, los factores, los procedimientos y otras variables de fenómenos y hechos. Este tipo de investigación no tiene hipótesis explicada.

3.1.2 Analítica: Es un procesamiento más complejo con respecto a la investigación descriptiva, que consiste fundamentalmente en establecer la comparación de variables entre grupos de estudio y de control sin aplicar o manipular las variables, estudiando éstas según se dan naturalmente en los grupos. Además, se refiere a la proposición de hipótesis que el investigador trata de probar o negar.

3.2 MÉTODO DE INVESTIGACIÓN

El método de investigación definido en este estudio es de tipo descriptivo**,** puesto que se conoce una situación problema, a partir de la cual se espera analizar y evaluar a través de variables los diferentes requerimientos para el análisis y diseño de un SGSI bajo la norma ISO/IEC 27001.

3.3 UNIVERSO Y MUESTRA

3.3.1 Población. Para la encuesta de los empleados, la población de estudio está conformada por el personal que labora en la curaduría urbana segunda de Pasto.

Tabla 1. Población conformada por el personal de la curaduría urbana segunda de Pasto.

Población	Número de Personas
Curaduría Urbana Segunda de Pasto	11 Empleados
Total	11 Empleados

Fuente: Esta Investigación

[22] Ciclo PDCA. Sistemas de Gestión de Seguridad de la Información. Obtenido de http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-14-agosto-2013/135_ciclo_pdca__edward_deming.htmll

3.3.2 Muestra

- Teniendo en cuenta que el personal que labora en la Curaduría es igual a un número de personas relativamente pequeño, se tomó como muestra el total de personas = 11.

3.4 RECOLECCIÓN DE LA INFORMACIÓN

La información que se pretende recopilar se obtendrá de la curaduría urbana segunda de Pasto, su perfil, generalidades, situación actual y en general el análisis de riesgos de seguridad en el área de informática

3.4.1 Información primaria: Encuestas y pruebas: A través de las encuestas aplicadas a los empleados de la Curaduría se determinará la problemática interna de la Curaduría referente al manejo de la información, los procedimientos de seguridad actuales e la implementación de políticas de seguridad necesarias para disminuir riesgos, además de la realización de pruebas como reconocimiento, mapeo y escaneo de red que permitan detectar posibles riesgos a los que está expuesta la información.

3.4.2 Información secundaria: Para determinar los requerimientos externos se tendrá en cuenta toda la información de tipo bibliográfico, los conceptos aprendidos en la transcurso de la especialización, los cuales permiten enfocarnos en el problema de investigación, así como páginas de Internet con información del tema de estudio.

3.4.3 Instrumentos de recolección de información. Para la recolección de la información se utilizó la técnica de observación directa, la técnica de la encuesta y realización de pruebas:

3.4.3.1 Técnica de Observación: (Modalidad de observación – Número de Observadores: Individual; según el lugar donde se realiza: En la vida real) Se observó cómo se realizan siguientes actividades como: Inicio del sistema, ubicación del servidor, ingreso de datos al sistema, elaboración de copias de seguridad, actualización de información, manejo de correos electrónicos.

3.4.3.2 Técnica de Encuesta: Para la encuesta empleados, consiste en un cuestionario que contiene preguntas cerradas, preguntas categorizadas con respuesta en abanico, preguntas de estimación. Para la estructuración del documento se tomó en cuenta variables como: Tiempo, frecuencia, calidad, problemas, estados, reportes y nivel de satisfacción.

3.4.3.3 Técnica de realización de pruebas: Consiste en la realización de pruebas con herramientas de escaneo o de análisis de tráfico de red, cuando la red esté operando, para verificar cuál es su funcionamiento.

3.4.4 Muestras

3.4.4.1 Muestra Empleados: Técnica de Encuesta: Para la estructuración del documento se tomó en cuenta aspectos como: Eventos presentados referentes a la confidencialidad, integridad y disponibilidad de la información, manejo de contraseñas, medidas y políticas de seguridad, fallos, robos, virus etc.

3.4.4.2 Características de la encuesta para empleados de la Curaduría. El instrumento consta de: 10 ítems, la forma de contestar es escrita en un tiempo de 10 a 15 minutos.

3.4.4.5 Descripción del Instrumento:

Presentación: Los instrumentos están diseñados con base en el siguiente criterio: El cumplimiento de los Objetivos.

Normas de Administración: Los instrumentos fueron aplicados en forma individual a los empleados de la Curaduría. El diseño de ítems consta de preguntas cerradas, preguntas categorizadas con respuesta en abanico, preguntas de estimación y de opción múltiple las cuales el sujeto puede elegir la respuesta con la que mayor se identifique.

Áreas que explora: La elaboración de los instrumentos permite indagar si existen falencias y dificultades en los procesos de manejo y seguridad de la información.

3.5 PROCESAMIENTO DE LA INFORMACIÓN

La información de la cual se dispone para el diseño e implementación de un SGSI para el área de Informática de la curaduría urbana segunda de Pasto se clasifica y analiza minuciosamente para determinar riesgos, debilidades, amenazas y políticas de seguridad a implementarse a través del SGSI.

3.5.1 Metodología para el análisis y diseño. En el diseño de un SGSI se debe seguir una serie de procesos que permitan organizar las actividades para construir el producto, teniendo en cuenta un conjunto de métodos y técnicas que permitan desarrollar un SGSI de calidad.

Para el desarrollo del presente proyecto se toma como guía el método denominado Ciclo PDCA (en español PHVA)

Para la implantación de un sistema de Gestión de la seguridad de la información, se requiere del desarrollo de actividades que marquen un orden lógico para llevar organizado todo el proceso. El modelo PDCA (Plan, do, check, act), en su

equivalencia en español es Planificar, hacer, verificar y actuar (PHVA), es una estrategia de mejora continua de calidad en cuatro pasos. Este modelo es muy utilizado para implantación de sistemas de gestión, como los sistemas de gestión de la calidad que muchas empresas de hoy lo implantan para la calidad administrativa y de servicios con el objetivo de perfeccionarlos y continuar en un proceso de mejora continua[23].

Para el caso de la implantación de Sistemas de Gestión de la Seguridad informática, el ciclo PDCA es una estrategia efectiva para la organización y documentación que se requiere en este proceso.

El ciclo PDCA como modelo para implantación de SGSI, permanece en una constante revaluación, por cuanto funciona, bajo la filosofía del mejoramiento continuo; en seguridad sería la revaluación de las medidas de prevención, corrección y evaluación, manteniendo un constante ciclo que por sus características no podría terminar. A continuación se detalla cada uno de los pasos del modelo Deming como metodología apropiada los SGSI.

Planear: En esta etapa se enmarca todo el proceso de análisis de la situación en que actualmente se encuentra la empresa respecto a los mecanismos de seguridad implementados y la normativa ISO/IEC 17799:2005, la cual se pretende implantar para evaluación y certificación. Así mismo en la etapa de planeación se organizan fases relevantes como son:

- Establecer el compromiso con los directivos de la empresa para el inicio, proceso y ejecución
- Fase de análisis de información de la organización, En esta fase se comprueba cuáles son los sistemas informáticos de hardware y los sistemas de información que actualmente utiliza la empresa para el cumplimiento de su misión u objeto social.
- Fase de evaluación del riesgo; En esta fase se evalúa los riesgos, se tratan y se seleccionan los controles a implementar.

Hacer: En esta etapa se implementan todos los controles necesarios de acuerdo a una previa selección en la etapa de planeación, teniendo en cuenta el tipo de empresa. También se formula y se implementa un plan de riesgo

Verificar: Consiste en efectuar el control de todos los procedimientos implementados en el SGSI. En este sentido, se realizan exámenes periódicos para asegurar la eficacia del SGSI implementado, se revisan los niveles de riesgos

[23] Ciclo PDCA. Sistemas de Gestión de Seguridad de la Información. Obtenido de http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-14-agosto-2013/135_ciclo_pdca__edward_deming.htmll

aceptables y residuales y se realicen periódicamente auditorías internas para el SGSI.

Actuar: Desarrollar mejoras a los hallazgos identificadas al SGSI y validarlas, realizar las acciones correctivas y preventivas, mantener comunicación con el personal de la organización relevante.

3.5.2 Análisis de la encuesta realizada a los empleados de Curaduría Urbana Segunda de Pasto. Después de analizada la información recolecta por medio de la encuesta a los empleados de la Curaduría a través de 10 preguntas que están encaminadas a evaluar los siguientes aspectos como incidentes presentados, manejo y cambio de contraseñas, medidas y políticas de seguridad adoptadas actualmente por la empresa, se pueden exponer las siguientes conclusiones:

- Se puede decir que el manejo y cambio de contraseñas no es el más adecuado y no se cambian las contraseñas con frecuencia.

- Los empleados manifiestan que todos han tenido inconvenientes al utilizar su computador como instrumento de trabajo, ya sea por lentitud, por bloqueo, por mensajes de error, inconvenientes de acceso a red. Además manifiestan no conocer políticas concretas que se deben tener en cuenta para proteger la información.

Por lo anteriormente mencionado se hace necesario implementar un SGSI que permita clasificar la información, conocer que activos son los más importantes para la empresa, realizar un análisis de riesgos, definir salvaguardas, definir responsabilidades en el manejo de la información y adoptar políticas y controles de seguridad para proteger el área de informática de la Curaduría Urbana Segunda de Pasto. (Anexo A.)

3.5.3 Descripción y análisis de la prueba realizada a la red de la Curaduría Urbana Segunda de Pasto, con Wiresshark. Adicionalmente se realiza un análisis de tráfico para la red de la Curaduría Urbana Segunda de Pasto, utilizando la herramienta Wireshark con virtualbox con kali Linux, donde se puede observar las actividades de cada uno de los host que integran la red, la dirección Ip del servidor, la dirección ip de los host, los protocolos de transmisión como UDP, TCP, HTTPs, ARP, DNS, el tiempo, la fuente, el destino, el protocolo utilizado, la longitud, las solicitudes que se realizan al servidor, los accesos a páginas de internet etc. El informe y pantallazos sobre el análisis de la red se encuentra en el anexo B

4. SGSI PARA LA CURADURIA URBANA SEGUNDA DE PASTO

Teniendo en cuenta el ciclo PDCA que permite realizar una serie de pasos y procesos para la construcción de un SGSI, a continuación se procede a realizar cada una de estas etapas:

4.1. ESTABLECER EL SGSI

4.1.1 Alcance. Con el fin de mejorar la calidad en la prestación del servicio en el otorgamiento de licencias urbanísticas se aplica el SGSI a los procesos, recursos informáticos y tecnológicos que hacen parte del área de informática de la Curaduría Urbana Segunda de Pasto con el fin de establecer políticas para gestionar adecuadamente la seguridad de la información y debe ser aplicada y cumplida por todos los empleados de la organización.

4.1.2 Política del Sistema de Gestión. La Curaduría Urbana Segunda de Pasto pretende que la información manejada por la entidad referente al estudio, tramite, otorgamiento y archivo sobre la expedición de licencias urbanísticas; esté debidamente protegida con el fin de preservar y salvaguardar la confidencialidad, disponibilidad e integridad de la información, ya que es una entidad privada con función pública encargada de autorizar licencias que cumplan con las normas urbanísticas, arquitectónicas, jurídicas y estructurales tanto locales como nacionales.

El Curador Urbano es el responsable de la implementación de los requerimientos de seguridad con el fin de proteger la información por lo tanto en su organización se debe elaborar un análisis y evaluación del riesgo para gestionarlos adecuadamente y disminuir eventos indeseados.

4.1.3 Metodología de Evaluación del Riesgo. Se elige la metodología Magerit para el análisis y gestión de los de riesgos porque:

- Los pasos para su ejecución están claramente definidos.
- La documentación es clara, amplia y permite realizar una identificación adecuada del entorno donde va a ser aplicada.
- Permite enfocar los esfuerzos al análisis de riesgos críticos para la empresa, por lo tanto se puede trabajar más claramente en las posibles soluciones para dichos riesgos.

- Se puede decir que por estar incluida en los estándares ISO, sirve como como punto de partida para procesos de certificación y mejoramiento del sistema de gestión para la empresa.

- Permite el análisis a riesgos, donde se identifican y valoran los diferentes componentes que pueden tener los riesgos.

- Permite la minimización de riesgos mediante la implementación de medidas de seguridad.

- MAGERIT le permita una empresa saber cuánto valor está en juego y le ayudará a protegerlo.

- Con MAGERIT los resultados de análisis de riesgos se pueden expresar en valores cualitativos y cuantitativos, lo que permite a los directivos tomar decisiones.

Según MAGERIT: El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados estos pasos son:

Paso 1: Inventario de Activos
Paso 2: Valoración de los activos
Paso 3: Amenazas (identificación y valoración)
Paso 4: Salvaguardias
Paso 5: Impacto residual y riesgo residual
Resultados del análisis de riesgos

4.1.4 Análisis de Riesgos de la Curaduría Urbana Segunda de Pasto

4.1.4.1. Inventario de Activos. Las empresas deben proteger la confidencialidad, integridad y disponibilidad de la información para velar por la continuidad del negocio independientemente de su actividad social. Para proteger dicha información de riesgos y amenazas la Curaduría Urbana Segunda de Pasto realiza un inventario de sus activos teniendo en cuenta la metodología Magerit que los clasifica en los siguientes grupos.

- Activos esenciales
- Datos o información (catalogados como fundamentales),
- Servicios,
- Las aplicaciones de software.
- Equipos informáticos
- Personal
- Redes de Comunicación

- Soportes de Información
- Equipamiento Auxiliar
- Instalaciones

4.1. 4.1.1 Activos esenciales

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[vr]	Datos vitales	[I_Proyectos]	Información de Proyectos radicados (base de datos y registro de proyectos)
		[I_Licencias]	Información de Licencias
		[I_Normativa]	Información de Normativa (Normas locales, nacionales, POT, acuerdos, decretos, Cartografía)
[per]	Datos de Carácter Personal	[I_Contabilidad]	Contabilidad de la empresa
[classified]	Datos clasificados	[E_S_Licenciador]	Ejecutable software Licenciador
		[D_Históricos]	Datos Históricos de proyectos radicados
		[D_Proyectos]	Documentación de proyectos tramitados.

4.1. 4.1.2 Datos/Información

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[files]	Ficheros	[A_proyectos]	Archivos de proyectos radicados
		[A_Clientes]	Archivos de Clientes
		[A_Contabilidad]	Archivo de Contabilidad
		[A_Informes y Licencias]	Archivos de Informes y licencias expedidas
[backup]	Copias de Respaldo	[A_Copias de Seguridad]	Archivo de Copias de seguridad de la información
[conf]	Datos de configuración	[D_Configuracion_ser]	Datos de configuración de servidores y equipos
[int]	Datos de gestión interna	[D_GestionProyectos]	Datos de Gestión de proyectos radicados
[password]	Credenciales	[Pass_usuarios]	Contraseñas de acceso de empleados

4.1.4.1.3 Claves Criptográficas. Debemos garantizar cifrado de datos y comunicaciones por el hecho de manejar aplicaciones bancarias.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[encrypt]	Claves de cifra	[CC_Aplicaciones_bancarias]	Claves de cifra de aplicaciones bancarias

4.1.4.1.4 Inventario de Servicios. Los servicios son para los clientes y empleados.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[ext]	A usuarios externos (bajo una relación contractual)	[S_U_Externo]	Servicios prestados a usuarios externos bajo relación contractual (Clientes de proyectos)
[int]	Interno (a usuarios de la propia organización)	[S_U_Interno]	Servicios prestados a trabajadores tanto al interior como haciendo uso de internet.
[www]	World wide web	[S_Internet]	Servicio de internet al que pueden acceder los empleados.
[email]	Correo electrónico	[S_correo]	Manejo de correos electrónicos
[file]	Almacenamiento de ficheros	[S_A_Bases de datos]	Servicio de almacenamiento de información en el servidor de bases de datos.
[ipm]	Gestión de privilegios	[G_privilegios]	Manejo de privilegios de acuerdo al rol dentro de la empresa y el lugar de donde esté ingresando, considerando el desempeño como teletrabajo.

4.1.4.1.5 Software – Aplicaciones Informáticas. Ya que la empresa se dedica al otorgamiento de licencias urbanísticas cuenta con un servidor y software licenciador donde se registra, actualiza y almacena el estado de cada proyecto, genera reportes y licencias.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[app]	Servidor de aplicaciones	[Server_App]	Servidor de aplicaciones
[dbms]	Sistema de gestión de bases de datos	[S_BaseDeDatos]	Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa.
[Oficce]	Ofimática	[Oficce]	Office 2010
[av]	Antivirus	[Antivirus]	McAfee original con actualizaciones automáticas.
[os]	Sistema operativo	[OS_Win7]	Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas.

4.1.4.1.6 Equipos Informáticos. Se consideran todos los equipos informáticos de la empresa.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[host]	Grandes equipos (Servidor de bases de datos, servidores de aplicación)	[S_Aplicaciones]	Servidor Aplicaciones
		[S_Database]	Servidor de Base de Datos
[mid]	Equipos medios (Equipos de trabajo conectados a través de red inalámbrica por red 802.1x)	[PC_trabajadores]	Equipos de mesa
[pc]	Equipos que son fácilmente transportados	[PC_portatiles]	Equipos Portatiles
[print]	Equipos de impresión	[E_Impresoras]	Impresoras
[router]	Enrutadores	[R_enrutadores]	Enrutadores

4.1.4.1.7 Redes de comunicaciones. Se considera las redes de comunicaciones.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[wifi]	Red inalámbrica	[R_wifi]	Red Inalámbrica
[LAN]	Red local	[R_Local]	Red local
[Internet]	Internet	[Internet]	Internet

4.1.4.1.8 Soportes de Información _almacenamiento electrónico. Se considera dispositivos físicos de almacenamiento electrónico.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[cd]	Discos	[A_CD]	Almacenamientos en Disco Duro
[cd]	Cederrom (CD_ROM)	[A_CD]	Almacenamiento en CD
[USB]	Memorias	[A_Memorias]	Almacenamiento en Memorias
[dvd]	DVR	[A_DVD]	Almacenamiento en DVD

4.1.4.1.9 Soportes de Información _almacenamiento no electrónico. Se considera dispositivos físicos de almacenamiento no electrónico.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[printed]	Material impreso	C_Documentaciónproyecto	Carpetas con la documentación de cada proyecto(documentación, planos, memorias de cálculo y estudios de suelos)
		C_Reporteseinformes	Carpetas de reportes e informes impresos
		C_SoprtesContabilidad	Carpetas facturas y soportes contabilidad
		C_varios	Carpetas varios

4.1.4.1.10 Equipamiento auxiliar. Equipos de soportes a los sistemas informáticos sin estar directamente relacionados.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[printed]	Sistemas de Alimentación ininterrumpida	U_Computadores	Ups computadores
[suplly]	Suministros Esenciales	Esenciales	Suministros esenciales tales como: Papel, sobres, carpetas, tinta, etc.
[Furniture]	Mobiliario	M_Mobiliario	Mobiliario: Estantes, armarios, escritorios, archivadores, etc.

4.1.4.1.11 Instalaciones

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[building]	Edificio	[E_empresa]	Edificio de la empresa (Curaduría)

4.1.4.1.12 Personal

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[ui]	Usuarios internos	[E_personal]	Personal de recepción, área técnica, administrativa y archivo
[adm]	Administradores de sistemas	[A_sistemas]	Administrador de sistemas

4.1.4.2. Valoración cualitativa de los activos. Teniendo en cuenta que todos los activos no tienen la misma relevancia e importancia para la empresa y que cada uno de estos en caso de ser atacado o sufrir un incidente genera un impacto diferente en la organización, se procede a realizar una valoración cualitativa para cada uno de los activos teniendo en cuenta las dimensiones de seguridad como confiabilidad, integridad, autenticidad, disponibilidad y trazabilidad de acuerdo a la siguiente Tabla.

Tabla 2: Criterios de Valoración

valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Fuente: Tomado del Magerit V3 libro 2 Catalogo de elementos

4.1.4.2.1 Valoración Cualitativa de Activos esenciales

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[vr]	Datos vitales	[I_Proyectos]	Información de Proyectos radicados (base de datos y registro de proyectos)	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	
				Trazabilidad	
		[I_Licencias]	Información de Licencias	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	
		[I_Normativa]	Información de Normativa (Normas locales, nacionales, POT, acuerdos, decretos, Cartografía)	Confiabilidad	
				Integridad	3
				Autenticidad	
				Disponibilidad	3
				Trazabilidad	
[per]	Datos de Carácter Personal	[I_Contabilidad]	Contabilidad de la empresa	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[classified]	Datos clasificados	[E_S_Licenciador]	Ejecutable software Licenciador	Confiabilidad	
				Integridad	6
				Autenticidad	
				Disponibilidad	3
				Trazabilidad	
		[D_Históricos]	Datos Históricos de proyectos radicados	Confiabilidad	3
				Integridad	3
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
		[D_Proyectos]	Documentación de proyectos tramitados.	Confiabilidad	
				Integridad	
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	

4.1.4.2.2 Valoración Cualitativa de Datos/Información

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[files]	Ficheros	[A_proyectos]	Archivos de proyectos radicados	Confiabilidad	6
				Integridad	6
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
		[A_Clientes]	Archivos de Clientes	Confiabilidad	6
				Integridad	6
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
		[A_Contabilidad]	Archivo de Contabilidad	Confiabilidad	6
				Integridad	6
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
		[A_Informes y Licencias]	Archivos de Informes y licencias expedidas	Confiabilidad	6
				Integridad	6
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	
[backup]	Copias de Respaldo	[A_Copias de Seguridad]	Archivo de Copias de seguridad de la información	Confiabilidad	
				Integridad	6
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
[conf]	Datos de configuración	[D_Configuracion_ser]	Datos de configuración de servidores y equipos	Confiabilidad	
				Integridad	
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[int]	Datos de gestión interna	[D_GestionProyectos]	Datos de Gestión de proyectos radicados	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	
[password]	Credenciales	[Pass_usuarios]	Contraseñas de acceso de empleados	Confiabilidad	
				Integridad	
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	

4.1.4.2.3 Valoración Cualitativa de Claves Criptográficas. Debemos garantizar cifrado de datos y comunicaciones por el hecho de manejar aplicaciones bancarias.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[encrypt]	Claves de cifra	[CC_Aplicaciones_bancarias]	Claves de cifra de aplicaciones bancarias	Confiabilidad	6
				Integridad	7
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	

4.1.4.2.4 Valoración Cualitativa de Servicios. Los servicios son para los clientes y empleados.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[ext]	A usuarios externos (bajo una relación contractual)	[S_U_Externo]	Servicios prestados a usuarios externos bajo relación contractual (Clientes de proyectos)	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[int]	Interno (a usuarios de la propia organización)	[S_U_Interno]	Servicios prestados a trabajadores tanto al interior como haciendo uso de internet.	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[www]	World wide web	[S_Internet]	Servicio de internet al que pueden acceder los empleados.	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[email]	Correo electrónico	[S_correo]	Manejo de correos electrónicos	Confiabilidad	6
				Integridad	6
				Autenticidad	7

				Disponibilidad	
				Trazabilidad	
[file]	Almacenamiento de ficheros	[S_A_Bases de datos]	Servicio de almacenamiento de información en el servidor de bases de datos.	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	
				Trazabilidad	
[ipm]	Gestión de privilegios	[G_privilegios]	Manejo de privilegios de acuerdo al rol dentro de la empresa y el lugar de donde esté ingresando, considerando el desempeño como teletrabajo.	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	
				Trazabilidad	

4.1.4.2.5 Valoración Cualitativa de Software – Aplicaciones Informáticas

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[app]	Servidor de aplicaciones	[Server_App]	Servidor de aplicaciones	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	
				Trazabilidad	
[dbms]	Sistema de gestión de bases de datos	[S_BaseDeDatos]	Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa.	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	
				Trazabilidad	
[Oficce]	Ofimática	[Oficce]	Office 2010	Confiabilidad	

				Integridad	
				Autenticidad	
				Disponibilidad	2
				Trazabilidad	
[av]	Antivirus	[Antivirus]	McAfee original con actualizaciones automáticas.	Confiabilidad	7
				Integridad	
				Autenticidad	
				Disponibilidad	7
				Trazabilidad	
[os]	Sistema operativo	[OS_Win7]	Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas.	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	4
				Trazabilidad	

4.1.4.2.6 Valoración Cualitativa de Equipos Informáticos

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[host]	Grandes equipos (Servidor de bases de datos, servidores de aplicación)	[S_Aplicaciones]	Servidor Aplicaciones Servidor de Base de Datos Servidor Aplicaciones Servidor de Base de Datos Servidor Aplicaciones	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	
		[S_Database]	Servidor de Base de Datos	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	
[mid]	Equipos medios (Equipos de trabajo	[PC_trabajadores]	Equipos de mesa	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	

	conectados a través de red inalámbrica por red 802.1x)			Trazabilidad	
[pc]	Equipos que son fácilmente transportados	[PC_portatiles]	Equipos Portatiles	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[print]	Equipos de impresión	[E_Impresoras]	Impresoras	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	4
				Trazabilidad	
[router]	Enrutadores	[R_enrutadores]	Enrutadores	Confiabilidad	7
				Integridad	7
				Autenticidad	7
				Disponibilidad	7
				Trazabilidad	

4.1.4.2.7 Valoración Cualitativa de Redes de comunicaciones

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[wifi]	Red inalámbrica	[R_wifi]	Red Inalámbrica	Confiabilidad	7
				Integridad	7
				Autenticidad	
				Disponibilidad	7
				Trazabilidad	
[LAN]	Red local	[R_Local]	[LAN]	Confiabilidad	7
				Integridad	7
				Autenticidad	
				Disponibilidad	7
				Trazabilidad	
[Internet]	Internet	[Internet]	[Internet]	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	7
				Trazabilidad	

4.1.4.2.8 Valoración Cualitativa de Soportes de Información _almacenamiento electrónico

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[cd]	Discos	[A_CD]	Almacenamientos en Disco Duro	Confiabilidad	
				Integridad	5
				Autenticidad	
				Disponibilidad	5
				Trazabilidad	
[cd]	Cederrom (CD_ROM)	[A_CD]	Almacenamiento en CD	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
[USB]	Memorias	[A_Memorias]	Almacenamiento en Memorias	Confiabilidad	
				Integridad	5
				Autenticidad	
				Disponibilidad	5
				Trazabilidad	
[dvd]	DVR	[A_DVD]	Almacenamiento en DVD	Confiabilidad	
				Integridad	5
				Autenticidad	
				Disponibilidad	5
				Trazabilidad	

4.1.4.2.9 Valoración Cualitativa de Soportes de Información _almacenamiento no electrónico

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[printed]	Material impreso	C_ Documentación proyecto	Carpetas con la documentación de cada proyecto(documentación, planos, memorias de cálculo y estudios de suelos)	Confiabilidad	
				Integridad	7
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
		C_ Reportes e informes	Carpetas de reportes e informes impresos	Confiabilidad	
				Integridad	7

				Autenticidad	
				Disponibilidad	
				Trazabilidad	
		C_Sop0rtesContabilidad	Carpetas facturas y soportes contabilidad	Confiabilidad	
				Integridad	7
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
		C_varios	Carpetas varios	Confiabilidad	
				Integridad	7
				Autenticidad	
				Disponibilidad	
				Trazabilidad	

4.1. 4.2.10 Valoración Cualitativa de Equipamiento auxiliar

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[printed]	Sistemas de Alimentación ininterrumpida	U_Computadores	Ups computadores	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	4
				Trazabilidad	
[suplly]	Suministros Esenciales	Esenciales	Suministros esenciales tales como: Papel, sobres, carpetas, tinta, etc.	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	2
				Trazabilidad	
Mobiliario	M_Mobiliario	Mobiliario: Estantes, armarios, escritorios, archivadores, etc.	Mobiliario	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	3
				Trazabilidad	

4.1.4.2.11 Valoración Cualitativa de Instalaciones

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[building]	Edificio	[E_empresa]	Edificio de la empresa (Curaduría)	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	5
				Trazabilidad	

4.1. 4.2.12 Valoración Cualitativa de Personal

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de Seguridad	Criterio
[ui]	Usuarios internos	[E_personal]	Personal de recepción, área técnica, administrativa y archivo	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	
[adm]	Administradores de sistemas	[A_sistemas]	Administrador de sistemas	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	

4.1.4.3. Identificación de Amenazas. La valoración de amenazas se realiza teniendo en cuenta la frecuencia con la que ocurre, las dimensiones de seguridad según Magerit y la escala de rango porcentual de impactos en los activos

Tabla 3: Escala de rango de frecuencia de amenazas

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada 1 semanas	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Fuente: Tomada del módulo de sistemas de gestión de la seguridad informática

Tabla 4: Dimensiones de seguridad según Magerit

Dimensiones de Seguridad a valorar	Identificación
Autenticidad	A
Confiabilidad	C
Integridad	I
Disponibilidad	D
Trazabilidad	T

Fuente: Esta Investigación

Tabla 5*:* Escala de rango porcentual de impactos en los activos para cada dimensión de seguridad.

Impacto	**Valor cuantitativo**
Muy alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy bajo	5%

Fuente: Tomada del módulo de sistemas de gestión de la seguridad informática

En la siguiente tabla se procede a identificar las amenazas para el inventario de activos realizado. En algunos casos se toma los activos más críticos o la categoría, identificando su frecuencia e impacto.

Relación de amenazas por activo identificando su frecuencia e impacto							
Amenaza	**Activo**	**Frecuencia de la amenaza**	**Impacto para cada Dimensión de seguridad (%)**				
			[A]	**[C]**	**[I]**	**[D]**	**[T]**
[N.1] Fuego [N.2] Daños por agua	**Equipos informáticos Instalaciones**	5				100 %	
[I.1] Fuego [I.2] Daños por	**Equipos informáticos**	10				100 %	

Relación de amenazas por activo identificando su frecuencia e impacto							
Amenaza	**Activo**	**Frecuencia de la amenaza**	**Impacto para cada Dimensión de seguridad (%)**				
			[A]	**[C]**	**[I]**	**[D]**	**[T]**
agua	**Instalaciones**						
[N.1] Fuego [N.2] Daños por agua	**Soporte de almacenamiento electrónico y no electrónico**	5				100 %	
[I.1] Fuego [I.2] Daños por agua	**Soporte de almacenamiento electrónico y no electrónico**	5				100 %	
[N.1] Fuego [N.2] Daños por agua	**Equipamiento Auxiliar**	5				50%	
[I.1] Fuego [I.2] Daños por agua	**Equipamiento Auxiliar**	5				50%	
[N.*] Desastres industriales	**Equipos informáticos,**	10				100 %	
	Soporte de Información	5				75%	
	Equipamiento Auxiliar	5				20%	
	Instalaciones	5				100 %	
[I.*] Desastres industriales	**Equipos Informáticos**	10				100 %	
	Soporte de Información	5				75%	
	Equipamiento Auxiliar	5				20%	
	Instalaciones	5				100 %	
[I.3] Contaminación mecánica	**Equipos Informáticos**	50				75%	
	Soporte de información	5				50%	
	Equipamiento	5				20%	

Relación de amenazas por activo identificando su frecuencia e impacto							
Amenaza	**Activo**	**Frecuencia de la amenaza**	**Impacto para cada Dimensión de seguridad (%)**				
			[A]	**[C]**	**[I]**	**[D]**	**[T]**
	auxiliar						
[I.4] Contaminación electromagnética	Router de acceso inalámbrico.	50				100 %	
[I.5] Avería de origen físico o lógico	**Software - Aplicaciones Informáticas**	50				100 %	
	Equipos informáticos	10				100 %%	
	Soportes de Información	5				20%	
	Equipamiento Auxiliar	5				20%	
[I.6] Corte del suministro eléctrico	**Equipos Informáticos**	50				100 %	
	Soporte de Información (electrónicos)	5				50%	
	Ups computadores	5				5%	
[I.7] Condiciones inadecuadas de temperatura o humedad	**Equipos Informáticos**	50				100 %	
[I.8] Fallo de servicios de comunicaciones	**Redes de comunicaciones (Red inalámbrica, red local e internet)**	50				100 %	
[I.9] Interrupción de otros servicios y suministros esenciales.	**Equipamiento Auxiliar**	5				5%	
[I.10] Degradación de los soportes de almacenamiento de la información.	**Soportes de Información**	5				5%	
[E.1] Errores de los usuarios	Archivos de proyectos radicados	50		100 %	100 %	75%	

Relación de amenazas por activo identificando su frecuencia e impacto							
Amenaza	**Activo**	**Frecuencia de la amenaza**	**Impacto para cada Dimensión de seguridad (%)**				
			[A]	**[C]**	**[I]**	**[D]**	**[T]**
Datos/Información	Archivos de Clientes	5		50%	100 %	50%	
	Archivo de Contabilidad	5		100 %	100 %	50%	
	Archivos de Informes y licencias expedidas	10		100 %	100 %	50%	
	Archivo de Copias de seguridad de la información	5		100 %	100 %	50%	
	Datos de configuración de servidores y equipos	5		100 %	100 %	50%	
	Datos de Gestión de proyectos radicados	5		100 %	100 %	100 %	
	Contraseñas de acceso de empleados	5		50%	50%	50%	
[E.1] Errores de los usuarios	**Claves Criptográficas**	5		100 %	100 %	100 %	
[E.1] Errores de los usuarios **Servicios**	Servicios prestados a usuarios externos bajo relación contractual (Clientes de proyectos)	5		50%	50%	50%	
	Servicios prestados a trabajadores tanto al interior como haciendo uso de internet.	5		100 %	100 %	75%	
	Servicio de internet al que pueden acceder los empleados.	10		75%	50%	50%	
	Manejo de correos electrónicos	5		50%	50%	75%	

Relación de amenazas por activo identificando su frecuencia e impacto							
Amenaza	**Activo**	**Frecuencia de la amenaza**	**Impacto para cada Dimensión de seguridad (%)**				
			[A]	**[C]**	**[I]**	**[D]**	**[T]**
	Servicio de almacenamiento de información en el servidor de bases de datos.	10		75%	75%	75%	
	Manejo de privilegios de acuerdo al rol dentro de la empresa y el lugar de donde esté ingresando, considerando el desempeño como teletrabajo.	5		100 %	75%	75%	
[E.1] Errores de los usuarios **Aplicaciones**	Servidor de aplicaciones	5		75%	75%	100 %	
	Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa.	5		100 %	100 %	100 %	
	Office 2010	5		75%	50%	75%	
	McAfee original con actualizaciones automáticas.	5		75%	20%	75%	
	Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas.	10		75%	20%	75%	

Relación de amenazas por activo identificando su frecuencia e impacto							
Amenaza	**Activo**	**Frecuencia de la amenaza**	**Impacto para cada Dimensión de seguridad (%)**				
			[A]	**[C]**	**[I]**	**[D]**	**[T]**
[E.1] Errores de los usuarios. **Soporte de información**	**Soportes de Información almacenamiento electrónico.**	10		50%	50%	50%	
	Soportes de Información _almacenamiento no electrónico.	10		50%	50%	50%	
[E.2] Errores del administrador	**Datos/Información**	50		100 %	75%	50%	
	Claves criptográficas	5		100 %	75%	50%	
	Servicios	5		75%	50%	75%	
	Aplicaciones	5		100 %	75%	75 %	
	Redes de Comunicación	10		100 %	75%	75 %	
[E.4] Errores de configuración	Datos de configuración de servidores y equipos	5			100 %		
[E.7] Deficiencias en la organización	Personal de recepción, área técnica, administrativa y archivo	50				75%	
	Administrador de sistemas	5				75%	
[E.8] Difusión de software dañino	**Software – Aplicaciones Informáticas**	5		50%	50%	75%	
[E.9] Errores de [re-]encaminamiento	**Servicios**	5		20%			
	Software – Aplicaciones	5		20%			

Relación de amenazas por activo identificando su frecuencia e impacto							
Amenaza	**Activo**	**Frecuencia de la amenaza**	**Impacto para cada Dimensión de seguridad (%)**				
			[A]	**[C]**	**[I]**	**[D]**	**[T]**
	Informáticas						
	Redes de comunicaciones	5		20%			
[E.14] Escapes de información	**Activos esenciales**	5		100 %			
	Datos / información	5		100 %			
[E.15] Escapes de información	**Datos / información**	10			100 %		
[E.18] Escapes de información	**Datos / información**	10					
	Aplicaciones	5				50%	
	Soporte Información	5				20%	
[E.19] Fugas de información	**Datos / información**	10		75%			
	Claves criptográficas	5		75%			
	Servicios	10		75%			
	Aplicaciones	10		50%			
	Personal	10		75%			
[E.20] Vulnerabilidades de los programas (software)	Servidor de aplicaciones	5		75%	50%	20%	
	Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa.	10		50%	20%	75%	
	Office 2010	5		5%	5%	5%	
	McAfee original con actualizaciones automáticas.	5		75%	20%	100 %	
	Sistema operativo Windows 7, en su versión professional	10		50%	20%	75%	

Relación de amenazas por activo identificando su frecuencia e impacto							
Amenaza	**Activo**	**Frecuencia de la amenaza**	**Impacto para cada Dimensión de seguridad (%)**				
			[A]	**[C]**	**[I]**	**[D]**	**[T]**
	con actualizaciones automáticas activadas						
[E.21] Errores de mantenimiento / actualización de programas (softwa-re)	Servidor de aplicaciones	5			20%	75%	
	Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la empresa.	10			20%	75%	
	Office 2010	5			20%	20%	
	McAfee original con actualizaciones automáticas.	10			5%	20%	
	Sistema operativo Windows 7, en su versión profesional con actualizaciones automáticas activadas	10			50%	50%	
[E.24] Caída del sistema por agotamiento de recursos	**Servicios**	5				100 %	
	Equipos Informáticos	10				100 %	
	Redes de comunicaciones	5				100 %	
[E.25] Pérdida de equipos -Robo	**Equipos Informáticos**	5		75%		100 %	
	Soporte Información	5		20%		100 %	
	Equipamiento Auxiliar	5		5%		20%	

Relación de amenazas por activo identificando su frecuencia e impacto							
Amenaza	**Activo**	**Frecuencia de la amenaza**	**Impacto para cada Dimensión de seguridad (%)**				
			[A]	**[C]**	**[I]**	**[D]**	**[T]**
[E.28] Indisponibilidad del personal	Personal de recepción, área técnica, administrativa y archivo	10				75%	
	Administrador de sistemas	5				100 %	
[A.5] Suplantación de la identidad del usuario	**Datos / información**	5	75%	75%	75%		
	Claves criptográficas	5	75%	75%	50%		
	Servicios	5	50%	75%	50%		
	Aplicaciones	5	20%	75%	50%		
	Redes de comunicaciones	5	20%	75%	75%		
[A.6] Abuso de privilegios de acceso	**Datos / información**	5		75%	100 %	5%	
	Claves criptográficas	5		75%	50%	5%	
	Servicios	5		50%	50%	75%	
	Equipos Informáticos	50		75%	75%	75%	
	Redes de comunicaciones	10		75%	50%	75%	
[A.7] Uso no previsto	**Servicios**	5		75%	75%	75%	
	Aplicaciones	10		75%	75%	75%	
	Equipos Informáticos	50		75%	75%	75%	
	Redes de comunicaciones	10		75%	75%	75%	
	Soporte de Información	5		20%	20%	20%	
	Equipamiento Auxiliar	5		20%	20%	20%	
	Instalaciones	10		75%	50%	20%	

Relación de amenazas por activo identificando su frecuencia e impacto							
Amenaza	**Activo**	**Frecuencia de la amenaza**	**Impacto para cada Dimensión de seguridad (%)**				
			[A]	**[C]**	**[I]**	**[D]**	**[T]**
[A.8] Difusión de software dañino	**Aplicaciones**	5		50%	75%	75%	
[A.11] Acceso no autorizado	**Datos / información**	10		100 %	75%	50%	
	Claves criptográficas	5		50%	75%	20%	
	Servicios	5		75%	50%	50%	
	Aplicaciones	10		75%	50%	50%	
	Equipos Informáticos	10		75%	20%	75%	
	Redes de comunicaciones	10		75%	20%	75%	
	Soporte de Información	5		20%	20%	20%	
	Equipamiento Auxiliar	5		5%	5%	5%	
	Instalaciones	5		75%	20%	20%	
[A.13] Repudio	**Servicios**	5			50%		75%
[A.14] Interceptación de información (escucha pasiva)	**Redes de comunicaciones**	5		75%			
[A.15] Modificación deliberada de la información	**Datos / información**	5			75%		
	Claves criptográficas	5			75%		
	Servicios	5			75%		
	Aplicaciones	5			75%		
[A.18] Destrucción de información	**Datos / información**	5				100 %	
	Claves criptográficas	5				100 %	
	Servicios	5				100 %	
	Aplicaciones	5				100 %	
	Soporte de la	5				75%	

Relación de amenazas por activo identificando su frecuencia e impacto							
Amenaza	**Activo**	**Frecuencia de la amenaza**	**Impacto para cada Dimensión de seguridad (%)**				
			[A]	**[C]**	**[I]**	**[D]**	**[T]**
	información						
[A.19] Divulgación de información	**Datos / información**	10		100 %			
	Claves criptográficas	5		100 %			
	Soporte de Información	5					
[A.22] Manipulación de programas	**Aplicaciones**	10		100 %	100 %	100 %	
[A.23] Manipulación de los equipos	**Equipos Informáticos**	50		75%		100 %	
	Soportes de Información	5		20%		20%	
	Equipamiento auxiliar	5		5%		5%	
[A.24] Denegación de servicio	**Equipos Informáticos**	5				75%	
	Servicios	5				75%	
	Redes de Comunicación	5				75%	
[A.25] Robo	**Equipos informáticos**	5		75%		100 %	
	Soporte de Información	5		75%		20%	
[A.26] Ataque destructivo	**Equipo Informáticos**	5				100 %	
	Soporte de Información	5				50%	
	Equipamiento Auxiliar	5				50%	
	instalaciones	5				75%	
[A.28] Indisponibilidad del Personal	**Personal**	5				75%	
[A.29] Extorsión	**Personal**	5		75%	75%	75%	
[A.30] Ingeniería	**Personal**	5		75%	75%	75%	

Relación de amenazas por activo identificando su frecuencia e impacto							
Amenaza	**Activo**	**Frecuencia de la amenaza**	**Impacto para cada Dimensión de seguridad (%)**				
			[A]	**[C]**	**[I]**	**[D]**	**[T]**
Social							

4.1.4.4. Salvaguardas

Una vez realizado el inventario de activos, e identificado las amenazas y vulnerabilidades, se definen las salvaguardas que son procedimiento tecnológico que reduce el riesgo, de acuerdo a los activos que se van proteger, en este caso se tiene en cuenta las salvaguardas definidas en Magerit.

Tabla 6: Tipos de salvaguardas según Magerit.

Efecto	Tipo
Preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Fuente: Magerit. V 3.0 Libro 1

4.1.4.4.1 Salvaguardas de Activos esenciales

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des. Salvaguarda
[vr]	Datos vitales	[I_Proyectos]	Información de Proyectos radicados (base de datos y registro de proyectos)	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información – Acceso restringido
				Recuperación (RC)	Copias de Seguridad (por lo menos dos respaldos guardados en sitios seguros)
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Eliminación (EL)	Gestión de contraseñas
		[I_Licencias]	Información de Licencias	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Recuperación (RC)	Copias de Seguridad de los archivos de licencias
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Eliminación (EL)	Gestión de contraseñas

		[I_Normativa]	Información de Normativa (Normas locales, nacionales, POT, acuerdos, decretos, Cartografía)	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
[per]	Datos de Carácter Personal	[I_Contabilidad]	Contabilidad de la empresa	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Recuperación (RC)	Copias de Seguridad de la información de contabilidad
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
[classified]	Datos clasificados	[E_S_Licenciador]	Ejecutable software Licenciador	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Eliminación (EL)	Gestión de contraseñas
		[D_Históricos]	Datos Históricos de proyectos	Preventivas(PR)	Políticas de seguridad para el personal

			radicados		que tiene acceso a la información. Acceso Restringido
				Recuperación (RC)	Copias de Seguridad de datos históricos guardadas en sitios seguros
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
		[D_Proyectos]	Documentación de proyectos tramitados.	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información. Acceso Restringido
				Recuperación (RC)	Copias de Seguridad de datos históricos guardadas en sitios seguros
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información

4.1.4.4.2 Salvaguardas de Datos/Información

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des. Salvaguarda
[files]	Ficheros	[A_proyectos]	Archivos de proyectos radicados	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información. Gestión de privilegios
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Eliminación (EL)	Gestión de contraseñas
		[A_Clientes]	Archivos de Clientes	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información. Gestión de privilegios
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Eliminación (EL)	Gestión de contraseñas
		[A_Contabilidad]	Archivo de Contabilidad	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información. Gestión de privilegios

				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Eliminación (EL)	Gestión de contraseñas
		[A_Informes y Licencias]	Archivos de Informes y licencias expedidas	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información. Gestión de privilegios
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Eliminación (EL)	Gestión de contraseñas
[backup]	Copias de Respaldo	[A_Copias de Seguridad]	Archivo de Copias de seguridad de la información	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información. Gestión de privilegios
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Eliminación (EL)	Gestión de contraseñas
[conf]	Datos de configuración	[D_Configuracion_ser]	Datos de configuración de servidores y equipos	Preventivas(PR)	Políticas de seguridad para el personal que tiene

					acceso a la información. Gestión de privilegios
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Eliminación (EL)	Gestión de contraseñas
[int]	Datos de gestión interna	[D_GestionProyectos]	Datos de Gestión de proyectos radicados	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información. Gestión de privilegios
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Eliminación (EL)	Gestión de contraseñas
[password]	Credenciales	[Pass_usuarios]	Contraseñas de acceso de empleados	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información. Gestión de privilegios
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Eliminación (EL)	Gestión de contraseñas

4.1.4.4.3 Salvaguardas de Claves Criptográficas

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Descripción Salvaguarda
[encrypt]	Claves de cifra	[CC_Aplicaciones_bancarias]	Claves de cifra de aplicaciones bancarias	Preventivas(PR)	Clasificación y Encriptación de la información Gestión de privilegios.
				Minimización (IM)	Detención del servicio en caso de ataque
				Correctivas(CR)	Gestión de incidentes
				Monitorización(Mn)	Registro de descarga
				Detección (DC)	Activación de IDS y Firewall, software de monitorización y escaneo, manejo de antivirus

4.1.4.4.4 Salvaguardas de Servicios

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Descripción Salvaguarda
[ext]	A usuarios externos (bajo una relación contractual)	[S_U_Externo]	Servicios prestados a usuarios externos bajo relación contractual (Clientes de proyectos)	Preventivas(PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios
				Recuperación (RC)	Copias de Seguridad

				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
[int]	Interno (a usuarios de la propia organización)	[S_U_Interno]	Servicios prestados a trabajadores tanto al interior como haciendo uso de internet.	Preventivas(PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios
				Recuperación (RC)	Copias de Seguridad de
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
[www]	World wide web	[S_Internet]	Servicio de internet al que pueden acceder los empleados.	Monitorización(Mn)	Registro de descarga
				Preventivas(PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios
				Recuperación (RC)	Copias de Seguridad de
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
[email]	Correo	[S_correo]	Manejo de	Monitorización(M	Registro de

	electrónico		correos electrónicos	n)	descarga
				Preventivas(PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios
				Recuperación (RC)	Copias de Seguridad de
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
[file]	Almacenamiento de ficheros	[S_A_Bases de datos]	Servicio de almacenamiento de información en el servidor de bases de datos.	Monitorización(Mn)	Registro de descarga
				Preventivas(PR)	Clasificación de la información en este caso catalogada como confidencial. Políticas de seguridad, Gestión de privilegios
				Recuperación (RC)	Copias de Seguridad de
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
[ipm]	Gestión de privilegios	[G_privilegios]	Manejo de privilegios de acuerdo al rol dentro de la empresa y el lugar de	Preventivas(PR)	Clasificación de la información en este caso catalogada como

			donde esté ingresando, considerando el desempeño como teletrabajo.		confidencial. Políticas de seguridad, Gestión de privilegios
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Eliminación (EL)	Eliminación de cuentas sin contraseña

4.1.4.4.5 Salvaguardas de Software – Aplicaciones Informáticas

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Descripción Salvaguarda
[app]	Servidor de aplicaciones	[Server_App]	Servidor de aplicaciones	Preventivas(PR)	Políticas de seguridad, Gestión de privilegios
				Preventivas(PR)	Clasificación de la información en este caso catalogada como confidencial
				Recuperación (RC)	Copias de Seguridad
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
[dbms]	Sistema de gestión de bases de datos	[S_BaseDeDatos]	Gestor base de datos, aplicación destinada a realizar el	Detección (DC)	Activación de IDS y Firewall, software de monitorización y escaneo,

			proceso de gestión de las bases de datos manejadas al interior de la empresa.		manejo de antivirus
				Preventivas(PR)	Políticas de seguridad, Gestión de privilegios
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Monitorización(Mn)	Registro de uso y descarga
				Eliminación (EL)	Eliminación de cuentas sin contraseña
				Correctivas(CR)	Gestión de incidentes
[Oficce]	Ofimática	[Oficce]	Office 2010	Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Monitorización(Mn)	Registro de uso y descarga
				Eliminación (EL)	Eliminación de cuentas sin contraseña
				Preventivas(PR)	Políticas de seguridad, Gestión de privilegios
[av]	Antivirus	[Antivirus]	McAfee original con actualizaciones automáticas.	Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Monitorización(Mn)	Registro de uso y descarga
				Eliminación (EL)	Eliminación de cuentas sin contraseña
				Preventivas(PR)	Políticas de seguridad, Gestión de privilegios
[os]	Sistema operativo	[OS_Win7]	Sistema operativo Windows 7, en su versión professional	Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Monitorización(M	Registro de

			con actualizaciones automáticas activadas.	n)	uso y descarga
				Eliminación (EL)	Eliminación de cuentas sin contraseña
				Preventivas(PR)	Políticas de seguridad, Gestión de privilegios

4.1.4.4.6 Salvaguardas de Equipos Informáticos

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Descripción Salvaguarda
[host]	Grandes equipos (Servidor de bases de datos, servidores de aplicación)	[S_Aplicaciones]	Servidor Aplicaciones	Preventivas(PR)	Políticas de seguridad, Gestión de privilegios
				Eliminación (EL)	Eliminación de cuentas sin contraseña
				Minimización (IM)	Detención del servicio en caso de ataque
				Correctivas(CR)	Gestión de incidentes
				Monitorización(Mn)	Registro de descarga, registro de acceso
				Detección (DC)	Activación de Firewall, software de monitorización y escaneo, manejo de antivirus
				Concienciación (AW)	Capacitación al personal en el manejo.
		[S_Database]	Servidor de Base de Datos	Preventivas(PR)	Políticas de seguridad, Gestión de privilegios
				Eliminación (EL)	Eliminación de cuentas sin

					contraseña
				Minimización (IM)	Detención del servicio en caso de ataque
				Correctivas(CR)	Gestión de incidentes
				Monitorización(Mn)	Registro de descarga, registro de acceso
				Detección (DC)	Activación de Firewall, software de monitorización y escaneo, manejo de antivirus
				Concienciación (AW)	Capacitación al personal en el manejo.
[mid]	Equipos medios (Equipos de trabajo conectados a través de red inalámbrica por red 802.1x)	[PC_trabajadores]	Equipos de mesa	Detección (DC)	Activación de IDS y Firewall, manejo de antivirus
				Preventivas(PR)	Políticas de seguridad, Gestión de privilegios
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Recuperación (RC)	Copias de Seguridad
				Eliminación (EL)	Eliminación de cuentas sin contraseña
				Correctivas(CR)	Gestión de incidentes
[pc]	Equipos que son fácilmente transportados	[PC_portatiles]	Equipos Portatiles	Detección (DC)	Activación de IDS y Firewall, manejo de antivirus
				Preventivas(PR)	Políticas de seguridad, Gestión de privilegios
				Concienciación (AW)	Capacitación al personal en el manejo de la información.

				Recuperación (RC)	Copias de Seguridad
				Eliminación (EL)	Eliminación de cuentas sin contraseña
				Correctivas(CR)	Gestión de incidentes
[print]	Equipos de impresión	[E_Impresoras]	Impresoras	Preventivas(PR)	Políticas de seguridad.
				Correctivas(CR)	Gestión de incidentes
[router]	Enrutadores	[R_enrutadores]	Enrutadores	Preventivas(PR)	Políticas de seguridad, Gestión de privilegios
				Minimización (IM)	Detención del servicio en caso de ataque
				Correctivas(CR)	Gestión de incidentes
				Monitorización(Mn)	Registro de descarga, registro de acceso
				Detección (DC)	Activación de Firewall, software de monitorización y escaneo, manejo de antivirus

4.1.4.4.7 Salvaguardas de comunicaciones

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Descripción Salvaguarda
[wifi]	Red inalámbrica	[R_wifi]	Red Inalámbrica	Preventivas(PR)	Políticas de seguridad, Gestión de privilegios
				Minimización (IM)	Detención del servicio en caso de ataque
				Correctivas(CR)	Gestión de incidentes

				Disuasión (DR)	Guardias de seguridad
[LAN]	Red local	[R_Local]	[LAN]	Preventivas(PR)	Políticas de seguridad, Gestión de privilegios
				Minimización (IM)	Detención del servicio en caso de ataque
				Correctivas(CR)	Gestión de incidentes
				Disuasión (DR)	Guardias de seguridad
[Internet]	Internet	[Internet]	[Internet]	Preventivas(PR)	Políticas de seguridad, Gestión de privilegios
				Minimización (IM)	Detención del servicio en caso de ataque
				Correctivas(CR)	Gestión de incidentes
				Disuasión (DR)	Guardias de seguridad

4.1.4.4.8 Salvaguardas de Soportes de Información _almacenamiento electrónico

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Descripción Salvaguarda
[cd]	Discos	[A_CD]	Almacenamientos en Disco Duro	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Disuasión (DR)	Guardias de seguridad
[cd]	Cederrom (CD_ROM)	[A_CD]	Almacenamiento en CD	Preventivas(PR)	Políticas de seguridad para

					el personal que tiene acceso a la información
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Disuasión (DR)	Guardias de seguridad
[USB]	Memorias	[A_Memorias]	Almacenamiento en Memorias	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Disuasión (DR)	Guardias de seguridad
[dvd]	DVR	[A_DVD]	Almacenamiento en DVD	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Disuasión (DR)	Guardias de seguridad

4.1.4.4.9 Salvaguardas de Soportes de Información _almacenamiento no electrónico

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Descripción Salvaguarda
[printed]	Material impreso	C_Documentaci ónproyecto	Carpetas con la documentació n de cada proyecto(docu mentación, planos, memorias de cálculo y estudios de suelos)	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Disuasión (DR)	Guardias de seguridad
		C_Reporteseinf ormes	Carpetas de reportes e informes impresos	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Disuasión (DR)	Guardias de seguridad
		C_Sop0rtesCont abilidad	Carpetas facturas y soportes contabilidad	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Capacitación al personal en el manejo de la información.

				Administrativas (AD)	Puesta en marcha del Plan Director
				Disuasión (DR)	Guardias de seguridad
		C_varios	Carpetas varios	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Disuasión (DR)	Guardias de seguridad

4.1.4.4.10 Salvaguardas de Equipamiento auxiliar

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Descripción Salvaguarda
[printed]	Sistemas de Alimentación ininterrumpida	U_Computadores	Ups computadores	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Disuasión (DR)	Guardias de seguridad
[suplly]	Suministros Esenciales	Esenciales	Suministros esenciales tales como: Papel, sobres, carpetas, tinta,	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la

			etc.		información
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Disuasión (DR)	Guardias de seguridad
Mobiliario	M_Mobiliario	Mobiliario: Estantes, armarios, escritorios, archivadores, etc.	Mobiliario	Preventivas(PR)	Políticas de seguridad para el personal que tiene acceso a la información
				Concienciación (AW)	Capacitación al personal en el manejo de la información.
				Administrativas (AD)	Puesta en marcha del Plan Director
				Disuasión (DR)	Guardias de seguridad

4.1.4.4.11Salvaguardas de Instalaciones

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Descripción Salvaguarda
[building]	Edificio	[E_empresa]	Edificio de la empresa (Curaduría)	Disuasión (DR)	Guardias de seguridad
				Detección(DC)	Detección de Incendios

4.1.4.4.12 Salvaguardas - Personal

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Descripción Salvaguarda
[ui]	Usuarios	[E_personal]	Personal de	Concienciación	Cursos de

	internos		recepción, área técnica, administrativa y archivo	(AW)	capacitación y entrenamiento
				Administrativas (AD)	Puesta en marcha del Plan Director
[adm]	Administradores de sistemas	[A_sistemas]	Administrador de sistemas	Concienciación (AW)	Cursos de capacitación y entrenamiento
				Administrativas (AD)	Puesta en marcha del Plan Director

4.1.4.5. Informe de Calificación del Riesgos. Teniendo en cuenta el análisis de riesgos se puede observar que existen activos de la Curaduría Urbana Segunda de Pasto que presentan riesgos catalogados como críticos y su probabilidad de frecuencia es alta tal es el caso de los equipos informáticos, datos e información, este riesgo puede generar perdida de la información, divulgación de la información confidencial, daño en equipos y servidor, manipulación y daños en la base de datos, propagación de virus y el cese de actividades de la empresa.

Referente a los activos de redes de comunicaciones (routers e acceso inalámbrico), software y aplicaciones informáticas también se puede decir que el riesgo es catalogado como crítico, el cual puede ser causado por errores de usuarios y de administrador; de allí la importancia de establecer políticas de seguridad encaminadas a proteger los activos de la organización y minimizar los riesgos para que en caso de presentarse el impacto sea mínimo.

Condiciones inadecuadas de temperatura y humedad, corte del suministro eléctrico, avería de orden físico y lógico y amenazas como manipulación no autorizada de equipos puede ocasionar daños en las aplicaciones, en el servidor y los equipos que pueden originar perdida de información vital, y retraso en el otorgamiento de licencias urbanísticas.

Deficiencias en la organización por parte del personal de recepción área técnica administrativa y archivo, abuso de privilegios de acceso y uso no previsto son amenazas que se deben de tener en cuenta ya que de acuerdo al análisis de riesgos están catalogadas como importantes y pueden ocasionar grandes daños a la empresa.

Por otra parte los impactos generados por los desastres naturales como fuego e inundaciones son críticos en el caso de que se llegasen a presentar afortunadamente la posibilidad de que ocurra es muy baja, esto no quiere decir que no se deba de tener en cuenta al contrario también se debe considerar como

una posibilidad y se debe establecer políticas y medidas de seguridad encaminadas a minimizar cada riesgo.

En este orden de ideas los activos con mayor necesidad de ser protegidos son: Equipos informáticos, datos e información, software y aplicaciones, redes de comunicación puesto que son vulnerables y blanco fácil de los atacantes.

De que se los debe proteger: Del uso no previsto, del abuso de privilegios, fallos en los servicios de comunicaciones, errores de usuarios y administradores del sistema, condiciones inadecuadas de seguridad, contaminación electromagnética y mecánica etc.

Como se los debe proteger: Definiendo e implementando políticas de seguridad que permitan capacitar al usuario y al administrador en el manejo y clasificación de la información, gestión de contraseñas, control de acceso, implementación de equipos y software que permitan mejorar la seguridad, seguridad física y lógica, actualizaciones permanentes del software, elaboración permanente de backups. Etc.

4.1.4.6. ¿Cómo quedarían reducidos los riesgos de seguridad a los que está expuesta el área de informática de la Curaduría Urbana Segunda de Pasto? Una vez realizado el análisis de riesgos para los activos de la Curaduría Urbana Segunda de Pasto y teniendo en cuenta los resultados obtenidos, se procede a especificar las políticas y objetivos de la seguridad del área de informática, teniendo como guía la norma ISO/IEC-27002.

Políticas y controles que se definen y se pretender implementar en cada dependencia con el fin de minimizar los riesgos encontrados.

4.1.4.6.1 Políticas y objetivos de seguridad del área de informática. Generalidades: La información actualmente es considerada como uno de los activos más importante de una empresa por lo tanto se puede decir que la seguridad de la misma es un pilar fundamental que contribuye al logro de la misión y cumplimiento de los objetivos en este caso de la Curaduría Urbana Segunda de Pasto que es prestar un servicio eficiente y de calidad en el otorgamiento de licencias urbanísticas.

Objetivo: Definir políticas de seguridad para el área de informática de la Curaduría Urbana Segunda de Pasto, que sirvan como estrategias de apoyo para lograr disminuir riesgos, evitar incidentes, mantener la confidencialidad, brindar un servicio eficiente y de calidad en el otorgamiento de licencias urbanísticas, manteniendo permanentemente una excelente imagen corporativa.

Alcance: Esta política se debe aplicar a todos los procesos y dependencias relacionados con el área de informática de la Curaduría Urbana Segunda de Pasto.

Responsables: La responsabilidad de la seguridad de la información está en cabeza del Curador Urbano, seguida por el responsable de la seguridad y el responsable del mantenimiento y todo el equipo de trabajo; es decir todos los empleados que hacen parte de la organización.

Para la aplicación de estas políticas de seguridad el Curador Urbano debe designar un responsable de seguridad informática y sistemas de información, un responsable de la seguridad de la información, responsable de recursos humanos, responsable del área legal y administrativa, los cuales conformaran el comité de seguridad.

- **Comité de seguridad de la información: Tiene las siguientes funciones** presentar al Curador la aprobación de las políticas de seguridad, monitorear riesgos y amenazas, plantear modificaciones en las políticas de seguridad, velar y controlar que sean cumplidas por todos los empleados de la Curaduría. Este comité debe elegir un coordinador que se encargara de coordinar las acciones de dicho comité y presentar solicitudes de modificaciones y requerimiento para la aprobación del Curador.

- **Comité de Revisión Interna o Control Interno**: Responsable de practicar auditorias periódicas sobre el manejo de los sistemas de información y la aplicación de las políticas de seguridad, estas deben estar debidamente documentas y son las responsables de encontrar fallas y brindar soluciones para corregir dichas fallas

- **Responsable del Área de Informática y de la seguridad informática:** Cumple la función de documentación, mantenimiento, actualización y gestión de políticas de seguridad para todos los recursos tecnológicos de la organización (Hardware, software, red, servidores etc) y se encarga de supervisar el cumplimiento de las políticas de seguridad,

- **Responsable de la Información y sistemas de información:** Es el encargado de clasificar la información de acuerdo a su grado de confidencialidad y definir los permisos de acceso a los usuarios, además se encargara de controlar, documentar y almacenar toda la información de la empresa, elaborar y almacenar copias de seguridad.

- **Responsable de Recursos Humanos:** Es el encargado de divulgar las políticas de seguridad y la obligatoriedad del cumplimiento de las mismas por todos los empleados de la empresa. Si se generan cambios este se encargara de divulgar dichos cambios.

- **Responsable del Área Legal y Administrativa:** Responsable del cumplimiento de todas las políticas de seguridad en todos los contratos laborales.

- **El propietario de la información**: Responsable de conocer y cumplir con todos los requerimientos y políticas de seguridad estipuladas por la empresa y encargado de contribuir con la confidencialidad, disponibilidad e integridad de la información

Política: Esta política define aspectos específicos y pautas sobre la seguridad para el área de informática de la Curaduría Urbana Segunda de Pasto tales como:

- **Organización de la seguridad**: Su objetivo es guiar la administración y dirección de la seguridad para su posterior implementación.
- **Clasificación y Control de Activos**: Su objetivo es clasificar jerárquicamente los activos de la organización y protegerlos de manera apropiada.
- **Control de Acceso:** Su objetivo es controlar y restringir el acceso a la información que es vital para la organización o es catalogada como confidencial.
- **Desarrollo y mantenimiento de los sistemas:** Su objetivo es implementar medidas de seguridad en el desarrollo (confidencialidad, copias de seguridad, acceso restringido), implementación y mantenimiento de los sistemas de información.
- **Administrador de Operaciones:** Su objetivo es contrarrestar las interrupciones en los procesos productivos, solucionar fallas y desastres.
- **Seguridad de los usuarios:** Su objetivo es reducir el riesgo que generan los errores humanos y también velar por la buena utilización de las instalaciones. (Capacitación permanente y adecuada para disminuir errores producidos por un manejo incorrecto o por desinformación)
- **Seguridad Física:** Su objetivo es impedir el acceso no autorizado y evitar daños y robos en la empresa. (Proteger tanto la planta)
- **Cumplimiento:** Su objetivo es hacer cumplir las políticas de seguridad anteriormente establecidas y hacer cumplir las obligaciones establecidas por las leyes, el reglamento, los contratos e imponer sanciones por incumplimiento de las mismas
- **Recursos**: La empresa en cabeza del Curador cada año debe disponer de un rubro destinado a la seguridad de la información.

4.1.4.6.2 Organización de la Seguridad de la Información

Generalidades: Establecer la seguridad de la información como una de los objetivos vitales para la Curaduría.

Objetivo: Organizar, controlar y administrar la información dentro de la organización.

Alcance: Esta política se debe aplicar a todos los procesos de la Curaduría Urbana Segunda de Pasto tanto internos como externos.

Responsables: La responsabilidad de la organización de seguridad de la información está en cabeza del Curador, seguida por director del comité de seguridad de la información y todos sus miembros así:

- **Comité de seguridad de la información:** Es el encargado de desarrollar la implementación de las políticas de seguridad. Se encargara de realizar seguimiento, monitoreo, análisis de riesgo, implementación de controles, velar por la continuidad y hacer conocer de los avances, cambios y dificultades a la dirección general.
- **Responsable del Área de Informática y de la seguridad informática:** Se encargara de dirigir la implementación de políticas de seguridad con la asesoría de profesionales especializados, e implementar medidas de seguridad como la restricción del acceso a la información que sea catalogada como confidencial
- **El comité de revisión Interna o control Interno**: Se encargara de revisar la vigencia y el cumplimiento de las políticas de seguridad.
- **Responsable del área de Administración**: Se encarga de destinar y disponer de recursos necesario para la adquisición de elementos necesarios para el cumplimiento de dichas políticas (Hardware, software, elementos de logística, asesoría especializada)
- **Responsable del Área Legal y Administrativa:** Responsable de informar a proveedores, y equipo de trabajo sobre las modificaciones en las políticas de seguridad.

Política: Infraestructura de la seguridad de la información

- **Organización Interna y coordinación de la seguridad de la información de la Curaduría Urbana Segunda de Pasto**: Crear un comité de seguridad de la información que garantice el apoyo a la implementación de todas las medidas de seguridad estructurado de la siguiente forma.

Tabla 8: Comité de Seguridad de la información

Comité de seguridad de la información	
Área o dependencia	Representante
Curador – Gerencia	
Responsable de la seguridad de la información	
responsable de recursos humanos	
responsable del área legal y administrativa	

Fuente: Modelo de política de seguridad para organismo de la administración pública nacional

- **Funciones del comité de seguridad:**

  - ✓ Revisar y proponer políticas de seguridad al director general.
  - ✓ Monitorear e identificar cambios que generen riesgos para la organización
  - ✓ Identificar amenazas y posibles vulnerabilidades.
  - ✓ Documentar y monitorear los incidentes concernientes a la seguridad
  - ✓ Evaluar las posibles soluciones y elegir la más adecuada encaminada a contribuir con la seguridad de la información.
  - ✓ Asegurase de que la seguridad haga parte del procesos de planificación de la organización
  - ✓ Determinar y organizar la implementación de controles de seguridad

- **Asignación de responsabilidades para la seguridad de la información:** El Curador asigna las funciones referentes a la seguridad informática al responsable del departamento de seguridad informática quien de ahora en adelante será el directo garante de la seguridad de la información de la empresa y responsable del cumplimiento de lo tratado en la presente política.

Asignación de responsabilidades, que deben quedar debidamente documentadas y aprobadas por el comité de seguridad de la información de acuerdo a la siguiente tabla.

Tabla 9: Asignación de responsables para la seguridad de la información

Proceso	Responsable
Control de Acceso	
Seguridad Física (industrial)	
Seguridad de la Información	
Seguridad de Usuarios (personal)	
Seguridad del software	
Seguridad de las comunicaciones (red y servidores)	
Seguridad en el desarrollo y mantenimiento de sistemas	
Seguridad Operacional	

Fuente: Modelo de política de seguridad para organismo de la administración pública nacional

Tabla 10: Encargados de la seguridad de la Información en la Organización

Información	Propietario	Recursos Asociados	Procesos Involucrados	Administrador

Fuente: Modelo de política de seguridad para organismo de la administración pública nacional

- **Proceso de autorización para los servicios de procesamiento de información:** Los nuevos servicios de procesamiento de información deben ser autorizados previamente por el responsable de la seguridad de la información y deben ser autorizados para el usuario apropiado; de igual manera al implementar hardware y software se debe verificar que sean compatibles con el sistema actual e identificar e implementar controles de seguridad para portátiles y computadores personales nuevos que ingresan a la empresa.

- **Acuerdos sobre confidencialidad:** Identificar y revisar con regularidad los requisitos de confidencialidad (suscribir contratos de confidencialidad y no divulgación para la protección de la información vital para la empresa.), que deben ser encaminados a proteger la información legalmente, para lo cual se debe tener en cuenta la clasificación de la información, en este caso se debe proteger la información confidencial, se debe definir por cuánto tiempo se va a proteger y designar un responsable para hacer buen uso de esta.

- **Contactos con las autoridades:** La organización debe mantener contactos adecuados con las autoridades que especializadas en seguridad y delitos informáticos para comunicarse de manera inmediata en caso de ser necesario. (Saber cuándo y a quién dirigirse en caso de incidentes)

- **Contactos con grupos de interés especiales:** Los responsables de la seguridad deben estar en contacto permanente con foros y empresas especializadas en seguridad ya que estos están a la vanguardia de las nuevas formas de ataque.

- **Revisión independiente de la seguridad de la información:** El comité de revisión interna o control interno se encargara de realizar revisiones independientes para garantizar el cumplimiento de las políticas de seguridad. Este comité debe informar al curador de las fallas encontradas y de las mejoras y cambios que son necesarios implementarse. (La revisión la deben realizar profesionales idóneos o expertos en seguridad, de ser necesario se debe contratar personal externo para realizar dicha revisión)

- **Partes externas y coordinación de la seguridad de la información:** Se debe controlar todo acceso a los servicios, comunicación, procesamiento de la información y comunicación que provienen de partes externas así:

  - ✓ Se debe definir un convenio con la parte externa para compartir información
  - ✓ Se deben identificar los riesgos provenientes de las partes externas e implementar controles adecuados antes de autorizar el acceso.
  - ✓ Identificar los servicios de los que va disponer la parte externa.
  - ✓ Definir el tipo de acceso que va a tener la parte externa: ya sea acceso físico, acceso lógico, acceso a la red etc.
  - ✓ Identificar el valor y la sensibilidad de la información a la que van a tener acceso
  - ✓ Implementar controles necesarios para proteger la información de terceros
  - ✓ Conocer los controles y medidas que implementara la parte externa para el manejo y uso de la información
  - ✓ Definir unos requisitos legales que está obligada a cumplir la parte externa para compartir información y servicios.
  - ✓ Establecer y definir posibles medidas de contingencia en caso de fallos, errores, ataques etc.,
  - ✓ Todo servicio con terceros se debe hacer mediante contrato y en cada contrato se deben definir claramente las obligaciones, las políticas de seguridad y las implicaciones legales en caso de incumplimiento.

Estas medidas deben ser tomadas para: Proveedores de servicios de red, de internet, de telefonía, de mantenimiento, de soporte, de auditoria, de gestión, de negocios, personal de trabajo temporal, clientes etc.

4.1.4.6.3 Gestión de Activos

Generalidades: Una vez realizado el inventario de activos y la evaluación de riesgos se clasifican los activos de acuerdo a su sensibilidad y vulnerabilidad.

Objetivo: Clasificar la información de acuerdo a su grado de confidencialidad, definir niveles de protección y garantizar que los activos de la organización sean protegidos de manera adecuada

Alcance: Esta política se debe aplicar a todos los activos de la organización.
Responsables: La responsabilidad de la seguridad de la información está en manos de:

- **Responsables de la Información:** Son los encargados de clasificar la información de acuerdo a su grado de confidencialidad, mantener actualizada y documentada la clasificación y de definir los permisos de acceso a los

usuarios. Cada dependencia debe supervisar que la clasificación y rotulado de la información sea correcto.

Política

- **Inventario de Activos:** Se realiza un inventario de activos los cuales debe estar debidamente clasificados y ordenados según su importancia, propietario, ubicación e información almacenada, este inventario debe ser actualizado constantemente y conservarse de manera ordenada.

- **Clasificación de la información:** Para clasificar la información de deben tener en cuenta los criterios básicos de seguridad:

Tabla 11: Clasificación de la Información

Categoría	Nivel de Confidencialidad:
0	Información pública: Que puede ser conocida por todo el personal interno y externo.
1	Reservada de uso interno (información que solo puede ser conocida por los miembros de la empresa).
2	Información reservada confidencial (información que solo es conocida por un grupo de la empresa).
3	Reservada secreta (información que solo es conocida por un grupo reducido de la empresa y su divulgación ocasionaría problemas o perdidas).
Categoría	**Nivel de Integridad:**
0	Si la información, es modificada sin previa autorización esta puede repararse y no afecta a la organización
1	Si la información es modificada sin previa autorización esta puede repararse , pero puede ocasionar perdidas leves
2	Si la información es modificada sin previa autorización esta no puede repararse y ocasiona pérdidas significativas a la organización.
3	Si la información es modificada sin previa autorización esta no puede repararse y ocasiona pérdidas graves a la organización
Categoría	**Nivel de Disponibilidad:**

0	Hace referencia a cuya información en caso de no poderse acceder, no afecta los procesos y servicios de la organización.
1	Hace referencia a cuya información que en caso de no poderse acceder en un plazo largo como una semana, puede ocasionar pérdidas significativas a la empresa
2	Hace referencia a cuya información que en caso de no poderse acceder en un plazo corto como un día, puede ocasionar pérdidas significativas a la empresa
3	Hace referencia a cuya información que debe estar disponible todo el tiempo y la inaccesibilidad mayor a una hora puede ocasionar pérdidas significativas a la empresa
Criticidad baja: ninguno de los valores asignados superan el **Criticidad media**: alguno de los valores asignados es 2 **Criticidad alta**: alguno de los valores asignados es 3	

Fuente: Modelo de política de seguridad para organismo de la administración pública nacional.

Teniendo en cuenta los anteriores criterios el propietario se encarga de clasificarla e identificar los elementos asociados:

- **Rotulado de la información:** Definir procedimientos de rotulado, almacenamiento y físico y electrónico de la información de acuerdo a su Nivel De Criticidad.

4.1.4.6. 4 Seguridad de los recursos humanos

Generalidades: Es fundamental educar y concienciar al personal sobre la importancia de la aplicación de las políticas de seguridad, desde el primer instante que se ingresa a la empresa y de las sanciones que conlleva el incumplimiento de las mismas. Por lo tanto es importante que el personal este consiente de la importancia, este capacitado y en caso de ocurrir un incidente informar en qué condiciones ocurrió para establecer mecanismos que conduzcan a que dichas fallas o incidentes no vuelvan a ocurrir y establecer los correctivos necesarios.

Objetivo: Minimizar los riesgos ocasionados por errores humanos y promover un uso adecuado de los recursos informáticos así como capacitar y concienciar sobre la importancia de la aplicación de las políticas de seguridad e información oportuna de incidentes para ser corregidos en debida forma.

Alcance: Esta política se debe aplicar a todo el personal de la organización, interno y externo

Responsables:

- **El personal de recursos humanos** que es el encargado de seleccionar el personal, informara, capacitara y establecerá acuerdos de confidencialidad y de cumplimiento de todas las políticas de seguridad con el personal que ingrese a la empresa.

- **Responsable del Área Legal y Administrativa:** Es el responsable de establecer términos y condiciones laborales. Mediante cláusulas en los contratos los acuerdos de confidencialidad y cumplimiento de políticas de seguridad con todo el personal y con terceros.

- **Responsable de la seguridad informática:** Se encargara de capacitar y concienciar al personal con asesoría de profesionales especializados, sobre el uso correcto de los recursos informáticos y el cumplimiento de las políticas de seguridad así como del acuerdo de confidencialidad.

Política

- **Antes de la contratación Laboral:** La organización antes de la contratación laboral debe documentar los roles y responsabilidades que estos van a desempeñar.

  En la selección del personal se debe revisar antecedentes (hoja de vida, experiencia laboral, experiencia crediticia etc.). Se debe seleccionar y clasificar que información va estar disponible para estos tanto para personal como para terceros.

  Términos y condiciones laborales: Tanto para empleados como para terceros estos deben conocer los términos y las condiciones del contrato laboral haciendo énfasis en los aspectos relativos a la seguridad, la confidencialidad y se debe verificar que los contratos estén firmados. (El contrato debe contener, derechos, deberes, responsabilidades, estar de acuerdo a la ley y posibles sanciones por incumplimiento).

- **Durante la Vigencia del contrato:** La dirección debe exigir que los empleados y terceras partes cumplan a cabalidad con las políticas de seguridad establecidas por la empresa. Para esto debe darles a conocer las

políticas de seguridad, motivarlos y verificar que estén de acuerdo con los términos y condiciones establecidas en el contrato laboral.

Capacitación y formación: La organización capacitara e informara sobre las políticas de seguridad establecidas en la organización, así mismo capacitara e informara cuando se presenten cambios y modificaciones.

La capacitación al personal y a terceras partes se realizara por personal especializado de la organización que resalte la importancia del cumplimiento de las políticas de seguridad y les enseñe como detectar posibles fallas e incidentes y les explique cómo comunicar estas fallas a la organización.

La organización lleva a cabo verificaciones del cumplimiento de las obligaciones en los puestos de trabajo.

El empleado debe someterse a: Cumplir con el control y la política de seguridad, formar y cumplir el compromiso de confidencialidad, cumplir los términos y condiciones del contrato, capacitarse, comunicar sobre incidentes y anomalías.

Para el personal y terceras partes que violen o incumplan las políticas de seguridad se llevara a cabo un proceso disciplinario de acuerdo a los estatutos de la empresa.

- **Terminación o Cambio del contrato laboral:** La organización gestiona de manera adecuada la terminación del contrato o cambio de contrato y una vez terminado el contrato verifica la suspensión de los servicios, la devolución de los activos, devolución de documentos, dispositivos (pc, celulares, usb etc), verifica y gestiona el cambio de contraseñas. Los responsables de realizar estos procesos son l responsable de seguridad y el área de recursos humanos.

4.1.4.6.5 Seguridad física y del entorno

Generalidades: Para la seguridad física se deben tener en cuenta los siguientes aspectos: La protección física de acceso, protección y mantenimiento de equipos de acuerdo a su importancia, los posibles daños e interferencias; El mantenimiento de las instalaciones se debe hacer bajo estrictas normas de seguridad.

Objetivo: Evitar el daño, interferencias y el acceso no autorizado a la información de la empresa.

Alcance: Esta política se debe aplicar la instalaciones de la Curaduría y todos sus equipos, expedientes, cableados, documentación etc.

Responsables:

- **Responsable de la seguridad informática: Este s**e encargara de dirigir las políticas a seguir en el resguardo de los equipos, su mantenimiento y control de acceso etc. También se encargara de clasificar las áreas (Para servidores se creara un área restringida que tendrá un tratamiento especial).
- **El Responsable del Área informática** se encargara de adoptar todas las políticas establecidas por el responsable de la seguridad y verificara el cumplimiento de las mismas.

Política

- **Perímetro de Seguridad Física:** El comité de seguridad con el responsable de seguridad definen un perímetro de seguridad para el área considerada como crítica que si no existen se debe crear (almacena todos los dispositivos considerados vitales como servidores y almacenamiento de información confidencial) y se deben adoptar las siguientes medidas:

  - ✓ Definir claramente el perímetro de seguridad
  - ✓ Establecer barreras de seguridad
  - ✓ Definir el personal autorizado para el acceso al área restringida.

- **Controles de Acceso Físico:** El responsable de la seguridad junto con el responsable del área de informática establecerán controles de acceso al área restringida:

  - ✓ Limitar el acceso al área donde se encuentra almacena la información, llevar un registro solo del personal autorizado.
  - ✓ Verificar que el personal que ingrese porte un documento visible que lo catalogue como personal autorizado.
  - ✓ Revisar periódicamente los registros del personal que accede.
  - ✓ Actualizar constantemente la lista de personal autorizado.

- **Seguridad de Oficinas e instalaciones;** Se debe tener en cuenta las condiciones de iluminación ventilación salubridad, equipamiento antiincendios, medidas que prevengan inundaciones robos etc. Preferiblemente el área de oficinas y atención al público debe estar alejada del área restringida, disponer de guardias de seguridad y de alarmas.

- **Ubicación y protección de copias de seguridad y equipamiento**: El equipamiento se ubicara en un sitio donde se minimice el riesgo, es decir en

un lugar aislado y protegido tanto de amenazas naturales ambientales, físicas y humanas, adicional a esta medida se restringirá el acceso. Por lo tanto solo podrá acceder personal autorizado con su credencial y los ingresos y tareas a realizar serán debidamente documentadas por el responsable de la seguridad; las labores de aseo serán verificadas para evitar daños y hurtos.

- **Suministro de Energía**: Periódicamente se deben revisar el buen funcionamiento de las instalaciones eléctricas para evitar incidentes, la organización debe optar por contrarrestar fallas en el suministro de energía tales como la adquisición de una planta eléctrica, la compra de ups para los pc etc.

- **Seguridad en el Cableado**: Proteger el cableado que transporta datos de daños e interceptación cumpliendo con las normas, que el cableado baya por conductos seguros, separa los cables de energía de los cables de comunicación etc.

- **Mantenimiento de Equipos**: Los responsables del área de informática deben someter todos los equipos periódicamente e mantenimiento preventivo, este mantenimiento debe ser registrado y documentado, cada equipo debe tener un inventario de dispositivos para saber qué cambio se hicieron y que dispositivos se retiraron.

- **Seguridad en la reutilización o eliminación de equipos**: Cuando un equipos es cambiado de sitio o eliminado se debe tener total precaución con los dispositivos de almacenamiento como discos duros los cuales deben ser formateados o destruidos de forma segura para evitar incidentes con la información.

4.1.4.6.6 Gestión de operaciones y comunicaciones

Generalidades: La Curaduría debe crear condiciones que garanticen la confidencialidad, integridad y disponibilidad de la información que se produce y se recibe a través de diferentes canales de comunicación.

Objetivo: Adoptar medidas de seguridad encaminadas a prevenir la proliferación y expansión de software malicioso que son catalogadas como amenazas en potencia, garantizar el adecuado funcionamiento de los sistemas de información y designar responsables encargados de adoptar todas las medidas de seguridad necesarias para prevenir posibles ataques

Alcance: Esta política se debe aplicar a todo el sistema informático (red, servidores, comunicaciones y equipos) etc.

Responsables:

- **El responsable de la seguridad informática:** Sera el encargado de definir procedimientos para el control actualización y modificación de los sistemas operativos tanto de servidores como pcs.

  - ✓ Toda actualización, modificación y mantenimiento debe estar debidamente documentada
  - ✓ Definir mecanismos para el reporte y manejo de incidentes
  - ✓ Definir políticas de control para el uso de correo electrónico, consulta de páginas, navegación en internet y uso de redes sociales.
  - ✓ Adquirir antivirus licenciado y verificar que las actualizaciones se estén realizando periódicamente.
  - ✓ Establecer y verificar políticas de control de usuarios mediante contraseñas y gestión de privilegios.
  - ✓ Controlar la realización de copias de seguridad
  - ✓ Solicitar recursos para actualizaciones (Software) para cubrir necesidades a futuro en materia de seguridad.
  - ✓ Adquirir herramientas de monitoreo de sistemas y verificar que estén siendo utilizadas para tal fin
  - ✓ Establecer protocolos para la destrucción de herramientas de almacenamiento, como discos duros, cintas, usb (en el caso de ya no ser necesarias)
  - ✓ Todo procedimiento debe ser debidamente documentado.

- **El Responsable del Área informática** se encargara de adoptar todas las políticas establecidas por el responsable de la seguridad y verificara el cumplimiento de las mismas.

- **El responsable del área legal,** junto con el responsable de la seguridad y el responsable de área informática se encargaran de verificar y hacer cumplir a cabalidad los contratos y acuerdos.

Política

- **Procedimientos y responsabilidades operativas**

  - ✓ **Documentación de los procedimientos operativos:** Los S.O. se actualizarán permanentemente y toda actualización y modificación de los S.O. será autorizada por el responsable de seguridad y debidamente documentada y realizada por el área de informática.

- ✓ **Control de Cambios en las Operaciones:** Todo cambio debe ser evaluado y aprobado previamente y se tendrán en cuenta los siguientes aspectos: Evaluación del cambio y posible impacto, planificación, prueba, e identificación de responsabilidades en caso de que el cambio sea fallido.
- ✓ **Procedimientos de Manejo de incidentes:** El responsable de la seguridad junto con el jefe del área de informática establecerán protocolo para el manejo de incidentes tales como: Definir los posibles tipos de incidentes (Fallas operativas, código malicioso, intrusiones, fraude informático, error humano, desastres naturales). En caso de presentarse incidentes comunicarlos a la dirección y seguir el plan de contingencia, implementar controles de acceso a los sistemas y medidas de recuperación.

- **Planificación y Aprobación de sistemas**

  - ✓ **Planificación de la Capacidad:** El responsable del área de seguridad informática es el encargado de evaluar constantemente las necesidades a futuro de los S.O. para evitar posibles fallas.
  - ✓ **Aprobación del sistema:** El responsable de la seguridad y el responsable del área informática sugieren a la dirección las posibles especificaciones necesarias para actualizar los sistemas Operativos.

- **Protección Contra software malicioso:** El responsable de la seguridad y el responsable del área de informática definen los siguientes criterios de seguridad y el cumplimiento de los mismos:

  - ✓ Prohibir las instalaciones y descargas en los pc de la empresa.
  - ✓ Verificar constantemente el contenido del software
  - ✓ Escanear constantemente el software
  - ✓ Monitorear constantemente el software de los servidores
  - ✓ Antes de realizar instalaciones o cambios verificar que toda información entrante esté libre de virus
  - ✓ Concientizar al personal de la importancia de la protección en el manejo de la información.

- **Mantenimiento**

  - ✓ **Resguardo de la información:** Los responsables de la información definirán un esquema de protección de la información entre ellas: Copias de seguridad y prueba de restauración, definir un esquema de rotulado de copias, almacenar copias de seguridad en una ubicación remota, el

almacenamiento de copias de seguridad debe estar físicamente protegida con un esquema de seguridad especial.

- ✓ **Registro de actividades del personal operativo:** El responsable de seguridad debe llevar un registro del uso de los sistemas como: Tiempo de inicio, cierre, errores del sistema, intentos de acceso al sistema, medidas tomada etc

- ✓ **Registro de fallas:** El responsable de seguridad debe llevar un registro fallas en los sistemas, como fueron resueltas, medidas correctivas etc (documentar todas las fallas de los sistemas)

- **Administración de la Red:** El responsable de la seguridad define y toma las medidas necesarias para proteger la red de datos para evitar posibles daños, interferencias etc.

  - ✓ Establece procedimiento de administración y delega un responsable que debe documentar todos los procedimientos realizados en la red
  - ✓ Establecer controles para asegurar la disponibilidad, la confidencialidad y la integridad de la información.
  - ✓ Garantizar mediante actividades de supervisión que los controles se apliquen.

- **Administración de medios de almacenamiento:** El responsable de la seguridad y el responsable del área de informática establecerán y verificaran el cumplimiento del correcto almacenamiento de respaldos de seguridad y eliminación de información de cintas magnéticas, discos duros para evitar incidentes con el manejo de la información.

  - ✓ **Eliminación de medios de información:** El responsable de la seguridad y el responsable del área de informática deben verificar la correcta eliminación de información desde dispositivos de almacenamiento.

  - ✓ **Procedimientos de manejo de información:** Para almacenar la información los empleados deben seguir el siguiente procedimientos tales como: Proteger documentos, redes y dispositivos informáticos, restringir el acceso a personal no autorizado, conservar los dispositivos de almacenamiento en medios seguros.

  - ✓ **Seguridad de la documentación del sistema:** La documentación del sistema debe estar almacenada en un lugar seguro y el acceso a esta debe ser restringido.

- **Intercambios de Información y de Software:** Se debe utilizar medios de mensajería confiable, se deben de tener en cuenta las siguientes recomendaciones: Uso adecuado por de la mensajería electrónica por parte del personal, no abrir mensajes de remitentes desconocidos, toda información que llega debe ser escaneada, se debe conocer los posibles riesgos de seguridad a los que se enfrenta un usuario al utilizar mensajería electrónica (interceptación, robo, engaños, bombas lógicas etc.) y transferir por este medio información confidencial.

4.1.4.6.7 Control del Acceso

Generalidades: La política de control debe ser documentada, revisada y actualizada constantemente con el fin de evitar el acceso a los sistemas de información, bases de datos y documentos por personal no autorizado que pongan en peligro la información de la empresa.

Objetivo: Controlar el acceso a la información

Alcance: Esta política se aplica a todas los procesos o formas de acceso a los sistemas de información, bases de datos o servicios de información de la empresa.

Responsables:

- **Responsable de la seguridad informática:** Es el encargado de definir normas, pautas y procedimientos para los accesos a los sistemas, bases de datos y servicios de información (acceso a los pc, acceso a la red, acceso a los servidores, acceso a internet, acceso a claves de seguridad, acceso a transacciones etc.). También debe realizar un control de los privilegios de los usuarios y concientizar a los usuarios de la importancia de la no divulgación de las contraseñas
- **El Responsable del Área informática S**e encarga de dirigir normas y procedimientos para implementar Sistemas operativos, Gateway, firewall, servicios de red etc., debe verificar que todos estos dispositivos y servicios queden debidamente configurados, debe realizar pruebas de escaneo, monitoreo para evitar intromisión. Además debe promover y realizar la gestión de contraseñas y privilegios, capacitar y concientizar a los usuarios de la utilización de las medidas de control de acceso.

Política

- **Política de Control de acceso:** El responsable del área de informática cumplirá con las siguientes funciones:

  - ✓ Implementar métodos de autenticación y control de acceso
  - ✓ Segmentar la red (adquirir enrutadores y gateways)
  - ✓ Implementar el control de puertos y ruteo de red
  - ✓ Efectuar un control de los registros de auditoria.
  - ✓ Definir perfiles de acceso
  - ✓ Controlar los cambios en los accesos

- **Administración de accesos de usuarios**

  - ✓ **Registración de usuarios:** Definir un registro formal de usuarios para otorgar y revocar accesos, utilizar identificadores de usuarios únicos.
  - ✓ **Administración de Privilegios:** Identificar los privilegios, asignar los privilegios de acuerdo a las necesidades del trabajo, mantener un registro actualizado de los privilegios.
  - ✓ **Administración de contraseñas de usuario:** Los usuarios deben comprometerse a utilizar y mantener en secreto sus contraseñas esto debe estar estipulado en el contrato laboral, cambiar periódicamente las contraseñas, las contraseñas deben cumplir con todos los criterios de seguridad.
  - ✓ **Administración de contraseñas críticas:** Para realizar configuraciones, asignaciones y cambios en los servidores, enrutadores etc., se utilizara contraseñas con un nivel de complejidad más alto

- **Responsabilidad de los usuarios:** Los usuarios deben usar contraseñas, deben mantener la contraseña en secreto, pedir cambio de contraseña en caso de riesgo, usar contraseñas de calidad etc. El usuario está obligado a proteger los equipos asignados, no debe dejar los equipos abandonados o desatendidos, una vez terminado un servicio debe cerrar cesión, cerrar cesión después de utilizar correos electrónicos, apagar el equipo en forma correcta.

- **Control de acceso a la red:** El responsable de la seguridad informática es el encargado de otorgar los permisos para el acceso a la red y sus recursos, realizar normas y procedimientos de autorización, establecer controles y procedimientos de control de acceso, para autenticación de usuarios para conexiones externas debe de escogerse un método de autenticación, un protocolo de autenticación, a autenticar las conexiones a sistemas informáticos remotos, protección de puertos para evitar accesos no autorizados, en lo posible subdividir o segmentar la red para realizar procesos separados con el fin de que si se presenta un incidente no se contamine toda la red o si un espía ingresa a esta no tenga acceso a toda la información, por otra parte se debe controlar el acceso lógico a los servicios, configurar los servicios de manera segura etc. El acceso a internet solo será autorizado por el jefe del área de informática.

  Se debe restringir algunos servicios como: Utilización de correo electrónico, transferencias de archivos, acceso interactivo y acceso a red fuera del horario laborar.

- **Control de Acceso al sistema operativo:** Los responsables de la seguridad y el jefe del área de informática deben definir los procedimientos para realizar la protección de los sistemas operativos, el acceso a los servicios de información solo se realizara a través de un proceso de conexión seguro, limitar el tiempo para el procesos de conexión, limitar el número de intentos de conexión; todos los usuarios utilizaran contraseñas seguras.

- **Control de Acceso a las aplicaciones:** Controlar los derechos los acceso de los usuarios, restringir la información, controlar el acceso a las funciones de los sistemas, revisar las salidas de información es decir que solo se envié la información solicitada.

- **Monitoreo de acceso y uso de los sistemas:** Revisar y monitorear que los usuarios solo estén realizando actividades que hayan sido autorizadas previamente, se debe monitorear, el acceso, la identificación de usuarios, fecha y hora de eventos, archivos accedidos, se debe supervisar el inicio y cierre del sistema, las operaciones con privilegios, cambios de configuración del sistema, intentos de acceso no autorizado, alertas fallas del sistema etc.

4.1.4.6.8 Adquisición, desarrollo y mantenimiento de sistemas de información

Generalidades: Se debe documentar y aprobar los requerimientos de seguridad a aplicar en la implementación de los sistemas de información; se debe llevar a cabo adecuadas políticas de seguridad para las bases de datos, los sistemas

operativos, todo esto con el fin de evitar que personas conocedoras de los procesos puedan cometer fraudes o ilícitos y si es el caso identificarlos de manera inmediata.

Objetivo: Adoptar medidas de seguridad en la implementación de los sistemas de información.

Alcance: Esta política se debe aplicar a todos los sistemas informáticos tanto sistemas operativos como software requerido para la entidad.

Responsables:

- **Responsable de la seguridad informática, el propietario de la información y el área de auditoria interna** se encargaran de definir e implementar controles en el desarrollo y mantenimiento de sistemas de información.

- **El Responsable del Área informática** se encargara de definir el procedimiento para asignar claves, de garantizar el cumplimiento de los requisitos de seguridad del software, de controlar los cambios en los sistemas etc.

- **El responsable del área legal y administrativa,** se encargara del licenciamiento del software adquirido y en el caso del software desarrollado por la organización de establecer las políticas de derechos de autor y fijar las condiciones de los contratos y de entrega.

Política

- **Requerimientos de seguridad de los sistemas:**

  - ✓ **Análisis y especificaciones de los requerimientos de seguridad:** Identificar y definir los requerimientos y controles necesarios en materia seguridad desde las etapas de análisis y diseño del sistema ya que implementar medidas de seguridad desde estas etapas sale menos costoso que hacerlo después.

  - ✓ **Seguridad en los sistemas de aplicaciones:** Se debe establecer controles de los registro de auditoria para evitar la pérdida de los datos de los sistemas de información (validación y autenticación de los datos de entrada y de salida)

  - ✓ **Validación de datos de entrada:** Se debe establecer un control de validación de los datos de entrada como: Revisión periódica de contenidos

de campos claves, se debe establecer como se realizara y con qué método, además se definirá las responsabilidades del personal.

- ✓ **Controles de procedimientos interno:** El responsable de la seguridad junto con el jefe del área de sistemas deben establecer controles para la etapa del diseño, se deben implementar procedimientos que permitan identificar el uso y localización en los aplicativos, controles y verificaciones, revisión periódica de los registros, controles de integridad de los registros y de los archivos, controles que verifique la consecución y orden en la ejecución de los aplicativos.

- ✓ También se deben implementar controles para la autenticación de mensajes y para la validación de datos de salida.

- **Controles criptográficos**

  - ✓ **Política controles criptográficos:** Se debe utilizar controles criptográficos para los siguientes casos: Protección de claves de acceso a sistemas, datos y servicios, transmisión de información clasificada, resguardo de información. El responsable de la seguridad se encargara de definir la política de controles criptográficos, el método y el responsable de administración de claves (Uso de algoritmo de cifrado y firma digital, servicios de no repudio)

  - ✓ **Administración de claves:** El responsable de administrar las claves debe aplicar las políticas de protección de las claves implementando un sistema de administración de claves criptográficas que permitan usar técnicas de clave secreta, estas claves serán protegidas contra copia, destrucción, divulgación, modificación etc**.**

- **Seguridad de los procesos de soporte**

  - ✓ **Procedimiento de control de cambios:** Verificar que los cambios sean propuestos por personal autorizado, mantener un registro del nivel de autorización, identificar todos los elementos que requieren modificaciones, obtener aprobación por parte del responsable del área de informática para cumplir con los requerimientos del software.

  - ✓ **Revisión técnica de los cambios en el sistema operativo:** Antes de realizar cambios en el sistema operativo se debe revisar y verificar que

los cambios son necesarios, que impacto genera, informar al área involucrada y verificar la continuidad del negocio.

- ✓ **Restricción del cambio de paquetes de software:** Se debe evaluar la necesidad, los costos, la parte legal (licencias) y el impacto del cambio que este genera en la organización

- ✓ **Canales ocultos y código malicioso:** Se debe adquirir software a personal confiable y conocido, examinar códigos fuentes que estén libres de virus, llevar un control de acceso al software y las modificaciones instaladas, utilizar antivirus y software de monitoreo y escaneo.

- ✓ **Adquisición de software:** Para la adquisición de software a terceros se deben establecer condiciones puntuales rigurosas tales como: acuerdos de licencias, procedimientos certificación de calidad, calidad en el software, verificación del cumplimiento de las condiciones de seguridad.

4.1.4.6.9 Gestión de los incidentes de seguridad de la información

Generalidades: Todos los empleados de la curaduría deben tener muy clara la obligación de reportar formalmente fallas, eventos y debilidades de manera inmediata al responsable de la seguridad.

Objetivo: Garantizar que todos los eventos maliciosos, como fallas y debilidades de la seguridad de la información sean comunicados de manera inmediata.

Alcance: Esta política la deben cumplir todos los empleados de la Curaduría.

Responsables:

- **Responsable de la seguridad informática:** El responsable de la seguridad debe establecer un protocolo el cual deben conocer todos empleados para conozcan cual es el procesos a seguir en caso de presentarse una falla. Es decir cómo y a quien reportarlo para que se tomen los correctivos necesarios.

- **El Responsable del Área informática** debe concientizar y capacitar a los empleados para que estén atentos a eventos sospechosos y en caso de presentarse los reporten de inmediato.

Política

- **Reportes sobre los eventos de seguridad de la información:** Se debe establecer un punto de contacto que siempre esté disponible y brinde respuesta oportuna y adecuada a los incidentes. Todos los empleados deben estar informados sobre la obligatoriedad de reportar e informar sobre incidentes, fallas, vulnerabilidades y debilidades observadas en el sistema (los empleados para reportar los incidentes deben diligencian un formato).

- **Gestión de incidentes y las mejoras en la seguridad de la información:** La organización en cabeza del responsable de la seguridad establece procedimientos para el manejo de eventos y debilidades de la seguridad. Se debe evaluar y gestionar todos los incidentes de seguridad de la información así:

  - ✓ **Responsabilidades y procedimientos:** Establecer procedimientos para manejar eventos como: Fallas en el sistema, virus, negación del servicio, violación de confidencialidad, integridad y disponibilidad, uso inadecuado de los sistemas informáticos, código malicioso; identificar la causa, implementar acciones correctivas y reportar todo el procesos realizado al responsable de la seguridad.

  - ✓ **Aprendizaje debido a los incidentes de seguridad informática:** El responsable del área de informática, debe llevar un registro de los incidentes presentados, de cómo se han manejado, las posibles causas y cuanto le cuestan a la empresa resolverlos, para en un futuro no cometer los mismos errores.

  - ✓ **Recolección de Evidencia:** En el caso de llevar a cabo una acción disciplinaria, se debe recolectar la evidencia siguiendo las siguientes pautas: No se debe manipular la evidencia, se debe crear una copia intacta de la evidencia y esta debe ser resguarda a través de una cadena de custodia.

4.1.4.6. 10 Gestión de la continuidad del negocio

Generalidades: Es indispensable que toda empresa disponga de un procesos de gestión de continuidad del negocio en caso de llegarse a presentar una eventualidad como un desastre natural, robo, daños en los servidores etc.

Objetivo: Asegurar el funcionamiento continuo de la organización

Alcance: Esta política se debe aplicar a todos los procesos críticos y prioritarios de la empresa.

Responsables:

- **El comité de seguridad junto con el responsable de la seguridad informática** debe identificar las amenazas, evaluar los riesgos identificar controles preventivos, desarrollar un plan estratégico y un plan de contingencia.
- **El Responsable del Área informática** participara en la elaboración y documentación del plan de contingencia.

Política

- **Proceso de la administración de la continuidad de la empresa:** El comité de la seguridad será el encargado de identificar los procesos críticos, asegurarse de que todos los empleados de la empresa comprendan y conozcan los riesgos, elaborar y documentar una estrategia de continuidad del negocio y proponer la adquisición de pólizas y seguros

- **Continuidad de las actividades y análisis de los impactos:** Antes de elaborar el plan de contingencia el comité de seguridad debe identificar los eventos o amenazas, evaluar los riesgos e identificar controles preventivos. Todo esto debe estar debidamente documentado.

- **Elaboración e implantación de los planes de continuidad de las actividades de la empresa:** El comité de seguridad junto con el responsable de la seguridad debe elaborar el plan de contingencia que debe contemplar los siguientes aspectos: Responsables de los procedimientos de emergencia, definir acciones y correctivos, implementar procedimientos de emergencia, documentar estos procedimientos e instruir al personal; actualizar constantemente el plan de contingencia.

- **Marco para la planificación de la continuidad de las actividades de la empresa:** Se debe especificar claramente los requisitos y condiciones para su puesta en marcha, los responsables y los requerimientos etc. Adicionalmente debe prever las condiciones de implementación, definir los procedimientos de emergencia, y las acciones a realizarse, describir los procedimientos de recuperación, definir un cronograma de mantenimiento y documentar las responsabilidades y funciones de las personas. (elaborar un documento muy completo del plan de contingencia.)

- **Ensayo, mantenimiento y reevaluación de los planes de continuidad de la empresa:** El comité de seguridad establecerá un cronograma de pruebas, el cronograma señalara quienes son los responsables, efectuara pruebas, realizara simulaciones y pruebas completas en las instalaciones, involucrando procesos y con todo el personal.

4.1.4.6. 11 Cumplimiento

Generalidades: Todas las empresas deben cumplir con las obligaciones estipuladas por la ley.

Objetivo: Cumplir con todas las obligaciones estipuladas por la ley

Alcance: Esta política se debe aplicar a todo el personal de la empresa.

Responsables:

- **Responsable de la seguridad informática:** Este se encargara de definir procedimientos encaminados a cumplir con todas las normas y restricciones legales, se encargara de realizar revisiones periódicas a la empresa para verificar el cumplimiento de las políticas de seguridad, solicitar auditorias periódicas, documentar y dar a conocer los requisitos normativos.
- **Todos los empleados y directivos** están obligados a conocer y dar a conocer a cumplir y hacer cumplir la presente política y la normativa vigente.

Política

- **Cumplimiento de requisitos legales:**

  - ✓ **Identificación de la legislación aplicable**: Se definirán claramente los requisitos normativos contractuales.

  - ✓ **Derechos de propiedad intelectual**: Solo se podrá utilizar material autorizado, respetando la propiedad intelectual.

  - ✓ **Derecho de propiedad intelectual del software**: El responsable de la seguridad junto con el responsable del área de informática implementar controles y procedimientos para el manejo de licencias.

  - ✓ **Protección de los registros de la empresa**: Los registros críticos serán debidamente protegidos contra pérdida, falsificación o robo. Para el almacenamiento y protección de los registros contables, base de datos y

otros de estos se debe realizar un inventario, implementar controles, y establecer procedimientos de almacenamiento, divulgación, manipulación o eliminación.

- ✓ **Protección de datos:** Todos los empleados están obligados a cumplir un compromiso de confidencialidad es decir a utilizar la información solo para bien de la Curaduría.

- ✓ **Prevención del uso inadecuado de los recursos de procesamiento de información:** Cuando un empleado utilice la información o los recursos de la organización sin ser autorizado será considerado como uso indebido y esto va en contra de las normas de la empresa y puede estar sujeto a sanciones.

- ✓ **Regulación de controles para el uso de criptografía:** Para hacer usos de herramientas criptográficas el responsable del área legal junto con el responsable del área de seguridad deben cumplir con las leyes de firma digital y encriptación vigentes en el país, una vez conozcan las normas de uso, se implementan los controles y se dan a conocer al encargado.

- ✓ **Recolección de Evidencia:** Cuando una acción indebida o inapropiada involucre la aplicación de la ley, la evidencia presentada debe cumplir con lo establecido en las leyes que rigen a nuestro país.

  Para la recolección de la evidencia se debe cumplir con las siguientes condiciones: Realizar una copia de seguridad para que la evidencia original no sea modificada, guardar la evidencia en un sitio seguro.

- **Revisión de las políticas de seguridad y la compatibilidad técnica**

  - ✓ **Cumplimiento de las políticas de seguridad:** El responsable del área de informática realizara revisiones del cumplimiento de las políticas de seguridad en la empresa.

  - ✓ **Verificación de la compatibilidad técnica:** El responsable de la seguridad revisara que los controles para el hardware y el software sean implementados correctamente.

- **Auditorías de sistemas**

  - ✓ **Controles de auditoria de sistemas:** Cuando se realicen auditorías a los sistemas, el responsable de la seguridad debe definir el área a

auditar, controlar el alcance de las comprobaciones, limitar la auditoria para evitar modificaciones.

- ✓ **Protección de los elementos utilizados por la auditoria de sistemas:** El responsable de la seguridad debe definir instrucciones y procedimientos para el acceso archivos, datos o software.

- **Sanciones previstas por incumplimiento**: El incumplimiento o violación de las políticas de seguridad implica sanciones, de acuerdo a los contratos suscritos con la empresa y en caso de acciones legales se procederá de acuerdo a la ley.

4.1. 4.2 Segunda Etapa – Implantar

4.1.4.2.1. Declaración de Aplicabilidad. En la declaración de aplicabilidad (Dda) se define como se implementaran los sistemas de seguridad de la información, ya que este documento aplica la relación entre la calificación y el tratamiento del riesgo y la implementación de un sistema de seguridad de la información y es un documento fundamental desde donde parte una auditoria.

Para la declaración de aplicabilidad de la Curaduría Urbana Segunda de Pasto, se ha tenido en cuenta los siguientes documentos: Los 133 controles sugeridos en el Anexo A de la norma ISO 27001, las política de Seguridad de la Información, la evaluación y tratamiento de riesgos y el Informe de evaluación y tratamiento de riesgos.

Una vez identificados los riesgos la declaración de aplicabilidad permite identificar los controles necesarios documentando si cada uno de estos controles es aplicable o no o si ya está implementado o no.

La declaración de aplicabilidad se realizó sobre el análisis de riesgos teniendo en cuenta los siguientes parámetros:

- Dominio: Que indica el número del control de acuerdo al anexo A de la Norma ISO/IEC 27001.
- Controles según la ISO/IEC 27001: Se identifica el nombre del control
- Aplicabilidad: Se identifica si es o no es aplicable a la Curaduría.
- Justificación: Explica porque es o no es aplicable dicho control.
- Objetivo del Control
- Actividades para la implementación del control
- Estado del control.

El estado del control se lo identifica y clasifica con la siguiente tabla teniendo en cuenta la abreviatura y el color

Tabla 12: Estado de los Controles

Estado	Abreviatura	Color
Planificado [No implementado]	(P)	Rojo
Parcialmente implementado	(PI)	Amarillo
Totalmente implementado	(TI)	Verde
No aplica	(NA)	Sin Color

Fuente: Basado en Magerit

4.1. 4.2.2. Aplicabilidad de los Controles

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
5	Políticas de seguridad					
5.1	Políticas de seguridad de la información.					
5.1.1	Documentos de políticas de seguridad de la información	Si	La implementación de las políticas de seguridad debe estar debidamente documentada y para que sirva como guía en la implementación del SGI	Garantizar que los procedimientos para el manejo de la información sean conocidos por los miembros de la Curaduría.	Documentación de todos los procesos a desarrollarse para la implementación de la seguridad	P
5.1.2	Revisión de políticas para seguridad de la información	Si	Es necesario revisar seguidamente las políticas de seguridad para verificar el cumplimiento de las mismas	Garantizar que las políticas de seguridad de la información se mantengan actualizadas.	Revisión de las políticas de seguridad de la información.	P
6	Aspectos organizativos de la seguridad de la información					
6.1	Organización interna					

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
6.1.1	Compromiso de la dirección con la seguridad de la información	Si	Cada trabajador debe conocer cuáles son sus responsabilidades frente al manejo de la información en la Curaduría para asumirlas de manera adecuada, además debe conocer a fondo el rol que desempeña.	Garantizar que sólo personas dentro de cierta jerarquía dentro de la empresa tengan acceso a la información.	Políticas de gestión de privilegios.	PI
6.1.2	Coordinación de la seguridad de la información	Si	Es importante que cada empleado que labora en la Curaduría conozca su límite en el manejo de la información	Garantizar que sólo personas idóneas tengan acceso a la información.	Políticas de seguridad para el personal que maneja la información al interior de la empresa.	PI
6.1.3	Asignación de las responsabilidades relativas a la seguridad de la información	Si	Los empleados de la Curaduría que tiene acceso a la información deben contribuir de manera exhaustiva al mejoramiento de la seguridad dentro de la empresa	Garantizar que las políticas de seguridad de la información estén acordes con los requerimientos y exigencias del entorno.	Planes de capacitación para el personal a cargo del manejo de la información.	PI
6.1.4	Procesos de autorización de recursos para el tratamiento de la información	Si	Toda información nueva que ingrese a la Curaduría debe ser protegida bajo los parámetros y políticas de seguridad (software nuevo, programas, bases de datos etc.)	Garantizar la protección de la información de nuevos clientes y proyectos que llega a la empresa.	Políticas de seguridad para nuevos activos de información.	PI
6.1.5	Acuerdos de confidencialidad	Si	Se deben definir acuerdos de confidencialidad para el manejo de la información que deben quedar establecidos en el contrato laboral o en los contratos de prestación de servicios.	Garantizar el adecuado manejo de la información en todos los niveles de acceso a la misma.	Acuerdos de confidencialidad para los empleados de la empresa.	PI

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
6.1.6	Contacto con las autoridades	Si	La información debe ser manejada de acuerdo a las políticas de seguridad y a través de canales de comunicación seguros para evitar incidentes.	Evitar fallas en los canales de comunicación para el manejo de la información.	Definir canales seguros para el manejo de la información.	PI
6.1.7	Contacto con los grupos de especial interés	Si	Para el cumplimiento de los objetivos y alcances del SGSI se deben definir políticas internas para la protección de la información que deben ser conocidas por todos los empleados de la Curaduría.	Estandarizar el manejo de la información a nivel interno.	Políticas para el manejo de la información al interior de la organización.	PI
6.1.8	Revisión independiente de la seguridad de la información	Si	Se debe definir de qué manera serán adoptadas y modificadas las políticas de seguridad cuando se presenten cambios en los activos de la empresa (nuevos programas, nuevos servicios etc.)	Dinamizar las políticas de seguridad para que se ajusten a los nuevos activos que entran a formar parte de la empresa.	Políticas pensadas en futuros activos que formaran parte de la empresa.	P
6.2	Terceros					
6.2.1	Identificación de los riesgos derivado del acceso a terceros	No	Es necesario identificar los posibles riesgos asociados a los accesos otorgados a la información entidades externas o a terceros, considerando el uso de aplicaciones web y portales electrónicos.(cuando se de la conectividad con planeación y se haga uso de un servidor web)	Identificar los riesgos asociados al acceso a la información y sistemas de información por parte de terceros.	Controles de acceso a la información redundantes.	NA
6.2.2	Tratamiento de la seguridad en la relación con los clientes	No	Es necesario que los terceros que necesiten acceder a la información conozcan bajo qué condiciones pueden tener acceso a la información.	Brindar lineamientos a la hora de que un clienta requiera tener acceso a la información.	Controles de seguridad para clientes externos.	NA

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
6.2.3	Tratamiento de la seguridad en contratos con terceros	No	Cualquier convenio o acuerdo realizado con otra entidad como planeación que implique la relación con los activos internos (información) de la curaduría deben garantizar el cumplimiento de requisitos de seguridad.	Establecer controles de seguridad para el acceso a activos internos de la empresa por parte de terceros.	Políticas para el manejo de acuerdos que impliquen la relación con información interna de empresa.	NA
7	Gestión de Activos					
7.1	Responsabilidad sobre los activos					
7.1.1	Inventario de activos	Si	Es importante identificar los activos de acuerdo a su grado de importancia dentro de la Curaduría, en la que se deja claro que el activo más relevante es la base de datos donde se registran los proyectos, el archivo de licencias y el archivo físico.	Jerarquizar la importancia de los activos al interior de la empresa.	Clasificación de los activos y establecimiento del nivel de importancia de los mismos.	P
7.1.2	Propietario de activos	Si	Cada activo dentro de la Curaduría debe tener relacionado un responsable de la seguridad.	Tener responsables de los activos que forman parte de la empresa.	Asignar responsables tanto para los activos de información a través del área de gestión de proyectos, como para activos físicos que forman parte de los sistemas de información.	TI

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
7.1.3	Uso aceptable de los activos	Si	Las políticas sobre manejo de la información deben permitir tener claridad acerca del manejo adecuado de activos.	Definir políticas para el manejo de activos.	Políticas de manejo de activos.	PI
7.2	Clasificación de la información					
7.2.1	Directrices de clasificación	Si	La información debe ser clasificada de acuerdo a su grado de importancia para establecer los controles adecuados para el manejo de la misma.	Identificar el nivel de importancia de los activos de información al interior de la empresa.	Establecimiento de prioridades en el manejo de la información.	PI
7.2.2	Etiquetado y manipulado de la información	Si	Cada tipo de información debe ser identificado para que cada persona conociendo su naturaleza respete su nivel de confidencialidad, es decir debe ser etiquetada relacionando sus restricciones.	Identificar el nivel de confidencialidad y acceso a la información.	Políticas de acceso a la información.	PI
8	Seguridad en los recursos Humanos					
8.1	Seguridad antes del empleo					
8.1.1	Funciones y responsabilidades	Si	Antes de contratar personal es necesario definir claramente el perfil y responsabilidades del cargo.	Contratar personal idóneo para ocupar un cargo determinado.	Claridad en las políticas de contratación.	P

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
8.1.2	Investigación de antecedentes.	Si	Para contratar al personal se deben evaluar las cualidades profesionales, el nivel de ética y compromiso con la empresa.	Garantizar en los nuevos empleados tanto cualidades profesionales específicas como principios éticos.	Claridad en las políticas de contratación.	TI
8.1.3	Términos y condiciones de contratación.	Si	Es necesario que los nuevos empleados conozcan políticas y responsabilidades en cuanto a sus funciones y manejo de la información	Establecer las reglas que debe seguir quien desee formar parte de la empresa.	Claridad en las políticas de contratación.	P
8.2	Seguridad en el desempeño de las funciones al interior de la empresa					
8.2.1	Responsabilidades de la dirección	Si	Se debe asegurar que las políticas diseñadas para el manejo de la información sean cumplidas por los empleados de la Curaduría	Garantizar que los empleados usen las políticas definidas por la empresa.	Definición de políticas de manejo de la información, acompañadas de planes de capacitación.	PI
8.2.2	Concienciación, formación y capacitación en seguridad de la información	Si	Todas las políticas de seguridad de la información deben ser conocidas al interior de la Curaduría.	Dar a conocer las políticas de seguridad de la información.	Planes de capacitación en políticas de seguridad de la información.	PI

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
8.2.3	Proceso disciplinario.	Si	Las posibles sanciones por incumplimiento de las políticas de seguridad o el mal manejo de la información que pongan en riesgo la seguridad de la información deben ser conocidas por todos los empleados de la Empresa.	Dar a conocer las sanciones que acarrea el mal manejo de la información.	Planes de capacitación en políticas de seguridad de la información.	P
8.3	Finalización o cambio de empleo					
8.3.1	Responsabilidad del cese o cambio	Si	Es necesario garantizar que después de la finalización de un contrato interno, la información que maneja esta persona no se vea afectada o divulgada.	Evitar impacto negativo en la información tras la salida de un empleado que tenga conocimiento sobre la misma.	Implementación de políticas de manejo de privilegios sobre la información.	P
8.3.2	Devolución de activos	Si	Se deben tener protocolos que garanticen que un empleado haga entrega de los activos que tiene a su cargo.	Garantizar que los activos no se vean afectados tras la salida de un empleado de la empresa.	Implementación de mecanismos para la devolución de activos.	TI
8.3.3	Retirada de los derechos de acceso	Si	Se debe contar con procedimientos para revocar privilegios a personal que no requiera de los mimos.	Evitar niveles de acceso a la información inadecuados, que pongan en riesgo la seguridad de la misma.	Implementación de políticas de manejo de privilegios sobre la información.	PI
9	Seguridad física y del ambiente					
9.1	Áreas Seguras					

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
9.1.1	Perímetro de seguridad física.	Si	Se debe garantizar la seguridad de las zonas que manejan información sensible (archivo físico, ubicación de servidores, equipos, almacenamiento copias de seguridad etc).	Asegurar las áreas que contengan información sensible.	Políticas de control de acceso físico a áreas que contienen información sensible.	PI
9.1.2	Controles físicos de entrada.	Si	Sólo personal autorizado debe acceder a áreas que contengan activos sensibles. (Archivo histórico físico, almacenamiento de copias de seguridad, uso de servidor).	Restringir el acceso a áreas que contengan información sensible.	Políticas de control de acceso físico a áreas que contienen información sensible.	PI
9.1.3	Seguridad de oficinas, despachos e instalaciones.	Si	En oficinas al interior de la Curaduría se puede tener acceso a información sensible por lo cual se debe aplicar controles de seguridad	Garantizar la seguridad en oficinas y despachos.	Políticas de control de acceso físico.	PI
9.1.4	Protección contra las amenazas externas y de origen ambiental.	Si	Se debe garantizar que ninguna amenaza ambiental externa pueda generar daño sobre la información.	Garantizar la protección contra amenazas ambientales externas.	Protección contra factores atmosféricos como temperatura, humedad, etc.	PI
9.1.5	Trabajo en áreas seguras.	Si	Las áreas sobre las que se desarrollan las actividades deben cumplir estándares de seguridad lo cual es muy importante tanto para equipos como para el personal.	Garantizar el desarrollo de las actividades sobre áreas seguras.	Verificación del nivel de seguridad de las áreas de trabajo.	PI

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
9.1.6	Áreas de acceso público y de carga y descarga.	Si	Las áreas como archivo histórico y ubicación de servidores se denominan áreas sensibles por la información que maneja, por tanto se debe evitar que terceros puedan llegar a tener acceso a esta.	Garantizar que el acceso a áreas sensibles dentro de la empresa tenga mecanismos de control.	Control de acceso físico a determinadas áreas de la empresa.	PI
9.2	Seguridad en equipos					
9.2.1	Emplazamiento y protección de equipos.	Si	Es necesario tener protecciones contra daños ambientales, especialmente para los servidores que se maneja al interior de la empresa.	Garantizar la integridad de los equipos al interior de la empresa.	Implementar controles para el control de factores ambientales como humedad, polvo, etc.	PI
9.2.2	Instalaciones de suministro.	Si	La integridad de los equipos depende de los controles para la protección antes fallas eléctricas, ya un fallo de energía puede dejar inutilizable un equipo, dañar su disco duro etc.	Garantizar que fallos eléctricos no afecten la integridad de los equipos que forman parte del sistema de información.	Implementar UPS.	PI
9.2.3	Seguridad del cableado.	Si	Se debe garantizar que las redes de datos no vean afectada su integridad y confidencialidad de los datos que transportan.	Garantizar que las redes de datos no sean alteradas físicamente y no puedan ser interceptados los datos que se transportan a través de estas.	Implementar y auditar los sistemas de cableado existentes.	TI
9.2.4	Mantenimiento de los equipos.	Si	Se debe realizar mantenimiento periódico de los equipos como política interna de la empresa.	Garantizar la integridad y disponibilidad de los equipos.	Implementar planes de mantenimiento de equipos al interior de la empresa	PI

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
9.2.5	Seguridad de los equipos fuera de las instalaciones.	No	Todo equipo que trabaje fuera de la empresa pero tenga injerencia interna debe tener reglas y restricciones de acceso.	Garantizar la seguridad al interior de la empresa al permitir acceso a equipos que trabajen fuera.	Aplicar controles de acceso a equipos externos que tengan que ver directamente con la actividad de la empresa (Acceso remoto derivado del teletrabajo)	NA
9.2.6	Reutilización o retirada segura de equipos.	Si	Al dar de baja un equipo puede quedar almacenada información que puede comprometer la confidencialidad de la empresa.	Garantizar que ningún dato sensible o licencia sean expuestos a terceros tras un proceso de baja de equipos.	Establecer políticas para el proceso de baja de equipos.	TI
9.2.7	Retirada de materiales propiedad de la empresa.	Si	Tanto las aplicaciones propias como de terceros que la empresa utiliza deben ser protegidas para evitar que puedan ser sacadas de la empresa.	Garantizar que ningún tipo de aplicación salga de la empresa.	Establecer políticas sobre el manejo de aplicaciones y licencias al interior de la empresa.	TI
10	Administración de comunicaciones y operaciones					
10.1	Procedimientos y responsabilidades operacionales					

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
10.1.1	Documentación de los procedimientos de operación.	Si	Para garantizar la continuidad de procesos se debe contar con bitácoras que permitan conocer los procedimientos operacionales especialmente los que tengan que ver con activos esenciales.	Garantizar la documentación de procesos operacionales.	Políticas para la documentación de procedimientos.	P
10.1.2	Gestión de cambios.	Si	Se debe tener claridad de quienes serán los encargados de realizar el proceso de administración de la información.	Gestionar los cambios de roles encargados de la administración de la información.	Implementación de políticas de manejo de privilegios sobre la información.	P
10.1.3	Segregación de tareas.	Si	Sólo el personal autorizado debe tener acceso a la información.	Garantizar que un número reducido de personas tengan acceso a la información.	Implementación de políticas de manejo de privilegios sobre la información.	PI
10.1.4	Separación de los recursos de desarrollo, prueba y operación.	Si	Cada área dentro de la empresa debe ser separada de acuerdo a sus funciones y competencias.	Reducir los riesgos de acceso no autorizado a la información.	Implementar controles de acceso a áreas seguras.	TI
10.2	Supervisión de los servicios prestados por terceros					
10.2.1	Provisión de servicios	No	Cualquier servicio subcontratado debe contar con políticas de seguridad de la información.	Garantizar que los servicios prestados por terceros cumplan con requerimientos mínimos de seguridad.	Definir políticas para la integración y control de sistemas de terceros al interior de la empresa.	NA

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
A.10.2.2	Supervisión y revisión de los servicios prestados por terceros.	No	Cualquier servicio prestado por terceros debe ser controlado internamente mediantes procesos de autoridad.	Garantizar la calidad en la prestación de servicios ofrecidos por tercero.	Definir políticas para la integración y control de sistemas de terceros al interior de la empresa.	NA
A.10.2.3	Gestión del cambio en los servicios prestados por terceros.	No	Cualquier cambio en los servicios prestados por terceros debe ser monitoreado constantemente.	Garantizar que los cambios en la prestación de servicio sean acordes con las necesidades y requerimientos de la empresa.	Definir políticas para la integración y control de sistemas de terceros al interior de la empresa.	NA
A.10.3	Planificación y aceptación del sistema					
A.10.3.1	Gestión de capacidades.	Si	Es importante que dentro de las políticas internas sea planificado el crecimiento de la empresa para que los recursos sean acordes con el mismo.	Garantizar que los recursos con los que cuenta la empresa sean acordes con los requerimientos de la misma.	Planificación de recursos acordes con las necesidades y proyecciones de crecimiento de la empresa.	TI
10.3.2	Aceptación del sistema.	Si	Se debe definir la capacidad de integración de nuevos elementos al sistema, ya sea por actualización, renovación o totalmente nuevos.	Garantizar la compatibilidad de nuevos elementos en cuanto a sus dimensiones físicas y lógicas que garanticen la seguridad de la información.	Definición de políticas para la integración de nuevos elementos al sistema de información.	P
10.4	Protección contra software malicioso y código móvil.					

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
10.4.1	Controles contra el código malicioso.	Si	Se deben tener controles que garanticen que códigos maliciosos no terminen afectando el sistema.	Garantizar la seguridad en contra de amenazas lógicas al sistema de información.	Implementar mecanismos de seguridad para garantizar el control lógico al interior de la empresa (Antivirus, sistemas de encriptación y manejo de aplicaciones seguras).	TI
10.4.2	Controles contra el código descargado en el cliente.	No	Por seguridad no se autoriza el uso de código móvil.	NA	NA	NA
10.5	Gestión interna de soportes y recuperación					
10.5.1	Copias de seguridad de la información.	Si	Respaldar la información garantiza que ante cualquier problema de seguridad se tendrá una fácil recuperación de la información. bases de datos, archivo de licencias, archivo de contabilidad, archivo de manejo técnico, bases de datos de clientes, ingenieros arquitectos, documentos auxiliares, normativa), de acuerdo con la política de recuperación	Garantizar políticas de respaldo para el manejo de la información.	Backups regulares de la información.	TI
A.10.6	Gestión de redes					
A.10.6.1	Controles de red.	Si	Es necesario que la red inalámbrica que maneja la empresa sea controlada.	Garantizar la protección de las redes contra ataques informáticos.	Definición de políticas de administración y uso de redes.	PI

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
A.10.6.2	Seguridad de los servicios de red.	Si	Deben existir políticas que permitan la definición de acuerdos sobre el manejo de las redes.	Garantizar el uso adecuado de los recursos de red en cada nivel del servicio.	Definición de políticas de administración y uso de redes.	PI
A.10.7	Utilización y seguridad de los soportes de información					
A.10.7.1	Gestión de soportes extraíbles.	Si	No se permite el uso de medios informáticos removibles para evitar fugas y amenazas que puedan contener.	Garantizar que la información no sea extraída por los trabajadores de la empresa	Definición de políticas para que la información no sea extraída	PI
A.10.7.2	Retirada de soportes.	Si	Se debe contar con políticas que permitan eliminar de forma segura los soportes de información de la empresa. (Destrucción segura de elementos desde papel hasta discos duros.)	Evitar que información almacenada en medios que van a ser eliminados pueda quedar expuesta a terceros.	Definir políticas para la gestión y eliminación de medios de almacenamientos.	PI
10.7.3	Procedimientos de manipulación de la información.	Si	Se debe garantizar que la información en cualquier nivel sea manipulada y almacenada de forma segura.	Evitar que malas manipulaciones puedan dejar expuesta la información.	Definir políticas para la manipulación y almacenamiento de información.	TI
10.7.4	Seguridad de la documentación del sistema.	Si	La documentación de los sistemas (información de proyectos y bases de datos) deben ser protegidos.	Garantizas la protección del activo más importante al interior de la empresa.	Definir políticas y sistemas de protección para la documentación de los sistemas de información.	TI
10.8	Intercambio de información y software					

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
10.8.1	Políticas y procedimientos de intercambio de información.	Si	Se debe garantizar que la información se encuentre segura al ser transportada haciendo uso de diferentes servicios de comunicación.	Garantizas la seguridad de la información al ser enviada por diferentes medios de comunicación.	Diseñar políticas e implementar controles para el intercambio seguro de información.	TI
.10.8.2	Acuerdos de intercambio.	Si	Se debe tener claridad de la forma como se puede compartir información al interior de la empresa.	Garantizar el intercambio seguro de información.	Diseñar políticas e implementar controles para el intercambio seguro de información.	TI
10.8.3	Soportes físicos en tránsito.	Si	Se debe proteger la información durante el transporte de la misma	Garantizar la protección de la información al ser transportada.	Implementar mecanismos de protección de información como por ejemplo encriptación (se garantiza con los controles con que cuenta la empresa).	P
10.8.4	Mensajería electrónica.	Si	Se debe proteger la información contenida en correos electrónicos.	Garantizar que la información de mensajería electrónica se encuentre totalmente protegida.	Implementar mecanismos de protección para evitar accesos no autorizados a los servicios de mensajería.	TI
10.8.5	Sistemas de información empresariales.	Si	Todos los sistemas de información tanto internos como externos deben estar conectados de forma segura.	Garantizar la conexión segura entre los sistemas de información.	Políticas para el acceso a la información tanto a nivel interno como externo.	TI
10.9	Servicios de comercio electrónico					

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
10.9.1	Comercio electrónico	Si	De debe garantizar que la información involucrada en comercio sea protegida, por la naturaleza de la empresa esto se puede garantizar.	Proteger la información que usada en comercio electrónico.	Implementación de mecanismos para la protección de la información involucrada en comercio electrónico (Los mecanismos de seguridad de las aplicaciones permiten garantizar esto.)	NA
10.9.2	Transacciones en línea	Si	La información involucrada en procesos de transacciones electrónicas que maneja la empresa por su actividad económica deber ser protegida para evitar problemas de seguridad.	Garantizar la seguridad de la información involucrada en transacciones en línea.	Implementar mecanismos de seguridad para garantizar la seguridad de la información usada en transacciones en línea.	TI
10.9.3	Información públicamente disponible	Si	La información que se maneja por aplicaciones de acceso público debe ser protegida.	Garantizar la integridad de la información disponible en sistemas de acceso público.	Políticas para la verificación de la integridad de sistemas de información de acceso público.	NA
10.10	Monitorización					
10.10.1	Registros de Auditoria	Si	Se deben tener registros de auditorías que permitan facilitar investigaciones futuras en caso de detectarse algún incidente de seguridad.	Contar con soportes de actividades para procesos de investigación asociados a los mismos.	Políticas de implementación y control de registros de actividad.	P

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
10.10.2	Supervisión del usos del sistema	Si	Se debe realizar monitoreo de cualquier cambio en los sistemas de información, revisando sus resultados. Revisar las actividades de monitoreo	Verificar la instalación de sistemas de información.	Políticas de implementación y control de registros de actividad.	P
10.10.3	Protección de la información de los registros	Si	Se debe tener control sobre los registros de actividad para que no puedan ser alterados (intentos forzosos o no autorizados)	Proteger los registros de actividad contra acciones de modificación de los mismos.	Políticas de implementación y control de registros de actividad.	P
10.10.4	Registros de administración y operación.	Si	Es muy importante que la actividad de quienes tengan mayores privilegios sean monitoreados.	Garantizar que las acciones de tipo administrativo se realicen de forma adecuada.	Políticas de implementación y control de registros de actividad.	P
10.10.5	Registro de fallos.	Si	Se debe controlar cualquier avería que se presente en el sistema de información.	Garantizar la trazabilidad de averías en el sistema.	Políticas de control y gestión de fallas en el sistema.	
10.10.6	Sincronización del reloj.	Si	Es muy importante que todos los sistemas estén sincronizados para que cualquier registro coincida en tiempos y se pueda hacer la trazabilidad del mismo.	Garantizar que todo el sistema esté sincronizado.	Políticas de implementación y control de registros de actividad.	P
11	Control de acceso					
11.1	Requisitos de negocio para control de accesos					
11.1.1	Política de control de acceso.	Si	Basado en los servicios que presta la Curaduría que es otorgar licencias urbanísticas, se deben establecer políticas de control de acceso.	Controlar el acceso de acuerdo a las actividades que desarrolla la empresa.	Definir políticas para el control de acceso teniendo en cuenta áreas críticas.	PI

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.2	Gestión de acceso de usuario					
11.2.1	Registro de usuario.	Si	Es importante gestionar los usuarios para que sean asignados y dados de alta en el sistema sin generar problemas de seguridad.	Brindar o quitar acceso a usuarios basado en procedimientos propios de la empresa.	Definir políticas para el ingreso o eliminación de usuarios del sistema.	P
11.2.2	Gestión de privilegios.	Si	Se debe garantizar que cada usuario tenga acceso al sistema de información basado en privilegios.	Controlar los privilegios de acceso.	Definir políticas para la gestión de privilegios.	P
11.2.3	Gestión de contraseñas de usuario.	Si	Debe existir un procedimiento para la asignación de contraseñas al interior de la empresa.	Asignar contraseñas de forma segura.	Establecer políticas para la asignación de contraseñas.	P
11.2.4	Revisión de los derechos de acceso de usuario.	Si	Se debe verificar que los usuarios puedan acceder sólo a los sistemas que tienen permiso.	Verificar el acceso a sistemas de información.	Establecer políticas para la verificación regular del acceso a sistemas de información.	P
11.3	Responsabilidades del usuario					
11.3.1	Uso de contraseñas.	Si	Se debe definir y verificar el uso de contraseñas seguras.	Controlar el uso de contraseñas seguras.	Establecer políticas para que los usuarios realicen un adecuado manejo de los sistemas de información ofrecidos por la empresa.	PI

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.3.2	Equipo de usuario desatendido.	Si	Es importante que los servidores de los clientes tengan mecanismos de protección para los sistemas de la empresa que alojan en los mismos.	Garantizar la seguridad de las aplicaciones entregadas a los clientes.	Establecer políticas para que los usuarios realicen un adecuado manejo de los sistemas de información ofrecidos por la empresa.	PI
11.3.3	Política de puesto de trabajo despejado y pantalla limpia.	Si	Se debe evitar que por alguna razón quede expuesta información a la vista de terceros. Políticas para escritorios y monitores limpios de información	Garantizar que la información no sea expuesta a la vista de terceras personas.	Establecer políticas para que los usuarios realicen un adecuado manejo de los sistemas de información ofrecidos por la empresa.	P
11.4	Control de acceso en red					
11.4.1	Política de uso de los servicios en red.	Si	Los clientes de los servicios de la empresa sólo podrán tener acceso a los servicios autorizados.	Garantizar el acceso a servicios autorizados.	Establecer políticas de acceso a servicios ofrecidos por la empresa.	P
11.4.2	Autenticación de usuario para conexiones externas.	NO	Tanto para clientes externos de servicios alojados en la empresa como para empleados con acceso remoto deben existir políticas de acceso adecuadas.	Garantizar el acceso remoto seguro.	Establecer políticas de acceso a servicios ofrecidos por la empresa.	NA
11.4.3	Identificación de los equipos en las redes.	Si	Se debe garantizar conocer la procedencia de cualquier petición de servicio.	Garantizar que todas las conexiones establecidas sean seguras.	Establecer políticas de acceso a servicios ofrecidos por la empresa.	P

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.4.4	Protección de los puertos de diagnóstico y configuración remotos.	Si	El entorno de diagnóstico de la empresa debe estar protegido.	Proteger el sistema de diagnóstico de los sistemas de información.	Establecer políticas de acceso a servicios ofrecidos por la empresa.	P
11.4.5	Segregación de las redes.	Si	Se debe tener claramente definido el papel de cada usuario dentro de la red, asignándolo a un grupo determinado.	Garantizar la identificación de los usuarios en un grupo determinado.	Establecer políticas de acceso a servicios ofrecidos por la empresa.	PI
11.4.6	Control de la conexión a la red.	Si	El acceso a los sistemas internos de la empresa debe estar limitado para que no se puedan usar servicios que pongan en juego la seguridad.	Restringir el acceso a servicios de red desde ubicaciones externas.	Establecer políticas de acceso a servicios ofrecidos por la empresa.	TI
11.4.7	Control de encaminamiento (routing) de red.	Si	Se debe controlar el enrutamiento de información.	Garantizar que la información de la empresa no use rutas que pongan en peligro su integridad.	Establecer políticas de enrutamiento de la información.	P
11.5	Control de acceso al sistema operativo					
11.5.1	Procedimientos seguros de inicio de sesión.	Si	Se debe controlar el acceso a los sistemas operativos con los procedimientos adecuados.	Controlar el acceso al SO con procedimientos seguros.	Establecer políticas de acceso a los sistemas operativos.	P
11.5.2	Identificación y autenticación de usuario.	Si	Deben existir mecanismos de identificación únicos para los usuarios.	Garantizar que los usuarios tengan credenciales únicas de acceso.	Establecer políticas de manejo de credenciales de usuarios.	P
11.5.3	Sistema de gestión de contraseñas.	Si	Se debe garantizar que los sistemas de gestión de contraseñas sean eficientes.	Garantizar la eficiencia y seguridad en los sistemas de gestión de contraseñas.	Establecer políticas de manejo de credenciales de usuarios.	P

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.5.4	Uso de los recursos del sistema.	Si	Se debe controlar el uso de aplicaciones administrativas seguras que pueden ser usadas para generar algún tipo de daño al sistema.	Realizar control sobre el uso de aplicaciones administrativas.	Establecer políticas de uso de aplicaciones de carácter administrativo propias del sistema.	P
11.5.5	Desconexión automática de sesión.	Si	Se debe controlar el tiempo de inactividad del equipo.	Garantizar el bloqueo de equipos tras cierto tiempo de inactividad.	Establecer políticas de acceso a los sistemas operativos.	P
11.5.6	Limitación del tiempo de conexión.	Si	Se debe controlar el tiempo de conexión al SO basado en el uso de aplicaciones.	Controlar el uso del sistema operativo.	Establecer políticas de acceso a los sistemas operativos.	P
11.6	Control de acceso a las Aplicaciones					
11.6.1	Restricción del acceso a la información.	Si	Se debe restringir el acceso a los sistemas en especial al programa que maneja la base de datos, genera licencia, reportes, notificaciones, citaciones y estado de cada proyecto.	Generar restricciones a la gestión de aplicaciones.	Establecer controles para el acceso a los diferentes niveles de aplicaciones, considerando que se manejan diferentes entornos	PI

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
11.6.2	Aislamiento de sistemas sensibles.	Si	Los sistemas sensibles como copias de seguridad, archivo físico y servidores deben estar aislados	Garantizar que los sistemas sensibles de la empresa tengan un entorno informático propio.	Establecer controles para el acceso a los diferentes niveles de aplicaciones, considerando que se manejan diferentes entornos como desarrollo y pruebas.	PI
11.7	Informática móvil y tele trabajo					
11.7.1	Ordenadores portátiles y comunicaciones móviles.	Si	La conexión a través de red inalámbrica hace necesario la definición de políticas de protección en cuento a recursos móviles.	Brindar protección contra riesgos derivados del uso de recursos móviles.	Establecer políticas para el manejo de riesgos derivados de la informática móvil.	NA
11.7.2	Teletrabajo.	NO	Ya que se considera el teletrabajo al interior de la empresa es necesario considerar políticas y procedimientos tanto para acceso como para cumplimiento de funciones.	Garantizar el desempeño seguro y eficiente de actividades de teletrabajo.	Diseñar e implementar políticas para la gestión del teletrabajo.	NA
12	Adquisición, desarrollo y mantenimiento de sistemas de información					
12.1	Requisitos de seguridad de los sistemas					

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
12.1.1	Análisis y especificación de los requisitos de seguridad	Si	Es importante que todo nuevo sistema de seguridad especifique los controles necesarios para su implementación.	Garantizar que todo nuevo sistema incluya controles de seguridad.	Establecer políticas para la integración de sistemas de información.	P
12.2	Seguridad de las aplicaciones del sistema	Si	Las aplicaciones del sistema deben brindar seguridad.	Garantizar seguridad en las aplicaciones del sistema.	Establecer políticas de seguridad para las aplicaciones.	P
12.2.1	Validación de los datos de entrada.	Si	Cualquier acceso debe ser validado para garantizar que se esté haciendo desde una aplicación confiable.	Garantizar la seguridad del acceso a las aplicaciones.	Establecer políticas de seguridad para las aplicaciones.	P
12.2.2	Control del procesamiento interno.	Si	Se deben verificar las aplicaciones para detectar alteraciones en la información.	Garantizar que la información no haya sido modificada durante el procesamiento o de forma deliberada.	Establecer políticas de seguridad para las aplicaciones.	P
12.2.3	Integridad de los mensajes.	Si	Se debe asegurar la autenticidad de la información en los mensajes en las aplicaciones.	Garantizar que los mensajes en las aplicaciones no sean modificados.	Establecer políticas de seguridad para las aplicaciones.	P
12.2.4	Validación de los datos de salida.	Si	Se debe garantizar la correcta funcionalidad de la aplicación al arrojar los datos esperados.	Garantizar la integridad de la información de salida de la aplicación.	Establecer políticas de seguridad para las aplicaciones.	P
12.3	Controles criptográficos					
12.3.1	Política de uso de los controles criptográficos.	No	Es necesario contar con políticas de protección de la información al ser entregada al usuario.	Garantizar la confidencialidad de la información	Establecer políticas de protección de la información.	NA
12.3.2	Gestión de claves.	No	Se debe gestionar adecuadamente las claves como por ejemplo haciendo uso de un PKI.	Garantizar la gestión adecuada de claves al interior de la empresa.	Establecer políticas de protección de la información.	NA

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
12.4	Seguridad de los ficheros del sistema					
12.4.1	Control del software en explotación.	No	Es necesario controlar la instalación de software de tal manera que responda a las necesidades de la empresa.	Controlar la instalación de software.	Establecer políticas para la instalación de software y modificación de ficheros del sistema.	NA
12.4.2	Protección de los datos de prueba del sistema.	No	Se deberían seleccionar, proteger y controlar cuidadosamente los datos utilizados para las pruebas.	Proteger la información empleada en el entorno de pruebas.	Establecer políticas para la protección de códigos fuente y archivos del sistema.	NA
12.4.3	Control de acceso al código fuente de los programas.	No	Se debería restringir el acceso al código fuente de los programas	Garantizar la protección del código fuente de aplicaciones desarrolladas por la empresa.	Establecer políticas para la protección de códigos fuente y archivos del sistema.	NA
12.5	Seguridad en los procesos de desarrollo y soporte					
12.5.1	Procedimientos de control de cambios.	Si	Se debe tener control de versiones de aplicaciones para que los cambios sean realizados conforme a necesidades reales de la empresa.	Garantizar que los cambios respondan a procedimientos formales dentro de la empresa.	Establecer políticas para garantizar la seguridad de las aplicaciones en desarrollo y funcionamiento.	P

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Si	Se debe revisar la funcionalidad de las aplicaciones tras realizar cambios en el Sistema Operativo para no crear conflictos	Garantizar que un cambio en el SO no afecte el funcionamiento de las aplicaciones.	Establecer políticas para garantizar la seguridad de las aplicaciones en desarrollo y funcionamiento	PI
12.5.3	Restricciones a los cambios en los paquetes de software.	Si	Se debe tener control de cualquier modificación en el software de la empresa.	Garantizar el adecuado funcionamiento de las aplicaciones.	Establecer políticas para garantizar la seguridad de las aplicaciones en desarrollo y funcionamiento	TI
12.5.4	Fugas de información.	Si	Se debe garantizar la confidencialidad de la información referente a aplicaciones como programa licenciador, base de datos, licencias etc.	Garantizar la confidencialidad de la información.	Establecer políticas para garantizar la seguridad de las aplicaciones en desarrollo y funcionamiento	PI
12.5.5	Externalización del desarrollo de software.	No	Si se contrata desarrollo de software a la medida es importante realizar monitorización para evitar incidentes en el manejo.	NA	NA	NA
12.6	Gestión de las vulnerabilidades técnicas					

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
12.6.1	Control de Vulnerabilidades técnicas	Si	Se debe estar verificando constantemente las vulnerabilidades que puedan presentar los sistemas o tecnologías usadas dentro de la Curaduría.	Garantizar la protección contra vulnerabilidades de los sistemas empleados en la empresa.	Definir políticas para la gestión de vulnerabilidades de aplicaciones o sistemas usados por la empresa.	P
13	Gestión de incidentes de seguridad de la información					
13.1	Comunicación de eventos y debilidades en la seguridad de la información					
13.1.1	Notificación de los eventos de seguridad de la información.	Si	Se deben disponer canales de comunicación que permitan dar a conocer eventos de seguridad que afecten la seguridad de la empresa.	Garantizar la pronta solución a eventos de seguridad presentes en la empresa.	Definir políticas para la gestión de incidentes de seguridad de la información.	PI
13.1.2	Notificación de puntos débiles de seguridad.	Si	Se deben definir mecanismos para que todas las personas que tengan que ver con el sistema de información puedan reportar incidentes de seguridad.	Garantizar la rápida solución de incidentes informáticos.	Definir políticas para la gestión de incidentes de seguridad de la información.	PI
13.2	Gestión de incidentes y mejoras en la seguridad de la información					

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
13.2.1	Responsabilidades y procedimientos.	Si	Se debe establecer quién es el responsable de manejar determinado tipo de incidente para que sea mucha más rápida la respuesta.	Definir responsables para la gestión de eventos de seguridad.	Definir políticas para la gestión de incidentes de seguridad de la información.	PI
13.2.2	Aprendizaje de los incidentes de seguridad de la información.	Si	Se debe poder establecer el costo de un evento de seguridad de la información.	Determinar el costo de un evento de seguridad informática.	Definir políticas para la gestión de incidentes de seguridad de la información.	PI
13.2.3	Recopilación de evidencias.	Si	Se deben tener mecanismos para determinar la forma como se debe actuar contra personas que se les compruebe la generación de eventos de seguridad informática.	Definir medidas en contra de quienes generen eventos de seguridad informática.	Definir políticas para la gestión de incidentes de seguridad de la información.	P
14	Gestión de continuidad del negocio					
14.1	Aspectos de la gestión de continuidad del negocio					
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	Si	Es necesario contar con procesos de seguridad de la información que aseguren la continuidad del negocio al interior de la empresa.	Contar con procedimientos de seguridad de la información que garanticen la continuidad del negocio.	Definir políticas de seguridad de la información que garanticen la continuidad del negocio.	PI

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
14.1.2	Continuidad del negocio y evaluación de riesgos.	Si	Es necesario tener claridad de los eventos que pueden afectar el negocio y el impacto de los mismos.	Tener claridad del grado de afectación sobre el negocio de un evento determinado.	Definir políticas de seguridad de la información que garanticen la continuidad del negocio.	P
14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.	Si	Es muy importante contar con planes de contingencia que permitan la recuperación del negocio ante cualquier evento que ponga en riesgo la información.	Tener planes de contingencia ante eventos informáticos.	Definir políticas de seguridad de la información que garanticen la continuidad del negocio.	P
14.1.4	Marco de referencia para la planificación de la continuidad del negocio.	Si	Es ideal tener estandarizado el esquema del plan de continuidad para garantizar su fácil aplicabilidad en la empresa.	Contar con un plan de continuidad estandarizado.	Definir políticas de seguridad de la información que garanticen la continuidad del negocio.	P
14.1.5	Pruebas, mantenimiento y reevaluación de planes de continuidad.	Si	Se deben evaluar los planes de continuidad garantizando que evoluciones con los requerimientos del negocio.	Garantizar que los planes de continuidad evolucionen en concordancia con los requerimientos del negocio.	Definir políticas de seguridad de la información que garanticen la continuidad del negocio.	P
15	Conformidad					
15.1	Conformidad con los requisitos legales					

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
15.1.1	Identificación de la legislación aplicable.	Si	Es muy importante que la empresa sea consciente de sus obligaciones legales para garantizar el cumplimiento de las mismas.	Alinear los sistemas de información con los requerimientos legales.	Definir políticas que permitan el cumplimiento de los requerimientos de carácter legal por parte de la empresa.	P
15.1.2	Derechos de propiedad intelectual (DPI).	Si	Se debe garantizar el uso de cualquier material u software de acuerdo a las licencias definidas para los mismos.	Garantizar el uso de software debidamente licenciado y contenidos respetando los derechos de autor.	Definir políticas que permitan el cumplimiento de los requerimientos de carácter legal por parte de la empresa.	PI
15.1.3	Protección de los documentos de la organización	Si	Se debe garantizar la integridad de los registros importantes para evitar cualquier pérdida de información.	Definir mecanismos para garantizar la integridad de los registros importantes de carácter legal.	Definir políticas que permitan el cumplimiento de los requerimientos de carácter legal por parte de la empresa.	PI
15.1.4	Protección de datos y privacidad de la información de carácter personal.	Si	Debe garantizar la protección de los datos en concordancia con requerimientos de carácter legal y que mucha de la información que maneja tiene esta característica.	Brindar protección de los datos de acuerdo a requerimientos de carácter legal.	Definir políticas de protección de información alineadas con requerimientos de carácter legal.	PI
15.1.5	Prevención del uso indebido de recursos de tratamiento de la información.	Si	Se debe garantizar que los recursos empleados para el tratamiento de la información sean dedicados sólo a este fin.	Garantizar el uso exclusivo de los sistemas de tratamiento de la información para este propósito.	Definir políticas para el manejo de los sistemas de información.	TI

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
15.1.6	Regulación de los controles criptográficos.	No	Los controles empleados deben estar cifrados para asegurar su concordancia con la legislación vigente teniendo en cuenta el tipo de información que se maneja.	Garantizar la confidencialidad de los controles de seguridad y su concordancia con la legislación.	Definir políticas para el manejo de los sistemas de información.	NA
15.2	Revisiones de la política de seguridad y de la conformidad técnica					
15.2.1	Cumplimiento de las políticas y normas de seguridad.	Si	Cada director de área debe asegurarse de que los procedimientos de seguridad se realicen adecuadamente.	Garantizar la adecuada realización de los procedimientos de seguridad en cada área de la empresa.	Revisar el uso de procedimientos de seguridad de conformidad con los lineamientos de la empresa y estándares.	P
15.2.2	Comprobación del cumplimiento técnico.	Si	Es importante que los procedimientos de seguridad estén en concordancia con los estándares definidos para los mismos.	Garantizar la alineación entre procedimientos de seguridad y estándares.	Revisar el uso de procedimientos de seguridad de conformidad con los lineamientos de la empresa y estándares.	P
15.3	Consideraciones sobre la auditoría de sistemas					

Dominios	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/ No)	Justificación de elección/ no elección	Objetivo del control	Actividades para la implementación de los controles	Estado
15.3.1	Controles de auditoria de los sistemas de información	Si	Es muy importante tener control sobre los procedimientos de auditoría desarrollados al interior de la empresa sobre sistemas en funcionamiento.	Evitar que procedimientos de auditoría terminen sacando de funcionamiento algún sistema importante dentro de la empresa.	Establecer políticas para el desarrollo de procesos de auditoria.	P
15.3.2	Protección de las herramientas de auditoria de los sistemas de información	Si	Se deben tener control sobre el acceso a herramientas de auditoría ya que muchas pueden comprometer la seguridad al interior de la empresa.	Evitar el uso inadecuado de herramientas de auditoría.	Establecer políticas para el desarrollo de procesos de auditoria.	P

4.1.4.2.3. Definición del Plan de Tratamiento del Riesgo. En este documento se concreta claramente cómo se va a actuar en el control de los riesgos, se identifica los controles seleccionados, los responsables y el tiempo.

Para la definición del plan de tratamiento de riesgos se ha tenido en cuenta los siguientes documentos:

- Los 133 controles sugeridos en el Anexo A de la norma ISO 27001
- Análisis de riesgos de la Curaduría Urbana segunda de Pasto

Inventario de activos, valoración cualitativa de activos,
Identificación de amenazas,
Identificación de salvaguardas para los activos,
Valoración y evaluación del riesgo
Informe de calificación del riesgo
Políticas de seguridad

- Declaración de aplicabilidad y aplicabilidad de los controles

Se identifica el estado de la actividad de acuerdo a si está parcialmente implementado o si es propuesto para implementación.

Tabla 13: Identificación del estado de la Actividad

Estado de la Actividad	Abreviatura	Color
Planificado [No implementado]	(P)	Rojo
Parcialmente implementado	(PI)	Amarillo

Fuente: Esta Investigación

4.1.4.2.3.1 Plan de Tratamiento del Riesgos

Descripción de las actividades derivadas de los controles de seguridad y del análisis de riesgos	Responsables	Tiempo para la entrega de la actividad	Hallazgos	Estado de la Actividad
Documentación de todos los procesos a desarrollarse para la implementación de la seguridad	Curador, Jefe de Sistemas	2 meses	Es necesario que se defina una política para la documentación de todos los procedimientos en relación con las políticas de manejo de la información.	P
Revisión de las políticas de seguridad de la información.	Curador, Jefe de Sistemas	2 meses		P
Políticas de gestión de privilegios.	Curador, Jefe de Sistemas	1 mes	Es necesario que se definan políticas para la verificación de acceso a los sistemas de información y verificar los privilegios con los que tiene acceso.	PI
Políticas de seguridad para el personal que maneja la información al interior de la empresa.	Curador, Jefe de Sistemas	1 mes	Es necesario que los empleados que manejan la información conozcan y apliquen las políticas seleccionadas para el manejo de la información.	PI
Planes de capacitación para el personal a cargo del manejo de la información.	Curador, Jefe de Sistemas, Comité de seguridad	2 meses	Planes de capacitación para el personal a cargo del manejo de la información.	PI
Políticas de seguridad para nuevos activos de información.	Curador, Jefe de Sistemas, Comité de seguridad	2 meses	Es necesaria la definición de políticas de seguridad para nuevos y futuros activos dentro de la empresa.	PI

Descripción de las actividades derivadas de los controles de seguridad y del análisis de riesgos	Responsables	Tiempo para la entrega de la actividad	Hallazgos	Estado de la Actividad
Acuerdos de confidencialidad para los empleados de la empresa.	Curador	1 mes	Es necesario que los acuerdos de confidencialidad para el manejo de la información queden establecidos en el contrato laboral o en los contratos de prestación de servicios.	PI
Definir canales seguros para el manejo de la información.	Curador, Jefe de Sistemas	3 meses	Definir políticas de seguridad para evitar fallas en los canales de comunicación.	PI
Políticas para el manejo de la información al interior de la organización.	Curador, Jefe de Sistemas,	2 meses	Es necesario definir, documentar e informar sobre la implementación y cumplimiento de las políticas de seguridad para el manejo de la información al interior de la empresa.	PI
Políticas pensadas en futuros activos que formaran parte de la empresa.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesaria la definición de políticas de seguridad para nuevos y futuros activos dentro de la empresa.	P
Clasificación de los activos y establecimiento del nivel de importancia de los mismos.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario que se clasifiquen los activos de acuerdo al nivel de seguridad.	P
Políticas de manejo de activos.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario definir, documentar e informar sobre el manejo de los activos y las políticas de seguridad a aplicarse a dichos activos.	PI
Establecimiento de prioridades en el manejo de la información.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario definir	PI

Descripción de las actividades derivadas de los controles de seguridad y del análisis de riesgos	Responsables	Tiempo para la entrega de la actividad	Hallazgos	Estado de la Actividad
Políticas de acceso a la información.	Curador, Jefe de Sistemas, Comité de seguridad	2 meses	Es necesario definir, documentar e informar sobre la implementación y cumplimiento de las políticas de seguridad para el acceso a la información.	PI
Claridad en las políticas de contratación.	Curador, Jefe de recursos humanos, Área Jurídica	1 mes	Es necesario definir e informar las políticas de confidencialidad dentro de la organización,	P
Definición de políticas de manejo de la información, acompañadas de planes de capacitación.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Aunque existen políticas de seguridad para la información, se debe definir la competencia de manejo de la misma y garantizar el conocimiento de las mismas por parte de todas las personas que tienen acceso a la misma.	PI
Implementación de políticas de manejo de privilegios sobre la información.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario que se definan políticas para la verificación de acceso a los sistemas de información y verificar los privilegios con los que tiene acceso.	P
Políticas de control de acceso físico a áreas que contienen información sensible.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Ya se encuentran implementados controles para acceso a la empresa mediante clave y al archivo solo a personal autorizado, es ideal que es extiendan a todas las áreas.	PI

Descripción de las actividades derivadas de los controles de seguridad y del análisis de riesgos	Responsables	Tiempo para la entrega de la actividad	Hallazgos	Estado de la Actividad
Políticas de control de acceso físico.	Curador	1 mes	Ya se encuentran implementados controles para acceso a la empresa mediante clave y al archivo solo a personal autorizado, es ideal que es extiendan a todas las áreas.	PI
Protección contra factores atmosféricos como temperatura, humedad, etc.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario establecer controles ambientales para evitar el deterioro de activos derivado de estos factores.	PI
Verificación del nivel de seguridad de las áreas de trabajo.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario establecer controles que permitan verificar de seguridad a aplicar en cada área de trabajo de acuerdo a la información que se maneje en cada dependencia.	PI
Control de acceso físico a determinadas áreas de la empresa.	Curador, Jefe de Sistemas, Comité de seguridad	1 mes	Es necesario establecer controles de seguridad para áreas críticas donde se debe seleccionar el personal que tiene acceso a esta y las responsabilidades que esto implica ejemplo: Área de archivo	PI
Implementar controles para el control de factores ambientales como humedad, polvo, etc.	Curador, Jefe de Sistemas, Comité de seguridad	1 mes	Es necesario establecer controles ambientales para evitar el deterioro de activos derivado de estos factores.	PI
Implementar UPS.	Curador	3 meses	Debe existir sistemas de respaldo ante caídas del suministro eléctrico. Para cada uno de los equipos.	PI

Descripción de las actividades derivadas de los controles de seguridad y del análisis de riesgos	Responsables	Tiempo para la entrega de la actividad	Hallazgos	Estado de la Actividad
Implementar planes de mantenimiento de equipos al interior de la empresa	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario que se establezca un plan para el mantenimiento de equipos al interior de la empresa.	PI
Políticas para la documentación de procedimientos.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario iniciar el proceso de implementación de un plan director debidamente documentado de seguridad de la información que permita cubrir cada uno de los aspectos que han sido enumerados.	P
Implementación de políticas de manejo de privilegios sobre la información.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario implementar controles y políticas de seguridad aplicados a los grupos de trabajos y adicionalmente realizar controles que permitan gestionar la gestión de privilegios dentros del sistema.	P
Definición de políticas para la integración de nuevos elementos al sistema de información.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario definir controles que se deben tener en cuenta en el caso de que ingresen nuevos elementos al sistema de informaciòn,	P
Definición de políticas de administración y uso de redes.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario definir políticas de seguridad para el manejo y administración de la red.	PI

Descripción de las actividades derivadas de los controles de seguridad y del análisis de riesgos	Responsables	Tiempo para la entrega de la actividad	Hallazgos	Estado de la Actividad
Definición de políticas para que la información no sea extraída	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Aunque existen restricciones que se deben tener en cuenta en cuanto al manejo de la información es necesario definir políticas de seguridad para evitar que la información sea extraída, además concientizar de las implicaciones legales a las que se expone quien lo haga.	PI
Definir políticas para la gestión y eliminación de medios de almacenamientos.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Se debe definir políticas a tener en cuenta para la eliminación de medios de almacenamiento tales como discos duros, CD, DVD, memorias usb y papel firmado o sellado ya que si es desechado de forma incorrecta puede ser utilizado de forma indebida por terceros y ocasionar problemas a la organización.	PI
Implementar mecanismos de protección de información como por ejemplo encriptación (se garantiza con los controles con que cuenta la empresa).	Curador, Jefe de Sistemas, Comité de seguridad	6 meses	Es necesario definir polticas de seguridad para el manejo de herramientas criptográficas, en caso de ser implementadas.	P
Políticas de implementación y control de registros de actividad.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario que sean definidos sistemas de registros de actividad para tener control de cualquier cambio en los sistemas de información.	P

Descripción de las actividades derivadas de los controles de seguridad y del análisis de riesgos	Responsables	Tiempo para la entrega de la actividad	Hallazgos	Estado de la Actividad
Políticas de control y gestión de fallas en el sistema.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necasrio definir políticas de seguridad para implentar la gestión de fallos (notifición, visualización y reparación de fallos).	P
Políticas de implementación y control de registros de actividad.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necasrio definir políticas de seguridad para la administración del registro de actividades.	P
Definir políticas para el control de acceso teniendo en cuenta áreas críticas.	Curador, Jefe de Sistemas, Comité de seguridad	1 mes	Es necesario definir políticas a seguir para controlar el acceso a áreas restringidas (llevar un registro detallado de ingreso a estas áreas)	PI
Definir políticas para el ingreso o eliminación de usuarios del sistema.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario definir políticas de seguridad a aseguir en el procesos de eliminación de usuarios.	P
Definir políticas para la gestión de privilegios.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario definir políticas de seguridad para la gestión de privilegios, esta labor la debe realizar el administrador del sistema que se encargara de definir los roles y permisos a los usuarios del sistema.	P
Establecer políticas para la asignación de contraseñas.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario establecer políticas de seguridad que permitan implementar el uso de contraseñas. Es decir para cada usuario y equipo una contraseña la cual debe cumplir con todas las condiciones de una contraseña segura.	P

Descripción de las actividades derivadas de los controles de seguridad y del análisis de riesgos	Responsables	Tiempo para la entrega de la actividad	Hallazgos	Estado de la Actividad
Establecer políticas para la verificación regular del acceso a sistemas de información.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Implmentar políticas de seguridad que permitan verificar los accesos a los sistemas de información.	P
Establecer políticas para que los usuarios realicen un adecuado manejo de los sistemas de información ofrecidos por la empresa.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario definir políticas que los trabajadores de la empresa deben poner en práctica para la utilización de los sistemas de información de la empresa adicionales a los ya existentes.	PI
Establecer políticas de enrutamiento de la información.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario definir políticas de enrutamiento de red.	P
Establecer políticas de acceso a los sistemas operativos.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario establecer políticas para el acceso y manejo del sistema operativo.	P
Establecer políticas de manejo de credenciales de usuarios.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario definir políticas de seguridad para el manejo de credenciales de usuarios (manejo del administrador de credenciales en el S.O.)	P
Establecer políticas de uso de aplicaciones de carácter administrativo propias del sistema.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario definir políticas de seguridad para el uso de aplicaciones de carácter administrativo propias del sistema.	P
Establecer controles para el acceso a los diferentes niveles de aplicaciones, considerando que se manejan diferentes entornos.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario definir políticas de seguridad para el uso y configuración de los diferentes niveles de aplicaciones que se manejan en los diferentes entornos.	PI

Descripción de las actividades derivadas de los controles de seguridad y del análisis de riesgos	Responsables	Tiempo para la entrega de la actividad	Hallazgos	Estado de la Actividad
Establecer políticas para la integración de sistemas de información.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario definir políticas de seguridad para la integración de sistemas de información para que la informaciòn sea compartidad de forma segura.	P
Establecer políticas para garantizar la seguridad de las aplicaciones en funcionamiento.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario definir políticas de seguridad para acada apliación manejada en la Curaduria.	P
Definir políticas para la gestión de vulnerabilidades de aplicaciones o sistemas usados por la empresa.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario definir políticas de seguridad para la gestión de vulnerabilidades de aplicaciones usadas por la empresa.	P
Definir políticas para la gestión de incidentes de seguridad de la información.	Curador, Jefe de Sistemas, Comité de seguridad	3 meses	Es necesario definir políticas de seguridad para la gestión de incidentes de seguridad de la información.	PI
Definir políticas de seguridad de la información que garanticen la continuidad del negocio.	Curador, Jefe de Sistemas, Comité de seguridad	6 meses	Es necesario y de suma importancia definir políticas de seguridad de la información a implementarse encaminadas a garantizar la continuidad del negocio (tramite y expedición de licencias urbanisticas)	P
Definir políticas de protección de información alineadas con requerimientos de carácter legal.	Curador, Jefe de Sistemas, Comité de seguridad	6 meses	Es necesario definir políticas de seguridad a implementarse con el fin de proteger la información teniendo en cuenta las normas legales.	PI

Descripción de las actividades derivadas de los controles de seguridad y del análisis de riesgos	Responsables	Tiempo para la entrega de la actividad	Hallazgos	Estado de la Actividad
Revisar el uso de procedimientos de seguridad de conformidad con los lineamientos de la empresa y estándares.	Curador, Jefe de Sistemas, Comité de seguridad	6 meses	Es necesario establecer políticas de seguridad que permitan verificar que los procedimientos se estén realizando de acuerdo a las políticas y estándares definidos por la empresa.	P
Establecer políticas para el desarrollo de procesos de auditoria.	Curador, Jefe de Sistemas, Comité de seguridad	6 meses	Es necesario definir políticas de seguridad que permitan desarrollar futuras auditorias.	P

4.1.4.2.4 Carta de Respuesta de la Curaduría Urbana Segunda de Pasto

CURADURIA URBANA SEGUNDA DE PASTO

Sitio web: http://gevelu.googlepages.com

CUS-0145

San Juan de Pasto,
29 de Mayo de 2015

Ingeniera
Alba Elisa Córdoba Suárez
Ciudad

Atento Saludo,

En respuesta a solicitud realizada para la implementación del SGSI para el área de informática de la Curaduría Urbana Segunda de Pasto bajo la norma ISO/IEC 27000 me permito manifestarle que se tendrá en cuenta todo el proceso y las recomendaciones realizadas por usted para el diseño e implantación del SGSI que incluye:

1) Análisis de riesgos de la Curaduría Urbana segunda de Pasto
   - Inventario de activos, valoración cualitativa de activos,
   - Identificación de amenazas,
   - Identificación de salvaguardas para los activos,
   - Valoración y evaluación del riesgo
   - Informe de calificación del riesgo
   - Políticas de seguridad
2) Declaración de aplicabilidad, aplicabilidad de los controles y Plan de tratamiento del riesgo.

Cabe señalar que todo el proceso por usted realizado es importante para la Curaduría Urbana Segunda de Pasto ya que contribuye a mejorar la seguridad de la información y disminuir incidentes de seguridad. Por lo tanto se tendrá en cuenta para ser implementado en el segundo semestre del año 2015 toda vez que ya se encuentra definida la declaración y aplicabilidad de los controles y el plan de tratamiento del riesgo que hacen parte de la etapa de implementación.

Atentamente,

Ing. HERNANDO CASTILLO BRAVO
Curador Urbano Segundo de Pasto (P)

Calle 18 No. 19-95 Ofc. 208 Tel: 7204488 – Telefax:7330203 Correocuraduria2pasto@gmail.com

CONCLUSIONES

Para conocer la estructura y servicios que presta la Curaduría y los posibles problemas de seguridad a lo que está expuesta de manera general; se utilizan herramientas como la observación directa, la aplicación de la encuesta y la aplicación de la prueba de análisis de la red, todo esto con el fin de recolectar información, tener mayor claridad y definir un punto de partida para desarrollar la primera fase del SGSI.

Se puede decir que mediante el análisis de riesgos elaborado se evidencian todos los problemas de seguridad de la curaduría urbana Segunda de Pasto ya que este permite encontrar todos los elementos críticos dentro de la empresa, valorar dichos riesgos, determinar las amenazas, el impacto para cada dimensión de seguridad, la frecuencia, valorar los riesgos y determinar las salvaguardas.

Para el análisis de riesgos de la Curaduría Urbana Segunda de Pasto se utilizó la metodología Magerit que permite documentar paso a paso el Inventario de activos, la valoración cualitativa de activos, Identificación de amenazas, Identificación de salvaguardas para los activos, Valoración y evaluación del riesgo y el Informe de calificación del riesgo donde se evidencia claramente los activos que se encuentran en riesgo y que deben ser tratados de inmediato.

Una vez realizado el proceso de análisis de riesgo que permite conocer a fondo los riesgos a los que está expuesta la empresa se procede a definir políticas de seguridad, la declaración de aplicabilidad y aplicabilidad de los controles teniendo como soporte la Norma ISO/IEC-27002 que sugiere 11 dominios, 39 objetivos de control y 133 controles en materia de seguridad que abarcan todos los aspectos a proteger en una empresa.

Se puede decir que todo el proceso realizado para el análisis de riesgos, la definición de políticas de seguridad, la declaración de aplicabilidad y aplicabilidad de los controles conforma el diseño del SGSI para la Curaduría Urbana Segunda de Pasto bajo la norma ISO/IEC 27001 teniendo como objetivo principal garantizar la confidencialidad, disponibilidad e integridad de la información.

Se desarrolla la primera fase de implementación del SGSI que hace referencia al plan de tratamiento del riesgo donde se define claramente cómo se va a actuar en el control de los riesgos, se identifica los controles seleccionados, los responsables y el tiempo. Por otra parte con la carta de respuesta del Curador se señala que se tendrá en cuenta todo el proceso realizado para continuar con la implementación.

De manera general se puede concluir que la implementación de un SGSI en el área de informática de la Curaduría Urbana Segunda puede generar grandes

beneficios a mediano y largo plazo, garantizando el cumplimiento de estándares que trabajan por la protección de la información y los activos relacionados. Además contribuyen a fortalecer la continuidad del negocio ya que su objetivo es disminuir al máximo los riesgos a los que está expuesta la información.

BIBLIOGRAFÍA

AMUTIO, Miguel y CANDAU, Javier. MAGERIT. Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I. Método. Ministerio de Hacienda y Administraciones Pública. España, 2012.

_____. Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II. Catálogo de Elementos. Ministerio de Hacienda y Administraciones Pública. España, 2012.

_____. Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III–Guía de técnicas. Ministerio de Hacienda y Administraciones Pública. España, 2012.

Ciclo PDCA. Sistemas de Gestión de Seguridad de la Información. Obtenido de http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-14-agosto-2013/135_ciclo_pdca__edward_deming.htmll

CORLETTI Alejandro, Controles de seguridad. 2006. Obtenido de http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_II.pdf.

ISO 27001. (2005). El portal de ISO 27001 en Español. Obtenido de http://www.iso27000.es/iso27000.html

ISO 27001. (2013). Statement of Applicability of ISO/IEC 27001 Annex A controls. Obtenido de www.ISO27001security.com

ISO 27001. (2013). Plan de tratamiento de riesgos, Obtenido de http://www.iso27001standard.com/es/documentacion/Plan-de-tratamiento-de-riesgos.

ISO / IEC 27002 (2013). Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información
MINVIVIENDA (2010). Decreto 1469, Obtenido: http://www.minvivienda.gov.co/

UNIVERSIDAD JAVERIANA. Manual del sistema de gestión de la seguridad de la información, Obtenido:

http://pegasus.javeriana.edu.co/~CIS0830IS12/documents/Anexo%20K%20MG-05%20Manual%20del%20Sistema%20de%20Gestion%20de%20Seguridad%20de%20la%20Informacion.pdf.

UNIVERSIDAD DISTRITAL. Seguridad de la Información: Política para la seguridad de la información de la Universidad Distrital Francisco José de Caldas, obtenido en: https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf

SUAREZ SIERRA, Lorena. (2013). Sistema de Gestion de La Seguridad de La Informacion.

ANEXOS

ANEXO A

ENCUESTA PARA EL PERSONAL DE LA CURADURIA

Como empleado de la Curaduría Urbana Segunda de Pasto le solicitamos completar esta pequeña encuesta para contribuir con su opinión a mejorar nuestros procesos y proteger la información.

Esta encuesta dura aproximadamente 10 minutos:

Basándose en su propia experiencia:

Marque con una X su respuesta

¿Con que frecuencia se cambian las contraseñas del pc a su cargo?

____ a) Entre 1 y dos meses

____ b) Entre 2 y 6 meses

____ c) Entre 6 meses y 1 año

____ d) más de 1 año

¿Con que frecuencia utiliza internet?

____ a) Una vez al día

____ b) Dos a 10 veces en el día

____ c) Muchas veces en el día

____ a) Todo el tiempo

Los problemas más frecuentes que se presentan en el pc a su cargo son: Siendo 1= Siempre, 2= Algunas veces, 3= nunca

Afirmaciones:	1	2	3
a) El pc se bloquea			
b) El pc presenta mensajes de error			
c) El pc no se conecta a la red			
d) El pc es lento			

Valore las siguientes afirmaciones: Siendo 1= malo, 2= Aceptable, 3= Bueno, 4= Excelente

Afirmaciones:	1	2	3	4
a) Cambio de Contraseñas periódicamente	___	___	___	___
b) Actualización de Software permanente	___	___	___	___
c) Almacenamiento y manejo de copias de seguridad	___	___	___	___
d) información sobre la responsabilidades en cuanto al manejo de la información	___	___	___	___
e) Ubicación estratégica de los equipos y servidores para ser protegidos.	___	___	___	___

En general: ¿Ha tenido usted algún problema en el momento de utilizar el pc?

SI:____ NO:____

¿Las dificultades presentadas influyen en la calidad de atención al cliente?

SI:____ NO:____

¿Las dificultades presentadas en su pc influyen en el tiempo utilizado y en la calidad de su trabajo?

SI:____ NO:____

¿Cree usted que las medidas de seguridad utilizadas son suficientes para proteger la información y prevenir posibles incidentes?

SI:____ NO:____

¿Recomendaría usted adoptar políticas de seguridad encaminadas a proteger la información y evitar posibles daños de la información?

SI:____ NO:____

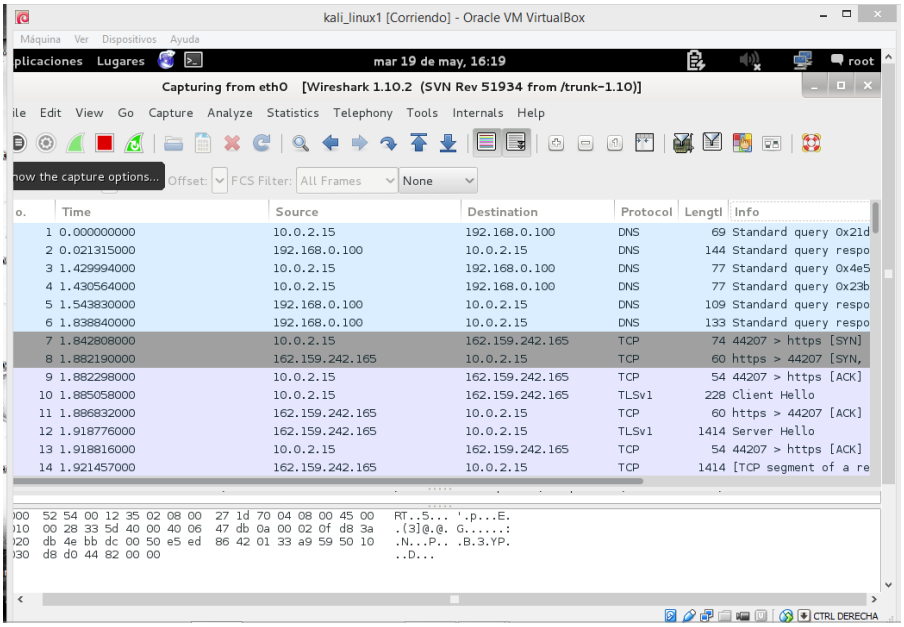
¿Recomendaría usted adoptar políticas de seguridad encaminadas a proteger la información y evitar posibles daños de la información?

SI:____ NO:____

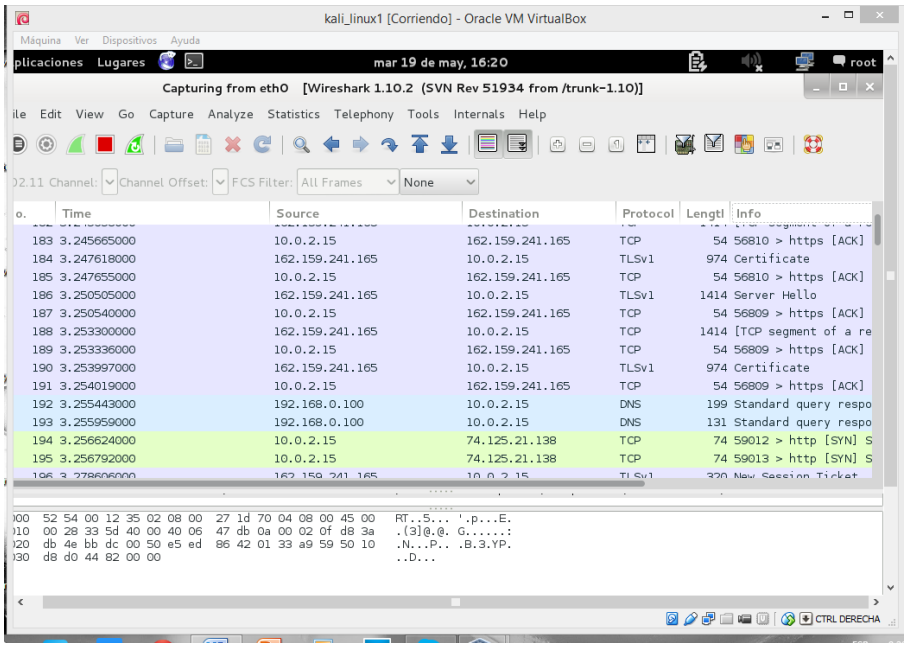
ANEXO B

ANÁLISIS DE TRÁFICO DE RED CON WIRESHARK DE LA RED DE LA CURADURIA URBANA SEGUNDA DE PASTO

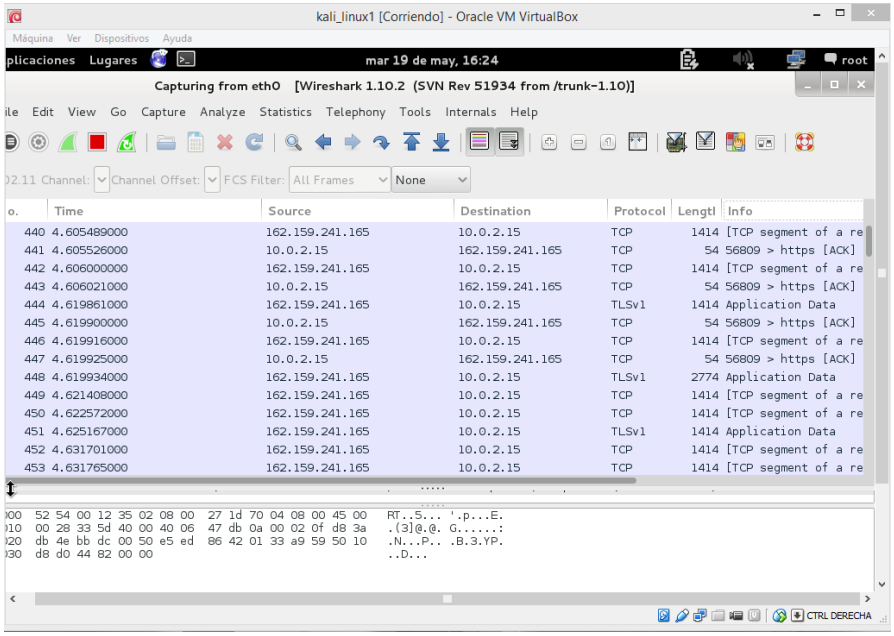
Whireshark es una herramienta utilizada para el análisis de tráfico de redes, que permite saber que sucede en la red, en la siguiente imagen se indica se puede observar los siguientes datos: El tiempo, la fuente, el destino, el protocolo utilizado, la longitud, las solicitudes que se realizan al servidor, los accesos a páginas de internet etc.



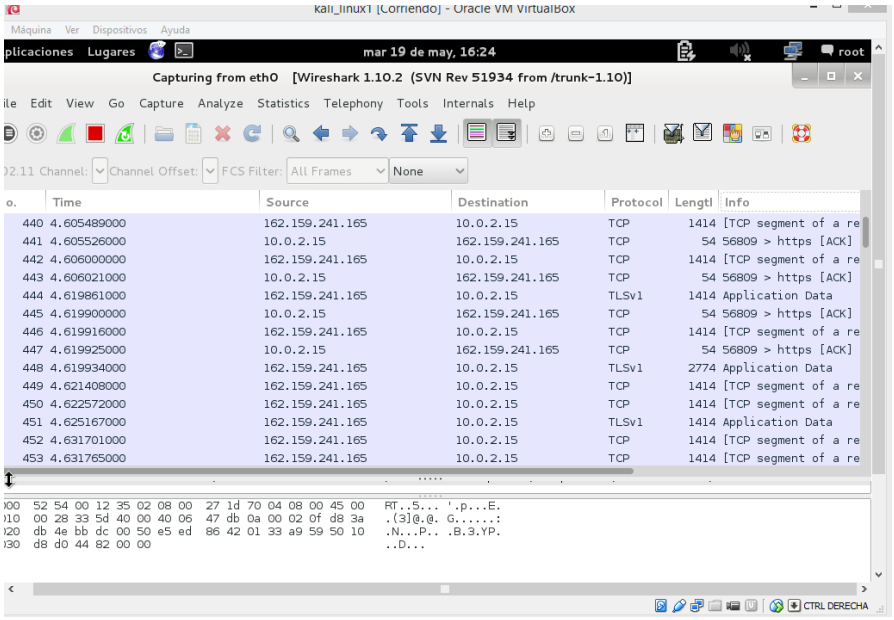
Whireshark captura todo lo que sucede en la red (todas las peticiones)



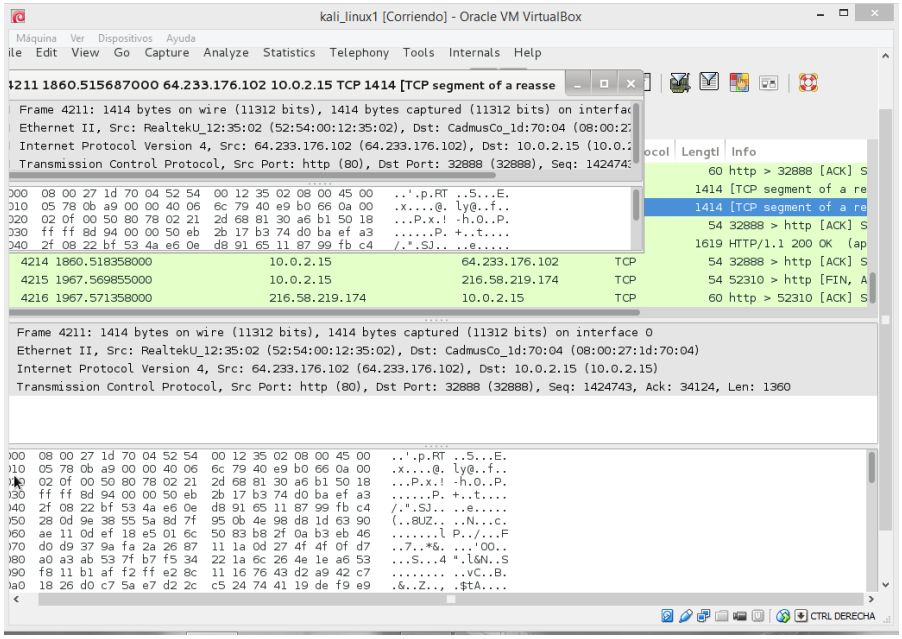
Se puede observar que el servidor se conectó a través de la petición DNS.

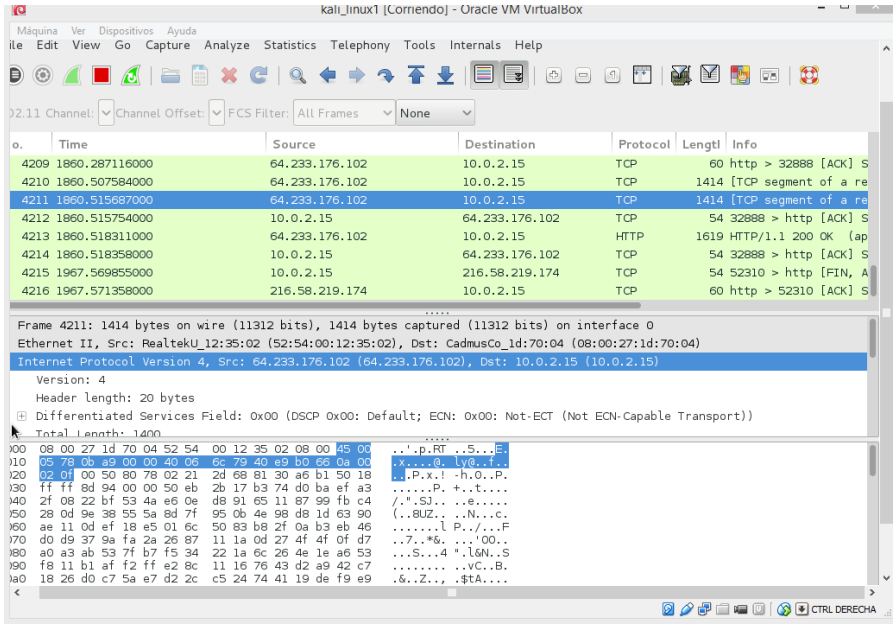


Al utilizar este programa podemos observar si se está generando tráfico no deseado como un virus que puede provocar lentitud.



Mediante este análisis se puede seleccionar un paquete y en panel de detalles de paquete se encuentra información adicional para casa paquete.




kali_linux1 [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
802.11 Channel: Channel Offset: FCS Filter: All Frames None
No. Time Source Destination Protocol Length Info
4209 1860.287116000 64.233.176.102 10.0.2.15 TCP 60 http > 32888 [ACK] S
4210 1860.507584000 64.233.176.102 10.0.2.15 TCP 1414 [TCP segment of a re
4211 1860.515687000 64.233.176.102 10.0.2.15 TCP 1414 [TCP segment of a re
4212 1860.515754000 10.0.2.15 64.233.176.102 TCP 54 32888 > http [ACK] S
4213 1860.518311000 64.233.176.102 10.0.2.15 HTTP 1619 HTTP/1.1 200 OK (ap
4214 1860.518358000 10.0.2.15 64.233.176.102 TCP 54 32888 > http [ACK] S
4215 1967.569855000 10.0.2.15 216.58.219.174 TCP 54 52310 > http [FIN, A
4216 1967.571358000 216.58.219.174 10.0.2.15 TCP 60 http > 52310 [ACK] S
Frame 4211: 1414 bytes on wire (11312 bits), 1414 bytes captured (11312 bits) on interface 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: CadmusCo_1d:70:04 (08:00:27:1d:70:04)
Internet Protocol Version 4, Src: 64.233.176.102 (64.233.176.102), Dst: 10.0.2.15 (10.0.2.15)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 1400
0000 08 00 27 1d 70 04 52 54 00 12 35 02 08 00 45 00 ..'.p.RT ..5...E.
0010 05 78 0b a9 00 00 40 06 6c 79 40 e9 b0 66 0a 00 .x....@. ly@..f..
0020 02 0f 00 50 80 78 02 21 2d 68 81 30 a6 b1 50 18 ...P.x.! -h.0..P.
0030 ff ff 8d 94 00 00 50 eb 2b 17 b3 74 d0 ba ef a3 ......P. +..t....
0040 2f 08 22 bf 53 4a e6 0e d8 91 65 11 87 99 fb c4 /."SJ.. ..e.....
0050 28 0d 9e 38 55 5a 8d 7f 95 0b 4e 98 d8 1d 63 90 (..8UZ.. ..N...c.
0060 ae 11 0d ef 18 e5 01 6c 50 83 b8 2f 0a b3 eb 46 ....l P../...F
0070 d0 d9 37 9a fa 2a 26 87 11 1a 0d 27 4f 4f 0f d7 ..7..*&. ...'OO..
0080 a0 a3 ab 53 7f b7 f5 34 22 1a 6c 26 4e 1e a6 53 ...S...4 ".l&N..S
0090 f8 11 b1 af f2 ff e2 8c 11 16 76 43 d2 a9 42 c7 ....vC..B.
00a0 18 26 d0 c7 5a e7 d2 2c c5 24 74 41 19 de f9 e9 .&..Z.., .$tA....
CTRL DERECHA