DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA GED (GESTION ESTRATEGIA Y DESARROLLO) DE LA CIUDAD DE BOGOTA

LINA PATRICIA MENDOZA PENAGOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
CENTRO DE EDUCACIÓN ABIERTA Y A DISTANCIA CEAD
ESPECIALIZACION SEGURIDAD INFORMATICA
GIRARDOT
2017

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA GED (GESTION ESTRATEGIA Y DESARROLLO) DE LA CIUDAD DE BOGOTA

LINA PATRICIA MENDOZA PENAGOS

Monografía para obtener el título de
Especialista en Seguridad Informática

ASESOR
Henry Aldemar Guerrero Erazo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
CENTRO DE EDUCACIÓN ABIERTA Y A DISTANCIA CEAD
ESPECIALIZACION SEGURIDAD INFORMATICA
GIRARDOT
2017

CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

LISTA DE ANEXOS

RESUMEN

El presente proyecto se realizo con el fin de Diseñar un Sistema de Gestión de Seguridad de la Información para la Empresa GED (Gestión Estrategia Y Desarrollo), para la cual se evaluo la situación actual de la empresa, y así enumerar los riesgos que la podrían afectar, también el impacto que produciría a la empresa en el caso de que se produzca estas amenazas.

Se realizó la valoración de los activos para luego determinar las vulnerabilidades, amenazas y riesgos de seguridad a los que podrían estar expuestos la información con la aplicación de la metodología MAGERIT, también se pudo verificar los riesgos a los que estarían expuestos cada proceso de la empresa.

Para terminar se definen las políticas y controles de seguridad, que tienen como fin tratar de disminuir los riesgos y mejorar la seguridad en la empresa.

ABSTRACT

The present project was carried out with the purpose of Designing an Information Security Management System for the Company GED, for which the current situation of the company was evaluated, and so to enumerate the risks that could affect it, also the impact that would produce to the company in case of these threats.

The valuation of the assets was carried out to determine the vulnerabilities, threats and security risks to which the information could be exposed with the application of the MAGERIT methodology. It was also possible to verify the risks to which each company process would be exposed.

Finally, it defines the security policies and controls, which aim to reduce risks and improve security in the company.

GLOSARIO

Información: Inteligencia o conocimiento capaz de ser representado en formas adecuadas para comunicación, almacenamiento o procesamiento[1].

Amenaza: Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema[2].

Riesgo: La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generándole pérdidas o daños, Las amenazas pueden ser de carácter físico o lógico, como ser una inundación en el primer caso, o un acceso no autorizado a una base de datos en el segundo caso[3].

Vulnerabilidad: Son ciertas condiciones inherentes a los activos o presentes en su entorno que facilitan que las amenazas se materialicen llevan a esos activos a ser vulnerables.
Mediante el uso de las debilidades existentes es que las amenazas logran materializarse, o sea, las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto.

Activos: Los activos a nivel tecnológico, son todos los relacionados con los sistemas de información, las redes y comunicaciones y la información en sí misma. Por ejemplo los datos, el hardware, el software, los servicios que se presta, las instalaciones, entre otros[4].

Virus: Es un programa parásito porque el programa ataca a los archivos o al sector de "arranque" y se replica a sí mismo para continuar su propagación. Algunos se limitan solamente a replicarse, mientras que otros pueden producir serios daños que pueden afectar a los sistemas. No obstante, absolutamente todos cumplen el mismo objetivo: propagarse[5].

Estándar: Administran las tecnologías de manera integral, sin embargo, existen distintos modelos aplicables en la administración de la seguridad[6].

---

[1] Glosario
http://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html
[2] Glosario de términos
http://datateca.unad.edu.co/contenidos/233004/riesgos/glosario_de_trminos.html
[3] [4] [5] Lección 3 Análisis de Riesgos http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_3_anlisis_de_riesgos.html
[6] Fundamentos de Seguridad Informática
http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Estandares.php
[7] [8] ¿Qué es un SGSI?
http://www.pmg-ssi.com/2015/07/que-es-sgsi/

Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados[7].

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso[8].

1. INTRODUCCIÓN

En la actualidad la seguridad informática se ha convertido en uno de los objetivos primordiales de las empresas por la cantidad de amenazas a las que puede ser expuesta la información, la preocupación por mejorar la seguridad es un tema que toma fuerza a medida que se facilita el acceso a esta y las vulnerabilidades son aún mayor.

Este proyecto pretende diseñar un sistema de gestión de seguridad de información para la empresa gestión estrategia y desarrollo el cual le permitirá identificar los riesgos que pueden afectar los recursos de la misma y dar solución al tratar de mitigarlos con la implementación de ciertos controles que permitan brindar un nivel aceptable de seguridad para la información.

2. DEFINICION DEL PROBLEMA

La seguridad de la información es muy importante para las empresas porque deben proteger su activo principal “datos”, la perdida de información se debe a la falta de controles de acceso a la información permite que los usuarios solo puedan ingresar a los datos relacionados con su trabajo, si no hay control las empresas del sector pueden obtener información sensible por medio de empleados que no se encuentren a gusto con su trabajo.

El activo importante en GED son los datos, los cuales están bajo peligro latente a pérdida o robo de información sensible por la falta de políticas de seguridad en GED, situación que permite inevitablemente el acceso no autorizado a la red de información o a los equipos, también porque cualquier usuario puede tener acceso a la información y porque no se trabaja sobre unas buenas prácticas de seguridad que cumpla con los requisitos legales en cuanto a la protección de la información, esto sucede si no se establece un control que ocasionara graves problemas para la empresa y sus clientes.

Un reciente estudio presentado por McAfee, compañía de software especializada en seguridad informática, reveló que Colombia presenta serios problemas en esta área, con tendencia a crecer.“ Las razones están vinculadas con la falta de normas y exigencias por parte del Estado a las empresas y la ausencia de concienciación de los directivos”.[9]

2.1 FORMULACION DEL PROBLEMA

¿Cómo se puede mejorar la Seguridad de la información en GED (Gestión Estrategia Y Desarrollo)?.

9 Colombia, líder en inseguridad informática en A. Latina.
Internethttp://www.elespectador.com/tecnologia/colombia-lider-inseguridad-informatica-latina-articulo-482097

3. JUSTIFICACION

En toda organización el activo sobre el cual se debe ejercer control y el más valioso es la información, pero en la actualidad es esencial no solo asegurar los datos, sino las aplicaciones y la infraestructura de la organización que se puede ver expuesta a diferentes vulnerabilidades, ataques y amenazas contra la seguridad.

Con el SGSI en GED se obtendrá la seguridad general de la empresa en su parte física porque brindará la tranquilidad de salvaguardar los activos que se pueden ver expuestos a robos por no tener un control de las personas que acceden al lugar, en la parte lógica aportará al mejoramiento de los procesos, la productividad, la eficiencia en la gestión de la empresa y también restringiendo el acceso clasificando qué usuarios pueden ingresar parcialmente según las funciones que desempeñan. Unos de los beneficios que puede obtener la empresa es lograr un posicionamiento en el país generando confianza y satisfacción a sus clientes.

Según Jon Parkes, vicepresidente de Preventa de Intel Security, dice que en el 2015 o el 2016 repuntaría el mercado en nuestro país, pues en los dos últimos años las empresas han adquirido mucha infraestructura en este campo que necesitarán proteger.[10]

La empresa aún no ha implementado un modelo que le permita ejercer y establecer el control de cada una de sus áreas que están expuestas a cualquier tipo de amenaza, por eso es importante que si se logra diseñar e implementar el SGSI sería posible reducir significativamente estas dificultades que podrían interferir con el desarrollo de sus labores diarias.

Al implementar SGSI, le dará un valor agregado a la empresa porque aumentará la confianza y mejorará su imagen frente a sus clientes.

GED debe implementar mecanismos que le permitan estar segura, para este caso debe aplicar el SGSI basado en la norma ISO 27001, efectuando diferentes procesos entre las cuales se encuentran políticas y procedimientos para controlar y garantizar la seguridad de su activo más importante, estableciendo la

10 La seguridad informática se contrajo 15 % en ventas. Internet http://www.portafolio.co/negocios/la-seguridad-informatica-se-contrajo-15-ventas

responsabilidad en cada una de las áreas en donde se tiene acceso y evitar que sea expuesto a vulnerabilidades como la perdida de información.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información que ayuda a reducir las amenazas de seguridad en que se encuentra la empresa GED en la ciudad de Bogotá.

4.2 OBJETIVOS ESPECÍFICOS

Identificar los activos informáticos mediante la aplicación de instrumentos de recolección de información para establecer los dominios del estándar ISO 27001 en GED.

Determinar las vulnerabilidades amenazas y riesgos de seguridad a los que pueda estar expuesta la información aplicando la metodología MAGERIT.

Revisar y verificar la existencia de controles de acuerdo a la norma ISO 27002 que ayude a definir la existencia de políticas y procedimientos de seguridad en GED.

Diseñar un sistema de gestión de seguridad de la información y sus respectivas normas de acuerdo a los resultados de la evaluación realizada.

5. MARCO DE REFERENCIA

5.1ANTECEDENTES

El proyecto denominado “Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda” presentado por Juan David Aguirre Cardona y Catalina Aristizabal Betancourt en la Universidad Tecnológica de Pereira (Colombia) – 2.013. Este proyecto explica cómo aplicar la norma 27001 en una empresa y se toma como ejemplo para el desarrollo y los pasos a seguir para el diseño del SGSI.

Proyecto denominado “Diseño de un sistema de gestión de la seguridad informática – SGSI–, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C., a través de la auditoría” presentado por Alexander Guzmán García y Carlos Alberto Taborda Bedoya en la Universidad Nacional Abierta y Distancia – UNAD (Colombia) – 2.013. Procedimiento sobre la Gestión de riesgos MAGERIT y explica de forma detallada la metodología para el desarrollo del SGSI.

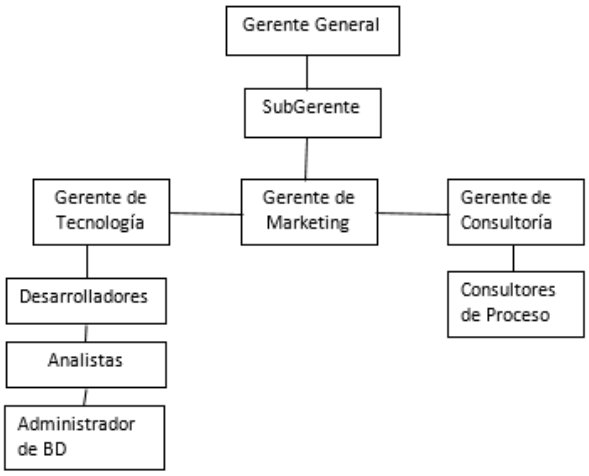
Proyecto denominado “Diseño de un sistema de gestión de seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 en la oficina de sistemas de información y telecomunicaciones de la universidad de córdoba” presentado por Andrés Felipe Doria Corcho en la Universidad Nacional Abierta y Distancia – UNAD (Colombia) – 2.015,donde se evalúan los riesgos a los que están expuestos los activos informáticos y emplear un enfoque metodológico que permita mitigarlos o mantenerlos a un nivel aceptable, además de establecer un plan de mejoramiento continuo.

5.2 MARCO CONTEXTUAL

Historia

Ged Nació como la idea de dos consultores de ingeniería Industrial, los cuales trabajan en un Excel el tema de Balance Score Card, y hacían consultoría en las empresas, para la planeación estratégica y generación de indicadores de desempeño y Calidad, a medida que las empresas fueron creciendo vieron la necesidad de crear empresa, ahi nació GED, se constituyó y género, debido a que el mercado exigía algo más sólido y evolucionar del Excel a una plataforma más tecnológica, alineadas en el mercado, como son las aplicaciones WEB.

Figura 1. Organigrama



El proyecto para el diseño del sistema de gestión de seguridad informática se realizará en el área de sistemas y a los funcionarios (asesoras y desarrolladores) que conocen el proceso de la información a tratar en el Sistema de Presentación integral de la Gestión Institucional P.I.G.I.
GED S.A.S. es una empresa colombiana con más de 10 años de trayectoria trabajando con el sector público y privado. Asegurando el desarrollo y mejoramiento continuo de las organizaciones reconociendo las necesidades y expectativas de nuestros clientes, garantizando la eficacia, eficiencia y efectividad en la ejecución de nuestras actividades.
Además de identificar, estructurar, organizar la información empresarial y facilitar la administración lógica de la empresa.

5.3 MARCO TEÓRICO

Sistema de Gestión de la Seguridad de la Información (SGSI),es un conjunto de datos organizados en cuanto a políticas de administración de información, el cual consiste en diseñar, implantar y mantener los procesos que permitan gestionar de manera eficiente el acceso a la información y se pueda asegurar la preservación de la confidencialidad, integridad y disponibilidad de los activos de una organización para minimizar los riesgos a los que se pueda exponer la información.

5.3.1 Para Que Sirve un SGSI

El activo significativo e importante de una organización es la información además de los procesos y el sistema que hacen uso de ella. La confidencialidad, integridad y disponibilidad de información sensible son esenciales para conservar los niveles de competitividad, rentabilidad y conformidad legal e imagen empresarial para que se logren los objetivos y se asegure el factor económico de la organización. En la actualidad los sistemas de información de las organizaciones se encuentran expuestos a amenazas cuando existen vulnerabilidades que someten a los activos de información sensibles a fraudes, espionaje, sabotaje o vandalismo, los virus, el hacking o ataques de denegación de servicio son los más comunes, también se deben tener en cuenta los riesgos de presentar incidentes de seguridad que pueden causarse de manera voluntaria o involuntaria dentro de la organización o factores ambientales como catástrofes naturales.
Los aspectos fundamentales en los que un SGSI es de gran utilidad y ayuda para la gestión de la organización son los siguientes:
Se debe dar cumplimiento a la legalidad, la adaptación de forma dinámica y precisa a las condiciones del entorno y la protección de los objetivos de la organización y que el nivel de seguridad que se alcancen por medios técnicos son muy limitados e insuficientes. La organización junto con la gerencia debe involucrar y educar a sus colaboradores en la gestión de seguridad para que esta sea efectiva.
Para la implementación del modelo de gestión de seguridad se debe examinarlos procedimientos que sean apropiados, además de la planificación e implantación de los controles de seguridad que se tendrán en cuenta en la evaluación de riesgos.

Figura 2. Para qué sirve SGSI

Fuente: http://www.iso27000.es/download/doc_sgsi_all.pdf

5.3.2 Qué Incluye un SGSI

Tomando como base la norma ISO 9001 la documentación del sistema de gestión de seguridad se representa gráficamente en forma de pirámide de cuatro niveles. Y al trasladarlo al Sistema de Gestión de la Seguridad de la Información basado en la norma ISO 27001 se representa de la siguiente forma:

Figura 3. Estructura del SGSI

Fuente: http://www.iso27000.es/download/doc_sgsi_all.pdf

En los documentos de Nivel 1se encuentra el Manual de seguridad donde se documenta como se va dirigir todo el sistema, además de exponer y determinar las intenciones, el alcance, los objetivos, las responsabilidades, y políticas del SGSI.
Los documentos de Nivel 2 están especificados los Procedimientos a nivel operativo, donde se establece la planificación y control de los procesos de seguridad de la información.
Documentos de Nivel 3 se realizan las Instrucciones, entre las que se encuentran checklists y formularios: para llevar el control de las tareas y actividades relacionadas con la seguridad de la información.
Documentos de Nivel 4 en los Registros donde se va evidenciando el cumplimiento del SGSI; además en la norma ISO 27001 el SGSI debe estar estructurado por los siguientes documentos:

- Alcance del SGSI
- Política y objetivos de seguridad
- Procedimientos y mecanismos de control
- Enfoque de evaluación de riesgos
- Informe de evaluación de riesgos
- Plan de tratamiento de riesgos
- Procedimientos documentados
- Registros

• Declaración de aplicabilidad

5.3.3 Implementación de un SGSI

Figura 4. Implementación SGSI

Fuente: http://www.iso27000.es/download/doc_sgsi_all.pdf

• 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.

La dirección de la organización debe comprometerse con establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI. Para lograr esto debe tomar las siguientes decisiones:

• 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.[11]

[11]Compromiso de la Dirección
http://www.iso27000.es/download/doc_sgsi_all.pdf

5.3.4 Iso 27001

Con la norma ISO 27001 se permite establecer el marco de trabajo para definir un SGSI, enfocándose en la gestión de la seguridad como un proceso continuo. Para realizar la certificación de un proceso u organización es necesario analizar y gestionar los riesgos fundamentales a los que se encuentra expuestos.
Cuando se identifican los riesgos se plantea una estrategia para cada uno, las alternativas son las siguientes:

- Se debe evitar el riesgo, se abandona la actividad que lo esté generando este exceda a los beneficios que aporta.
- Cuando se traslada el riesgo a terceros por ejemplo cláusulas contractuales o pólizas de seguros.
- Tratar el riesgo creando medidas que lo limiten para reducir la probabilidad de que causen algún tipo de consecuencias.

5.3.5 Iso 27002

Esta norma es una Guía que permite la implementación de controles para ejercer las buenas prácticas de seguridad en una organización y mejorar la seguridad de la información.
Esta norma está distribuida en diferentes dominios en donde se encuentran los aspectos que se tienen en cuenta en una organización.
A continuación los dominios que estructura la ISO 27002, entre los que se encuentra:

1. La política de seguridad.
2. La Organización.
3. Recursos Humanos
4. La gestión de activos.
5. La seguridad física y ambiental.
6. Las comunicaciones y operaciones.
7. Los controles de acceso a la información.
8. La adquisición, desarrollo y mantenimiento de los sistemas de información.
9. Incidentes.
10. La continuidad del negocio.
11. Cumplimiento

Un sistema informático está expuesto a ataques, de los cuales los datos y la información necesitan protección con técnicas de seguridad, ya que el objetivo principal de la seguridad informática es proteger la confidencialidad, la integridad y la disponibilidad de la información.

5.3.6 Magerit

Consiste en el análisis y gestión de riesgos la cual permite estudiar los riesgos que puede sufrir un sistema de información su entorno. Esta metodología MAGERIT reúne el análisis de los riesgos que implica la evaluación del impacto cuando se presenta una violación de seguridad dentro de una organización, donde se enumera los riesgos existentes, se identifican las amenazas y se determina la vulnerabilidad de sistema para luego obtener los resultados de esta investigación.

Estos resultados del análisis de riesgos es lo que permite en la gestión de riesgos realizar recomendaciones sobre cuáles son las medidas apropiadas que se deberían adoptar para conocer, prevenir, impedir, reducir y controlar los riesgos que se identifican y el reducirlos para evitar posibles riesgos que perjudiquen a la organización.

5.4 MARCO LEGAL

Para la seguridad de la información de las empresas en colombia se tiene en cuenta la Ley que se menciona a continuación con el fin de brindar la tranquilidad a sus clientes que los datos suministrados no van a sufrir ningun tipo de perdida, además de dar a conocer a sus empleados cada uno de los articulos de la ley para evitar cualquier uso mal intensionado de la información proporcionada por los usuarios.

LEY 1273 DE 2009

CAPITULO. I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.
Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.

CAPITULO. II

De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u

otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

6. MARCO METODOLOGICO

6.1 METODOLOGIA DE INVESTIGACION

Linea de Investigación

Según las lineas de investigación que ofrece la escuela ECBTI (Escuela de Ciencias Básica, Tecnología e Ingenierías), se aplicará la Linea de Investigación Gestion de Sistemas, la cual consiste en apoyar el desarrollo productivo, tecnológico y social empresarial a través del análisis, diseño, implementación o administración de sistemas de información y las TIC que estén basados en la plantificación, dirección, control, evaluación y realimentación de actividades procedimentales.

6.2 UNIVERSO Y MUESTRA

La población (Universo) que se tomará como objeto de investigación son todos los usuarios que tienen acceso a la información (Director, Desarrolladores, Administrativos y Asesoras) sin excepción.
El muestreo que se va a realizar se enfocará principalmente en los desarrolladores de software y las asesoras que brindan soporte a los clientes de la empresa.

6.3 INSTRUMENTO DE RECOLECCIÓN DE INFORMACIÓN

Para obtener la información necesaria que nos ayude en el desarrollo del proyecto esta se recopila por medio de una investigación directa al objeto de estudio, a través de los siguientes métodos:

- Entrevistas: A los desarrolladores de software que cuentan con la experiencia en la ejecución de los procesos de los sistemas de información, así como las asesoras encargadas de brindar el soporte de estos.
- Cuestionarios: Se realizan con el fin de conocer si la persona (asesoras) tiene conocimientos básicos de seguridad informática.
- Listas de Chequeo: Se realiza con el objetivo de verificar los procesos en la empresa.

6.4 METODOLOGÍA DE DESARROLLO

Para el desarrollo del Diseño e implementación de un SGSI se debe realizar:

1. Identificar y determinar los activos de la organización mediante la aplicación de instrumentos de recolección de información para establecer los dominios del estándar ISO 27001 en GED.

- Revisar el respectivo inventario de los activos (hoja de vida equipos).
- Realizar entrevistas al personal encargado de manejar los equipos.

2. Determinar las vulnerabilidades amenazas y riesgos de seguridad a los que pueda estar expuesta la información aplicando la metodología MAGERIT.

- Realizar la valoración respectiva de los activos del área de sistemas.
- Elaborar y aplicar cuestionarios sobre el uso de los equipos, dispositivos de almacenamiento para revisar el nivel de seguridad de la información que manipulan los usuarios (asesoras), clasificando las amenazas, para valorar la integridad, disponibilidad, confidencialidad y trazabilidad.

3. Revisar y verificar la existencia de controles de acuerdo a la norma ISO 27002 que ayude a definir la existencia de políticas y procedimientos de seguridad en GED.

- Solicitar información sobre los procesos de desarrollo del área de sistemas.
- Verificar con una lista de chequeo que se apliquen las respectivas políticas de seguridad informática y la información.
- Seleccionar que normas y controles se implementaran de acuerdo a la recolección de la información que se recolecto.

4. Diseñar e implementar un sistema de gestión de seguridad de la información y sus respectivas normas de acuerdo a los resultados de la evaluación realizada.

- Analizar y evaluar la información recopilada.
- Definir el objetivo y el alcance del SGSI.
- Definir y establecer las políticas, normas y controles de seguridad.
- Se elabora el informe Final.

7. IDENTIFICACION DE ACTIVOS Y AMENAZAS

Se realizó la identificación y determino los activos que están a disposición de la empresa GED Gestión estrategia y desarrollo para establecer las medidas a implementar en el proceso de diseño del sistema de gestión de seguridad informática.

Tabla 1**.** Inventario de activos.

INVENTARIO DE ACTIVOS	
Tipos de activos	**Descripción**
Activo de información	Sistema de Información PIGI
Software	Microsoft Windows 7 Professional Office 2013 Pro Microsoft Live Security Aplicativo Web SIKUA Aplicativo Web MAPA
Hardware	Servidor de ficheros e impresión Servidor web Servidor de bases de datos Computadoras
Red	Router
Equipamiento auxiliar	Red Wifi (conexión Inalámbrica) Internet Red Lan
Personal	1 persona encargada del funcionamiento y gestión del sistema 6 desarrolladores 3 asesoras

Fuente: el autor

- Revisión del respectivo inventario de los activos (hoja de vida equipos).

No cuenta con el inventario de Equipos.

- Lista de Chequeo (Tabla 21)

Se realiza para establecer los dominios del estándar ISO 27001 en GED con el objetivo de implantar, luego mantener y mejorar un sistema de gestión de la Empresa.

- Entrevistas al personal encargado de manejar los equipos (Anexo A)

Se realiza con la finalidad de establecer que conocimiento tiene el encargado del sistema y demás empleados sobre seguridad informática.

7.1valoración De Los Activos

Se determina la valoración de los activos de GED de acuerdo a la metodología MAGERIT Versión 3; se usa las siguientes dimensiones

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de la Información.
- [A] Autenticidad
- [T] trazabilidad

Tabla 2**.** Valoración de activos.

VALOR	
(MA)	Muy alto
(A)	Alto
(M)	Medio
(b)	Bajo
(MB)	Muy bajo

Tabla 3**.** Dimensiones de Seguridad.

VALOR	**CRITERIO**
10	Daño muy grave a la organización
7 - 9	Daño grave a la organización
4 - 6	Daño importante a la organización
1 - 3	Daño menor a la organización
0	Irrelevante para la organización

7.1.1Valoración de Los Activos

Tabla 4. Valoración de Activos: Datos/Información

Activo	**Dimensiones**				
	[D]	**[I]**	**[C]**	**[A]**	**[T]**
Sistema de Información PIGI	A	MA	A	A	A

Tabla 5. Valoración de Activos: Software

Activos	Dimensiones				
	[D]	[I]	[C]	[A]	[T]
Aplicativo Web MAPA	A	MA	MA	MA	MA
Aplicativo Web SIKUA	A	MA	MA	MA	MA
Office 2013 Pro	B	B	M	M	M
Microsoft Live Security	M	M	M	M	M
Microsoft Windows 7 Professional	M	M	M	M	M

Tabla 6. Valoración de Activos: Hardware

Activos	Dimensiones				
	[D]	[I]	[C]	[A]	[T]
Servidor de ficheros e impresión	A	M	M	M	M
Servidor web	MA	MA	MA	MA	MA
Servidor de bases de datos	MA	MA	MA	MA	MA
Computadoras personal	M	B	B	M	M

Tabla 7. Valoración de Activos: Red de Comunicación

Activos	Dimensiones				
	[D]	[I]	[C]	[A]	[T]
Router	MA	M	M	M	M

Tabla 8. Valoración de Activos: Equipamiento Auxiliar

Activos	Dimensiones				
	[D]	[I]	[C]	[A]	[T]
Red de Área Local	MA	A	A	A	A
Conectividad Inalámbrica	M	M	A	A	M

Tabla 9. Valoración de Activos: Personal

Activos	Dimensiones				
	[D]	[I]	[C]	[A]	[T]
Administrador de Sistema	A	A	A	A	A
Administrador de Bases de Datos	MA	MA	MA	MA	A
Desarrolladores de Software	A	A	A	MA	A
Asesoras	M	M	M	M	M

7.1.2Criterios de Valoración de Los Activos

Tabla 10. Valoración de Activos: [D] Datos/Información

Grupo de activo MAGERIT	Nombre del Activo	Dimensión de Seguridad	Criterio
Activo de Información	Sistema de Información PIGI	Confiabilidad	9
		Integridad	10
		Autenticidad	9
		Disponibilidad	9
		Trazabilidad	9

Tabla 11. Valoración de Activos: [SW] Software

Grupo de activo MAGERIT	Nombre del Activo	Dimensión de Seguridad	Criterio
Software	Aplicativo Web MAPA	Confiabilidad	10
		Integridad	9
		Autenticidad	10
		Disponibilidad	9
		Trazabilidad	10
	Aplicativo Web SIKUA	Confiabilidad	10
		Integridad	9
		Autenticidad	10
		Disponibilidad	9
		Trazabilidad	10
	Office 2013 Pro	Confiabilidad	3
		Integridad	2
		Autenticidad	3
		Disponibilidad	2
		Trazabilidad	3
	Microsoft Live Security	Confiabilidad	5
		Integridad	5
		Autenticidad	5
		Disponibilidad	5
		Trazabilidad	5
	Microsoft Windows 7 Professional	Confiabilidad	5
		Integridad	5
		Autenticidad	5
		Disponibilidad	5
		Trazabilidad	5

Tabla 12. Valoración de Activos: [HW] Hardware

Grupo de activo MAGERIT	Nombre del Activo	Dimensión de Seguridad	Criterio
Hardware	Servidor de ficheros e impresión	Confiabilidad	5
		Integridad	5
		Autenticidad	5
		Disponibilidad	7
		Trazabilidad	5
	Servidor web	Confiabilidad	10
		Integridad	10
		Autenticidad	10
		Disponibilidad	10
		Trazabilidad	10
	Servidor de bases de datos	Confiabilidad	10
		Integridad	10
		Autenticidad	10
		Disponibilidad	10
		Trazabilidad	10
	Computadoras personal	Confiabilidad	2
		Integridad	2
		Autenticidad	3
		Disponibilidad	5
		Trazabilidad	3

Tabla 13. Valoración de Activos: [COM] Red de Comunicación

Grupo de activo MAGERIT	Nombre del Activo	Dimensión de Seguridad	Criterio
Red de Comunicación	Router	Confiabilidad	5
		Integridad	5
		Autenticidad	5
		Disponibilidad	10
		Trazabilidad	5

Tabla 14. Valoración de Activos: [AUX] Equipamiento Auxiliar

	Activos	Dimensiones	Promedio
Equipamiento Auxiliar	Red de Área Local	Confiabilidad	8
		Integridad	8
		Autenticidad	8
		Disponibilidad	10
		Trazabilidad	8
	Conectividad Inalámbrica	Confiabilidad	8
		Integridad	5
		Autenticidad	8
		Disponibilidad	5
		Trazabilidad	5

Tabla 15. Valoración de Activos: [L] Personal

Grupo de activo MAGERIT	Nombre del Activo	Dimensión de Seguridad	Criterio
Personal	Administrador de Sistema	Confiabilidad	8
		Integridad	8
		Autenticidad	8
		Disponibilidad	8
	Administrador de Bases de Datos	Trazabilidad	7
		Confiabilidad	10
		Integridad	10
		Autenticidad	10
		Disponibilidad	10
		Trazabilidad	7
	Desarrolladores de Software	Confiabilidad	8
		Integridad	8
		Autenticidad	9
		Disponibilidad	8
		Trazabilidad	8
	Asesoras	Confiabilidad	5
		Integridad	5
		Autenticidad	5
		Disponibilidad	5
		Trazabilidad	5

7.2IDENTIFICACIÓN DE AMENAZAS

Las amenazas se clasifican en cuatro grandes grupos: Desastres naturales(N), de origen industrial (I), errores y fallos no intencionados (E), ataques deliberados o intencionados(A).

7.2.1Valoración de Amenazas

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: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/3232_valoracin_de_amenazas.html

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: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/3232_valoracin_de_amenazas.html

Tabla 16. Identificación y Valoración de Amenazas.

Amenaza	Activos	Frecuencia	Dimensiones				
			[A]	[C]	[I]	[D]	[T]
[N.1] Fuego	[HW] equipos informáticos.	5				100%	
	[AUX] equipamiento auxiliar.	5				100%	
	[L] instalaciones.	5				100%	
[N.2] Daños por agua	[HW] equipos informáticos.	5			20%	100%	
	[Media] soportes de información	5			20%	70%	
	[AUX] equipamiento auxiliar.	5				20%	
[N.7] Desastres naturales. Fenómeno sísmico.	[L] instalaciones.	5				100%	
	[AUX] equipamiento auxiliar.	5				100%	
	[HW] equipos informáticos.	5				100%	
	[Media] soportes de información.	5				100%	
[N.8] Desastres naturales. Fenómeno de origen volcánico.	[L] instalaciones.	5				100%	
	[AUX] equipamiento auxiliar.	5				100%	
	[HW] equipos informáticos.	5				100%	
	[Media] soportes de información.	5				100%	
[I.1] Fuego	[L] instalaciones.	5				100%	
	[HW] equipos informáticos.	5				100%	
	[Media] soportes de información	5				100%	
	[AUX] equipamiento auxiliar.	5				100%	

Tabla 16. (Continuación).

Amenaza	Activos	Frecuencia	Dimensiones				
			[A]	[C]	[I]	[D]	[T]
[I.2] Daños por agua	[HW] equipos informáticos.	5				100%	
	[Media] soportes de información	5				75%	
	[AUX] equipamiento auxiliar.	5				100%	
	[L] instalaciones.	5				100%	
[I.3] Contaminación mecánica.	[HW] equipos informáticos.	5				50%	
	Media] soportes de información.	5				50%	
	[AUX] equipamiento auxiliar.	5				50%	
[I.4] Contaminación electromagnética.	[HW] equipos informáticos.	5				5%	
	[SW] aplicaciones	10			100%	100%	
[I.5] Avería de origen físico o lógico.	(software) [HW] equipos informáticos	10			100%	100%	
	[AUX] equipamiento auxiliar.	5				100%	
	[Media] soportes de información.	5			100%	100%	
[I.6] Corte del Suministro eléctrico	[HW] equipos informáticos.	5				100%	
	[Media] soportes de información.	5			100%	100%	
	[AUX] equipamiento auxiliar.	5			100%	100%	
[I.7] Condiciones inadecuadas de temperatura o humedad	[HW] equipos informáticos (hardware)	5				75%	
[I.8] Fallo de servicios de comunicaciones	[COM] redes de comunicaciones (red inalámbrica, intranet, internet)	10			75%	75%	

Tabla 16. (Continuación).

Amenaza	Activos	Frecuencia	Dimensiones				
			[A]	[C]	[I]	[D]	[T]
[I.9] Interrupción de otros servicios y suministros esenciales	[AUX] equipamiento auxiliar	5			75%	75%	
[I.10] Degradación de los soportes de almacenamiento de la información	Media] soportes de información.	5			75%	75%	
[E.1] Errores de los usuarios.	[D] datos / información. Archivos de Contratistas.	10		20%	75%	75%	
	[D] datos / información. Archivos de Informes Jurídicos.	5		20%	75%	75%	
	[D] datos / información. Archivo de Copias de seguridad de la información	5		20%	75%	75%	
	[D] datos / información. Archivos de viabilidad Estaciones de servicio	5		20%	75%	75%	
	[D] datos / información. Contraseñas de acceso de empleados	10		20%	75%	75%	
	[keys] claves criptográficas	5		20%	75%	75%	
	[S] servicios. Servicios prestados a usuarios externos.	10		20%	75%	75%	

Tabla 16. (Continuación).

Amenaza	Activos	Frecuencia	Dimensiones				
			[A]	[C]	[I]	[D]	[T]
	[S] servicios. Servicios prestados a funcionarios tanto al interior como haciendo uso de internet.	10		20%	75%	75%	
	[S] servicios. Servicio de internet al que pueden acceder los funcionarios.	10		20%	75%	75%	
[E.2] Errores del administrador	[D] datos / información	5	75%	75%	75%	50%	50%
	[keys] claves criptográficas	5	75%	75%	75%	50%	50%
	[S] servicios	5	20%	20%	20%	20%	20%
[E.4] Errores de configuración	[SW] aplicaciones	5	75%	75%	75%	50%	50%
	[COM] redes de comunicaciones	5	75%	75%	75%	50%	50%
	[Conf.] datos de configuración	10	75%	75%	75%	75%	75%
[E.7] Deficiencias en la organización	[P] personal. Personal atención público, técnico, administrativo, archivo	5	75%	75%	75%	50%	50%
[E.8] Difusión de software dañino	[SW] aplicaciones (software)	10	20%	20%	20%		
[E.15] Alteración accidental de la información	[D] datos / información	5	20%	20%	20%		

Tabla 16. (Continuación).

Amenaza	Activos	Frecuencia	Dimensiones				
			[A]	[C]	[I]	[D]	[T]
[E.18] Destrucción de información	[D] datos / información	10	20%	20%	20%		
	[SW] aplicaciones	10		20%	20%	20%	
	[Media] soportes de información	10	50%	50%	50%	50%	
[A.6] Abuso de privilegios de acceso	[keys] claves criptográficas [S] servicios	10	50%	50%	50%	50%	
	[SW] aplicaciones	5	50%	50%	50%	50%	
[A.7] Uso no previsto	[HW] equipos informáticos	5				20%	
	[COM] redes de comunicaciones	10				20%	
	[S] servicios	10				20%	
	[SW] aplicaciones	10			50%	20%	
	HW] equipos informáticos (hardware) [COM] redes de comunicaciones	10				20%	
[A.7] Uso no previsto	[Media] soportes de información	10				20%	
	[AUX] equipamiento auxiliar	10				20%	
	[L] instalaciones	5				20%	
[A.8] Difusión de software dañino	[SW] aplicaciones	10	100%	75%	100%	100%	75%
	[D] datos / información [keys] claves criptográficas [S] servicios	10		20%	20%	75%	75%
	[SW] aplicaciones	10	75%	75%	75%	75%	75%

Tabla 16. (Continuación).

Amenaza	Activos	Frecuencia	Dimensiones				
			[A]	[C]	[I]	[D]	[T]
[A.11] Acceso no autorizado	(software) [HW] equipos informáticos (hardware)	10	50%	75%	50%	75%	50%
	[COM] redes de comunicaciones	10				75%	
	[Media] soportes de información	10				75%	
	[AUX] equipamiento auxiliar	10				75%	
	[L] instalaciones	10				75%	
[A.13] Repudio	[S] servicios	10				75%	
[A.14] Interceptación de información	[COM] redes de comunicaciones	10				75%	20%
[A.15] Modificación deliberada de la información	[D] datos / información [keys] claves criptográficas	10				75%	
	[S] servicios (acceso)	5				75%	
	[SW] aplicaciones	5				75%	
	[D] datos / información [keys] claves criptográficas	5				75%	
	[S] servicios (acceso)	5				75%	
[A.18] Destrucción de información	[SW] aplicaciones	5			75%	75%	75%
	[Media] soportes de información	5				75%	
	[D] datos / información [keys] claves criptográficas	5				75%	

Tabla 16. (continuación).

Amenaza	Activos	Frecuencia	Dimensiones				
			[A]	[C]	[I]	[D]	[T]
[A.19] Revelación de información	[S] servicios (acceso)	5				75%	
	[Media] soportes de información	5				75%	
[A.22] Manipulación de programas	[SW] aplicaciones	10				75%	
	[HW] equipos	5				75%	
[A.23] Manipulación de los equipos	[Media] soportes de información	5				75%	
	[AUX] equipamiento auxiliar	5				75%	
	[S] servicios	5				75%	
A.24] Denegación de servicios	[HW] equipos informáticos (hardware)	5				75%	
	[COM] redes de comunicaciones	5		50%	50%	75%	
	[HW] equipos informáticos	5				75%	
[A.25] Robo	[Media] soportes de información	5		20%	20%	100%	20%
	[AUX] equipamiento auxiliar	5				100%	
	[HW] equipos informáticos	5				100%	
[A.28] Indisponibilidad del personal	[P] personal interno	5				100%	
[A.29] Extorsión	[P] personal interno	5				100%	
[A.30] Ingeniería social	[P] personal interno	5				100%	

7.2.1.1 Comprobación Puertos Abiertos Con NMAP

Nmap es una conocida herramienta para realizar auditorías de seguridad de sistemas y redes que nos permite conocer una gran cantidad de información sobre estos. Una de las funciones que nos permite realizar es comprobar los puertos que están abiertos o cerrados en un sistema remoto como por ejemplo un servidor local para poderlo proteger correctamente y tomar las medidas necesarias.
Para realizar un escaneo básico de puertos se debe digitar la IP del servidor a escanear y en “Perfil” se selecciona “Intense SCAN, ALL TCP Ports”.

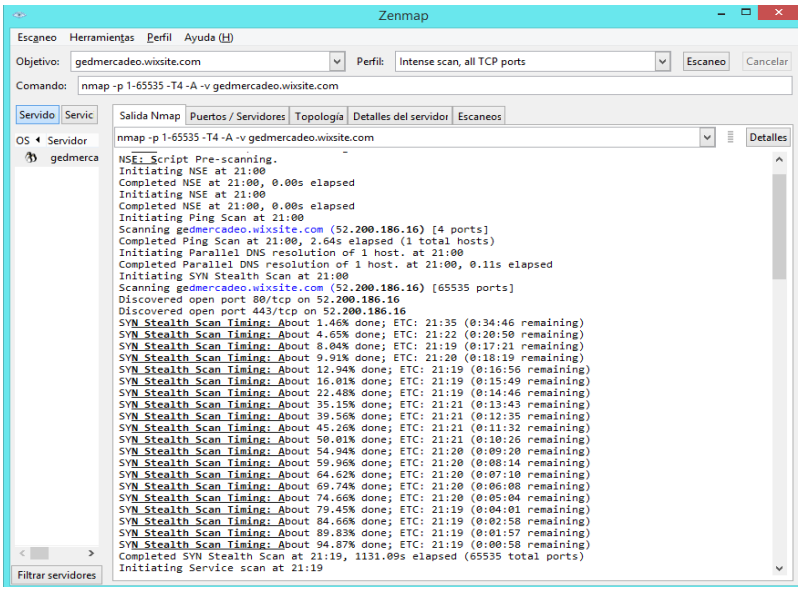


Figura 5. Escaneo básico

El comando que se ejecutó con el análisis intenso muestra información sobre todos los puertos TCP abiertos, servicios en ejecución y detalles sobre el dispositivo y sistema operativo que utiliza.
En la pestaña de Puertos se puede ver todos los puertos abiertos en el servidor remoto y el servicio que está haciendo uso de ellos.

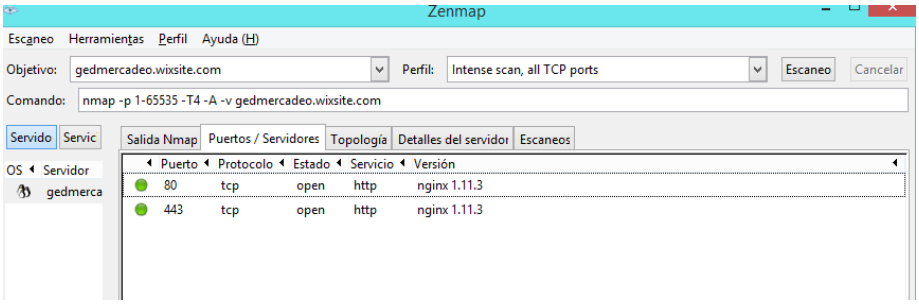


Figura 6. Puertos

7.2.2Estimación del Impacto

Los impactos se muestran en una escala de colores de acuerdo a su valor:

[10]: Crítico
[9,8]: Muy alto
[6,7]: Alto
[4,5]: Medio
[2,3]: Bajo
[0,1]: Despreciable

Tabla 17.Impacto sobre cada uno de los activos de información

Activos	Amenazas	Impacto				
		[A]	[C]	[I]	[D]	[T]
[D] Datos/Información	[N.1] Fuego	6	6			
	[N.2] Daños por agua	6	6			
	[N.*] Desastres naturales	6	6			
	[I.5] Avería de origen físico o lógico	6	6			
	[I.7] Condiciones inadecuadas de temperatura o humedad	4	4			
	[E.20] Vulnerabilidades de los programas (software)	3	3	3	3	
	[E.21] Errores de mantenimiento / actualización de programas (software)	5	5	5		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	5			
	[A.5] Suplantación de la identidad del usuario	7	7	7	7	
	[A.11] Acceso no autorizado			7	7	

Tabla 17. (Continuación)

[SW] Software	[I.5] Avería de origen físico o lógico	7	7			
	[E.1] Errores de los usuarios	5	5	5	5	
	[E.8] Difusión de software dañino	3	3	3	3	
	[E.20] Vulnerabilidades de los programas (software)	5	5	5	5	
	[E.21] Errores de mantenimiento / actualización de programas (software)	5	5	5		
	[A.7] Uso no previsto	3	3	3	3	
	[I.7] Condiciones inadecuadas de temperatura o humedad	9	9			
	[E.2] Errores del administrador del sistema / de la seguridad	5	5	5	5	
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	5			
	[A.11] Acceso no autorizado			7	7	
[HW] Hardware	[N.1] Fuego	5				
	[N.2] Daños por agua	5				
	[N.*] Desastres naturales	5				
	[I.*] Desastres industriales	3				
	[I.5] Avería de origen físico o lógico	5				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5				
	[E.24] Caída del sistema por agotamiento de recursos	5				
	[A.6] Abuso de privilegios de acceso	5	5			
	[A.7] Uso no previsto	5	5			

Tabla 17. (Continuación)

[COM] Red De Comunicación	[E.24] Caída del sistema por agotamiento de recursos	9				
	[E.2] Errores del administrador	3				
	[E.9] Errores de [re-]encaminamiento		3			
	[A.12] Análisis de tráfico		5	5		
	[A.14] Interceptación de información (escucha)			7		
	[A.24] Denegación de servicio	7				
	[A.9] [Re-]encaminamiento de mensajes			7	7	
	[A.10] Alteración de secuencia			7	7	
[COM] Equipamiento Auxiliar	[A.11] Acceso no autorizado	9				
	[E.24] Caída del sistema por agotamiento de recursos	9				
	[E.2] Errores del administrador	3				
	[E.9] Errores de [re-]encaminamiento		3			
	[A.12] Análisis de tráfico		5	5		
	[A.14] Interceptación de información (escucha)			7		
	[A.24] Denegación de servicio	7				
	[A.9] [Re-]encaminamiento de mensajes			7	7	
[L] Personal	[A.10] Alteración de secuencia	5				
	[A.11] Acceso no autorizado	5				
	[E.19] Fugas de información				7	
	[E.28] Indisponibilidad del personal	5				
	[E.7] Deficiencias en la organización	5				
	[A.28] Indisponibilidad del personal	5				

7.2.3Estimación del Riesgo

Tabla 18.Valores de frecuencia

Valor			Criterio
100	Muy frecuente	MF	A diario
10	Frecuente	F	Mensualmente
1	Normal	FN	Una vez al año
1/10	Poco frecuente	PF	Cada varios años

Se combina el impacto y frecuencia para calcular el riesgo:

Estimación Del Estado De Riesgo

Tabla 19.Valor estimación de riesgo

		FRECUENCIA			
RIESGO		PF	FN	F	MF
IMPACTO	**MA**	**M**	**A**	**MA**	**MA**
	A	**B**	**A**	**MA**	**MA**
	M	**B**	**M**	**A**	**A**
	B	**MB**	**B**	**M**	**A**
	MB	**MB**	**MB**	**B**	**B**

Fuente: Magerit V.3 – Libro II - Catálogo de Elementos

Tabla 20 Valoración de riesgo en activos de información

Activos	Amenazas	Impacto					Frecuencia	Riesgo
		[A]	[C]	[I]	[D]	[T]		
[D] Datos/Información	[N.1] Fuego	A	A	A	A	A	FN	A
	[N.2] Daños por agua	A	A	A	A	A	FN	A
	[N.*] Desastres naturales	A	A	A	A	A	FN	A
	[I.5] Avería de origen físico o lógico	A	A	A	A	A	FN	A
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	M	M	M	M	FN	M
	[E.20] Vulnerabilidades de los programas (software)	B	B	B	B	B	FN	B
	[E.21] Errores de mantenimiento / actualización de programas (software)	M	M	M	M	M	FN	M
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M	M	M	M	FN	M
	[A.5] Suplantación de la identidad del usuario	A	A	A	A	A	FN	A
	[A.11] Acceso no autorizado	A	A	A	A	A	FN	A
[SW] Software	[I.5] Avería de origen físico o lógico	A	A	A	A	A	FN	A
	[E.1] Errores de los usuarios	M	M	M	M	M	FN	M
	[E.8] Difusión de software dañino	B	B	B	B	B	FN	B
	[E.20] Vulnerabilidades de los programas (software)	M	M	M	M	M	FN	M
	[E.21] Errores de mantenimiento / actualización de programas (software)	M	M	M	M	M	FN	M
	[A.7] Uso no previsto	B	B	B	B	B	FN	B
	[I.7] Condiciones inadecuadas de temperatura o humedad	MA	MA	MA	MA	MA	FN	A
	[E.2] Errores del administrador del sistema / de la seguridad	M	M	M	M	M	FN	M
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M	M	M	M	FN	M
	[A.11] Acceso no autorizado	A	A	A	A	A	FN	A

Tabla 20. (Continuación)

Activos	Amenazas	Impacto					Frecuencia	Riesgo
		[A]	[C]	[I]	[D]	[T]		
[HW] Hardware	[N.1] Fuego	M	M	M	M	M	PF	B
	[N.2] Daños por agua	M	M	M	M	M	PF	B
	[N.*] Desastres naturales	M	M	M	M	M	PF	B
	[I.*] Desastres industriales	B					PF	MB
	[I.5] Avería de origen físico o lógico	M	M	M	M	M	FN	M
	[I.7] Condiciones inadecuadas de temperatura o humedad	M	M	M	M	M	FN	M
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M	M	M	M	M	FN	M
	[E.24] Caída del sistema por agotamiento de recursos	M	M	M	M	M	FN	M
	[A.6] Abuso de privilegios de acceso	M	M	M	M	M	FN	M
	[A.7] Uso no previsto	M	M	M	M	M	FN	M
[COM] Red De Comunicación	[E.24] Caída del sistema por agotamiento de recursos	MA	A	A	A	A	F	MA
	[E.2] Errores del administrador	B	B	B	B	B	FN	MB
	[E.9] Errores de [re-]encaminamiento	B	B	B	B	B	FN	MB
	[A.12] Análisis de tráfico	M	M	M	M	M	FN	M
	[A.14] Interceptación de información (escucha)	A	A	A	A	A	FN	A
	[A.24] Denegación de servicio	A	A	A	A	A	FN	A
	[A.9] [Re-]encaminamiento de mensajes	A	A	A	A	A	FN	A
	[A.10] Alteración de secuencia	A	A	A	A	A	FN	A

Tabla 20. (Continuación)

Activos	Amenazas	Impacto					Frecuencia	Riesgo
		[A]	[C]	[I]	[D]	[T]		
	[A.11] Acceso no autorizado	MA	A	A	A	A	FN	M
[COM] Equipamiento Auxiliar	[E.24] Caída del sistema por agotamiento de recursos	MA	A	A	A	A	F	A
	[E.2] Errores del administrador	B	B	B	B	B	FN	MB
	[E.9] Errores de [re-]encaminamiento	B	B	B	B	B	FN	MB
	[A.12] Análisis de tráfico	M	M	M	M	M	FN	M
	[A.14] Interceptación de información (escucha)	A	A	A	A	A	FN	A
	[A.24] Denegación de servicio	A	A	A	A	A	FN	A
	[A.9] [Re-]encaminamiento de mensajes	A	A	A	A	A	FN	A
[L] Personal	[A.10] Alteración de secuencia	M	M	M	M	M	FN	M
	[A.11] Acceso no autorizado	M	M	M	M	M	FN	M
	[E.19] Fugas de información	A	A	A	A	A	FN	A
	[E.28] Indisponibilidad del personal	M	M	M	M	M	FN	M
	[E.7] Deficiencias en la organización	M	M	M	M	M	FN	M
	[A.28] Indisponibilidad del personal	M	M	M	M	M	FN	M

Los resultados generales obtenidos del análisis de riesgos se reflejan principalmente con el poco conocimiento de cómo se deben aplicar las normas de seguridad de la información y que al no tomar las medidas necesarias se compromete la imagen de la organización frente a sus clientes.

Esto se debe a la falta de cultura sobre los temas relacionados con la seguridad de la información, el establecer responsables, el cumplimiento de políticas y procedimientos de seguridad en una organización, no contar con inventarios de los activos lo cual dificulta su protección frente a los riesgos y amenazas a las que se pueden enfrentar.

8. DECLARACION DE APLICABILIDAD

Revisar y verificar la existencia de controles que ayude a definir la existencia de políticas y procedimientos de seguridad en GED.

Tabla 21. Lista de chequeo basada en la norma ISO 27001

EVALUACION DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN						
CONTROL	**VERIFICAR**	**APLICA**	**NO APLICA**	**EN PROCESO**	**VERBAL**	**DOCUMENTO**
5.1.1 Políticas de seguridad de la información	**Existen políticas de seguridad en el manual de sistemas**		**X**			
5.1.2 Revisión de las políticas para la seguridad de la información	**Las políticas se revisan según los tiempos establecidos por el área de sistemas**		**X**			
EVALUACION DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN						
6.1.1 Roles y responsabilidades para la seguridad de la información	**Se define y asigna todas las responsabilidades de la seguridad de la información.**		**X**			
6.1.2 Separación de deberes	**La seguridad de la información es coordinada por los jefes de cada área de la organización.**		**X**			
6.1.5 Seguridad de la información en la gestión de proyectos	**Se revisan los acuerdos donde se establecen los requisitos de confidencialidad, no divulgación para la protección de la información.**		**X**			

Tabla 21. (Continuación)

EVALUACION DE SEGURIDAD DE LOS RECURSOS HUMANOS						
CONTROL	**VERIFICAR**	**APLICA**	**NO APLICA**	**EN PROCESO**	**VERBAL**	**DOCUMENTO**
7.1.1 Selección	**Se cuenta con procedimientos para la selección de personal que incluye investigación de antecedentes.**		**X**			
7.2.1 Responsabilidades de la dirección	**La dirección exige a los empleados el tener clara sus responsabilidades respecto a la seguridad de información**		**X**			
EVALUACION DE GESTIÓN DE ACTIVOS						
8.1.3 Uso aceptable de los activos	**Se identifica, documenta e implementan reglas para el uso de la información y de los activos asociados con la información.**		**X**			
EVALUACION DE CONTROL DE ACCESOS						
CONTROL	**VERIFICAR**	**APLICA**	**NO APLICA**	**EN PROCESO**	**VERBAL**	**DOCUMENTO**
9.1.1 Política de control de acceso	**Se controla el acceso a la información al establecer, documentar y revisar una política de control de acceso con base en los requisitos de la Organización.**		**X**			

Tabla 21. (Continuación)

9.2.1 Registro y cancelación del registro de usuarios	**Los equipos están protegidos para reducir el riesgo de amenazas, así como el acceso no autorizado.**		**X**			
9.4.1 Restricción de acceso a la información	**Se evita que usuarios no autorizados tengan acceso a los sistemas de información.**		**X**			
EVALUACION DE SEGURIDAD FÍSICA Y DEL ENTORNO						
CONTROL	**VERIFICAR**	**APLICA**	**NO APLICA**	**EN PROCESO**	**VERBAL**	**DOCUMENTO**
11.1.1 Perímetro de seguridad física	**Se limita la posibilidad de pérdida de activos de información definiendo perímetros de seguridad física.**		**X**			
11.1.4 Protección contra amenazas externas y ambientales	**Se protegen los activos de información contra desastres naturales, ataques maliciosos o accidentes.**		**X**			
11.2.3 Seguridad del cableado	**El cableado de energía eléctrica y de comunicaciones está protegido contra interceptación, interferencia o daño.**		**X**			
11.2.4 Mantenimiento de equipos	**Los equipos se mantienen correctamente para asegurar su disponibilidad continua.**	**X**				

Tabla 21. (Continuación)

EVALUACION DE SEGURIDAD DE LAS OPERACIONES						
CONTROL	**VERIFICAR**	**APLICA**	**NO APLICA**	**EN PROCESO**	**VERBAL**	**DOCUMENTO**
12.1.2 Gestión de cambios	**Controlar los cambios en procesos, instalaciones y sistemas de procesamiento de información que afectan la seguridad de la organización.**		**X**			
12.3.1 Respaldo de la información	**Se realizan copias de seguridad de información, del software de acuerdo a las políticas de copias de respaldo (Backup).**	**X**				
12.6.2 Restricciones en la instalación de software	**Se establecen las reglas con las que se rigen la instalación de software.**		**X**			
12.7.1 Controles de auditorías de sistemas de información	**Se realizan auditorías para verificar los sistemas de información con el fin de minimizar las interrupciones en los procesos.**		**X**			
EVALUACION DE SEGURIDAD DE LAS COMUNICACIONES						
CONTROL	**VERIFICAR**	**APLICA**	**NO APLICA**	**EN PROCESO**	**VERBAL**	**DOCUMENTO**
13.1.1.Controles de redes	**Se establece la gestión y control para proteger la información.**		**X**			
13.1.2 Seguridad de los servicios de red	**Se aseguran los servicios en la red.**		**X**			
13.2.4Acuerdos de confidencialidad o de no divulgación	**Se establecen acuerdos de confidencialidad o de no divulgación.**	**X**				

Tabla 21. (Continuación)

EVALUACION DE CUMPLIMIENTO						
CONTROL	**VERIFICAR**	**APLICA**	**NO APLICA**	**EN PROCESO**	**VERBAL**	**DOCUMENTO**
18.1.3 Protección de registros	**Se protegen los registros contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo de acuerdo con los requisitos de la Organización.**		**X**			
18.1.4 Privacidad y protección de información de datos personales	**Se protege la privacidad de la información de datos personales, como se establece en la ley.**	**X**				
18.2.2 Cumplimiento con las políticas y normas de seguridad	**Se revisan en los tiempos planificados o cuando ocurran cambios significativos, incluyendo la participación de las principales autoridades de la Organización.**		**X**			

9. DISEÑO DE UN SISTEMA DE SEGURIDAD INFORMATICA

9.1 Objetivo del Sistema de Gestión de Seguridad Informática

Establecer las políticas y normas para la protección de la información de la empresa GED (Gestión estrategia y desarrollo) de la ciudad de Bogotá.

9.2Alcance del Sistema de Gestión de Seguridad Informática

Diseñar el sistema de gestión de seguridad de la información y sus respectivas normas para establecer cuáles son las mejores prácticas en cuanto a la gestión de los riesgos y amenazas de la empresa GED (Gestión estrategia y desarrollo) de la ciudad de Bogotá.

Tabla 22. Dominios y procesos seleccionados

CONTROL
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
5.1.1 Políticas de seguridad de la información **5.1.2 Revisión de las políticas para la seguridad de la información**
EVALUACION DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
6.1.1 Roles y responsabilidades para la seguridad de la información
6.1.2 Separación de deberes
6.1.5 Seguridad de la información en la gestión de proyectos
EVALUACION DE SEGURIDAD DE LOS RECURSOS HUMANOS
7.1.1 Selección
7.2.1 Responsabilidades de la dirección
EVALUACION DE GESTIÓN DE ACTIVOS
8.1.3 Uso aceptable de los activos
EVALUACION DE CONTROL DE ACCESOS
9.1.1 Política de control de acceso
9.2.1 Registro y cancelación del registro de usuarios

Tabla 22. (Continuación)

9.4.1 Restricción de acceso a la información
EVALUACION DE SEGURIDAD FÍSICA Y DEL ENTORNO
11.1.1 Perímetro de seguridad física
11.1.4 Protección contra amenazas externas y ambientales
11.2.3 Seguridad del cableado
11.2.4 Mantenimiento de equipos
EVALUACION DE SEGURIDAD DE LAS OPERACIONES
12.1.2 Gestión de cambios
12.3.1 Respaldo de la información
12.6.2Restricciones en la instalación de software
12.7.1 Controles de auditorías de sistemas de información
EVALUACION DE SEGURIDAD DE LAS COMUNICACIONES
13.1.1.Controles de redes
13.1.2 Seguridad de los servicios de red
13.2.4Acuerdos de confidencialidad o de no divulgación
EVALUACION DE CUMPLIMIENTO
18.1.3 Protección de registros
18.1.4 Privacidad y protección de información de datos personales
18.2.2 Cumplimiento con las políticas y normas de seguridad

9.3 Plan De Auditoría Interna

FORMATO PARA LA PROGRAMACIÓN DE EL PLAN DE AUDITORIA INTERNA

PROGRAMA DE AUDITORIA INTERNA				
NUMERO DE AUDITORIA	**ALCANCE DE LA AUDITORIA**	**HOJA DE RUTA**	**AUDITOR**	**FECHA DE EJECUCION**
PROGRAMACION				
DIA / HORA	**PROCESO**		**DOCUMENTOS / REGISTROS REQUERIDOS**	
REVISION Y APROBACION DEL PROGRAMA DE AUDITORIA				
OBSERVACIONES:	**REVISADO POR:** **FIRMA** _____ **FECHA** _____		**APROBADO POR:** **FIRMA** _____ **FECHA** _____	

Objetivo

Identificar el nivel de cumplimiento del Sistema de Gestión de la Seguridad de la Información de GED con respecto a los controles de la norma ISO 27001:2013.

Alcance

Las actividades de la auditoría se realizaran en todas las áreas de la empresa.

Lugar

La auditoría al SGSI se realizaran GED.

Áreas Auditadas

Se auditaran todas las áreas de GED, las que están relacionadas con el alcance del SGSI, el área Administrativa y Tecnología.

Personal Auditado

Se auditara al siguiente personal de GED

- Gerente General
- Director Administrativo y Financiero
- Director de Tecnología
- Asesoras

Verificación de Controles

Cuando se complete la auditoria se realiza la revisión de los hallazgos y de resultados, incluida las observaciones de las entrevistas, se enumera las áreas de mejora y las acciones correctivas que se van a realizar.

Presentación de hallazgos a la Gerencia

Informe formal para comunicar los objetivos, el alcance, las observaciones y hallazgos que debe evaluar y facilitar las acciones correctivas.

10 RESULTADOS

Con el desarrollo del proyecto se obtuvo los siguientes resultados, la actividad inicial se efectúo con el fin de identificar las necesidades de la empresa con respecto al sistema de Gestión de Seguridad de la Información, para este diagnóstico se utilizó métodos de recolección y evaluación de la información.

La Evaluación se realizó debido a que se laboró en la empresa y se conoce el estado de esta en cuanto a la seguridad de la información.

En la Empresa no se tienen resultados anteriores de auditorías, así que no se cuenta con información que evidenciara las debilidades en cuanto a la seguridad de la información.

A continuación las situaciones que se identifican en el diagnóstico de la situación de la empresa:

• No hay concientización y conocimiento sobre los temas de seguridad por parte de los colaboradores.
• Los colaboradores no entienden la diferencia que hay entre seguridad informática y seguridad de la información.
• No se han definido los controles de seguridad.
• No hay políticas de seguridad.

Hardware

•No esta definida la restricción del uso de dispositivos de almacenamiento (USB, disco duros externos), se cuenta con protección Antivirus y spyware para evitar el riesgo por contagio de virus, pero las unidades de almacenamiento USB o disco duros externos pueden infectar el sistema.
•Si se presenta una falla de hardware en un equipo con información crítica no está estipulado un plan de contingencia para realizar el proceso de recuperación de la información de una manera rápida.

Software:

•No están definidos los registros de las actualizaciones de software o parches de seguridad en los sistemas críticos.

Instalación Física:

•En la empresa el estado del cableado estructurado no es el adecuado aunque es tipo UTP categoría 6 no cumple con las normas de instalación, en el caso de un rack de cableado, patch-cord, patchpanel, esta desorganizado y sin seguridad (Cualquier persona puede tener acceso al cableado o switch).
•En cuanto a la condición de seguridad el lugar donde se encuentra el cableado principal y los servidores, no cuentan con un sistema de prevención contra incendio, no hay cámaras de seguridad y no hay un control de acceso a estos lugares.

10.1 Política de Seguridad de la Información

La información es el recurso de mayor valor para GED, la cual debe ser protegida de forma debida. Establecer, mantener y seguir con un proceso de mejora continua para la aplicación de la Política de Seguridad de la Información que garantice el compromiso de proteger la información frente a diferentes amenazas, con esta política se trata de minimizar los riesgos y de que se asegure el cumplimiento de estas funciones.

10.1.1 Objetivos

Proteger y preservar los recursos de información de GED además de las herramientas que se utilizan para su procesamiento frente a las amenazas internas o externas, y así se pueda dar cumplimiento de la confidencialidad, integridad, disponibilidad y no repudio de la información.

10.1.2 Objetivos Específicos

Establecer las medidas de seguridad en cuanto al acceso, uso y la administración de la información.

Explicar a los colaboradores y a quienes tenga acceso a la información de las responsabilidades del uso de esta.

Indicar el desarrollo, implantación, mantenimiento y cumplimiento de las medidas de seguridad con la respectiva relación de los recursos humanos, tecnológicos y económicos.

10.2 Alcance

Esta política de Seguridad de la Información la debe cumplir cada uno de los colaboradores, clientes y directivos de GED que tengan acceso a la información.

10.3 Cumplimiento de la Política de Seguridad de la Información

Se debe dar cumplimiento a las políticas de seguridad de la Información, al igual que los estándares de seguridad por parte de los colaboradores, clientes y directivos quienes deben estar al tanto del rol que deben asumir en cuanto a la responsabilidad que adquieren al acceder, usar y manejar la información de GED, conociendo que al incumplir esta política deberán asumir las acciones disciplinarias que estén bajo los estatutos de la Organización.

10.4 Política de Seguridad de la Información

Estas políticas de Seguridad de la Información que GED va a practicar y serán desarrolladas con los estándares de seguridad y de gestión se efectúan así:

10.4.1 Protección de Activos de Información

Los Activos de información se protegerán de acuerdo al nivel de clasificación de estos.

El usuario está en la obligación de proteger el equipo que está bajo su responsabilidad, cuando no lo utilice y este contenga información confidencial.

El usuario tiene la responsabilidad de evitar alguna fuga de información de la Empresa que se encuentre almacenada en el equipo que tenga asignado.

10.4.2 Seguridad Física

GED aplicara las mejores prácticas de seguridad.

El cable de red se instalará de forma separada de cualquier otro tipo de cable, de corriente o energía eléctrica con el fin de evitar interferencias.

Los equipos con información crítica deben ubicarse en áreas seguras, con un nivel de seguridad que sea verificable y se maneje por la persona responsable de ese activo.

No se deberá dejar información que pueda estar expuesta a robo o manipulación, sin importar en que medio se encuentre, de forma que pueda ser adquirida por terceros que no deben tener acceso a esta información.

Se deberá llevar un cronograma para el mantenimiento preventivo y otro para el mantenimiento correctivo que se les hará a los equipos.

Las áreas de trabajo deben tener en su inventario, herramientas como extintores, alarmas contra incendios, necesarias para salvaguardar la información y sus recursos tecnológicos.

El ingreso a las áreas de almacenamiento y tratamiento de información crítica (área de informática) deberá ser registrada.

El suministro de energía eléctrica para los equipos debe ser independiente, el circuito que se utilice no se le deben conectar equipos que exijan gran cantidad de energía.

El suministro de la energía eléctrica debe estar polarizado (polo a tierra).

Las áreas de trabajo deben contar con el suministro e instalación de UPS para poder proteger la información y evitar la interrupción y problemas eléctricos que afecten las labores de la Empresa.

La sala o áreas donde se procesa la información deben contar con señalización, sobre el acceso, alimentos u otra actividad.

10.4.3 Control de Acceso

Para el acceso a las instalaciones se debe contar con una identificación y respectiva autenticación.

Control de acceso lógico de los empleados a los Sistemas de información de la empresa.

Todos los empleados de la empresa (asesoras, desarrolladores, y demás) son responsables del usuario y contraseña que recibe para el uso y acceso de los recursos tecnológicos.

Los empleados no deben proporcionar información a personal externo, sobre los mecanismos de control de acceso a la instalación e infraestructura tecnológica de GED, a menos que tenga el permiso del proporcionar la información por parte del director de informática de la empresa.

GED proporciona a sus colaboradores los recursos tecnológicos necesarios para que desempeñen sus funciones, por tal motivo no se permite el uso de dispositivos móviles o fijos (portátiles, enrutadores, tablets) que no estén autorizados por el área de sistema.

El área de sistemas suministra a los usuarios las claves para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, estas son de uso personal e intransferible. Esta bajo responsabilidad del usuario el uso que se les dé a las claves asignadas.

Solo el personal designado por el área de informática está autorizado para la instalación de software en los equipos, servidores e infraestructura de telecomunicaciones de GED.

10.4.4 Cumplimiento y Gestión

GED se encargara de gestionar todo lo relacionado con los requisitos legales.

GED proporciona a sus empleados todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales son contratados, por tal motivo no se permite conectar a la red o instalar dispositivos (tales como portátiles, enrutadores, tablets) que no sean autorizados por el área de informática.

GED suministra a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo que le dé a las claves asignadas.

10.5 Declaración de Aplicabilidad

Tabla 23. Declaración de Aplicabilidad y controles

DECLARACION DE APLICABILIDAD			
OBJETIVOS DE CONTROL **POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**CONTROL**	**APLICABLE**	**JUSTIFICACION**
5.1.1 Políticas de seguridad de la información	**Crear la documentación donde se detalle las políticas y estándares de seguridad de la información, estos deben ser aprobados por la Dirección, luego deben ser divulgados a todos los empleados.**	**SI**	**GED** (Gestión estrategia y desarrollo) de la ciudad de Bogotá **se debe regir por estas políticas**
			Definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a las partes y las partes externas pertinentes.
			Todas las áreas de la organización deben tener la misma atención en los niveles de seguridad para la protección de la información.
5.1.2 Revisión de las políticas para la seguridad de la información	**Revisar anualmente las políticas de seguridad de información con el fin de garantizar la protección de la información.**	**SI**	**Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúa.**
EVALUACION DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
6.1.1 Roles y responsabilidades para la seguridad de la información	**Respaldar la iniciativa de seguridad con el compromiso de asignar y aprobar las responsabilidades en la seguridad de la información dentro de la Empresa.**	**SI**	**Compromiso de las principales autoridades de GED (Gestión estrategia y desarrollo) de la ciudad de Bogotá junto con los jefes de cada área.** **Se debe definir y asignar todas las responsabilidades de la seguridad de la información.**
6.1.5 Seguridad de la información en la gestión de proyectos	**Verificar la seguridad de la información que se tiene en cuenta en la Planeación de los proyectos.**		**La seguridad de la información se debe tratar en la gestión de proyectos de la organización.**
EVALUACION DE SEGURIDAD DE LOS RECURSOS HUMANOS			
7.1.1 Selección	**Definir y documentar el rol y la responsabilidad de la seguridad de los colaboradores, de acuerdo con la política de seguridad de la información de la organización.**	**SI**	**Políticas institucionales en relación con la selección de Personal**
7.2.1 Responsabilidades de la dirección	**Realizar la revisión de los antecedentes de los candidatos al empleo conforme a los requerimientos de la Organización y de la información a la cual se tiene acceso.**		**GED realiza una inducción acerca de la importancia de la seguridad de la información y el cumplimiento de las políticas.** **La dirección debe exigir a todos los colaboradores y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por GED.**

Tabla 23. (Continuación)

EVALUACION DE GESTIÓN DE ACTIVOS			
8.1.1 Inventario de activos	**Los activos deben estar identificados, elaborando un inventario.**	**SI**	**Realizar el inventario y clasificación de los activos de información.**
8.1.3 Uso aceptable de los activos	**Como obligación los empleados deben conocer las políticas para el uso de los recursos tecnológicos.**		**Estas Políticas deben estar registradas en el Manual de seguridad de la Información, además del manejo de la información y el uso de los Recursos tecnológicos.**
EVALUACION DE CONTROL DE ACCESOS			
9.1.1 Política de control de acceso	**Los perímetros de seguridad se deben utilizar para proteger el área donde está la información y los recursos para su procesamiento y almacenamiento.**	**SI**	**Establecer, documentar y revisar controles de acceso a la información**
9.4.1 Restricción de acceso a la información	**Los usuarios deben tener acceso a los servicios para los cuales tienen autorización.**		**Política de seguridad en relación con el Control de Acceso.**
EVALUACION DE SEGURIDAD FÍSICA Y DEL ENTORNO			
11.1.1 Perímetro de seguridad física	**Control de acceso de acuerdo a las necesidades de seguridad de la Organización.**	**SI**	**Se deben establecer políticas de control de acceso a la organización.** **Protegerlas áreas que contengan información confidencial además de las instalaciones de manejo de información.**
DECLARACION DE APLICABILIDAD			
CONTROL **POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**CONTROL**	**APLICABLE**	**JUSTIFICACION**
11.1.4 Protección contra amenazas externas y ambientales	**Sistema de protección con UPS y Planta Eléctrica, extintores y las condiciones de control de acceso seguro.**	**SI**	**Implementar la protección física contra desastres naturales o ataques maliciosos.** **Se debe instalar UPS y una planta eléctrica, contar con extintores para sala de informática y control de acceso para personal externo.**
11.2.3 Seguridad del cableado	**Revisar que el cableado de datos se encuentra protegido de acuerdo con lo establecido en la norma IEEE 568B.**		**Los cables de energía y telecomunicaciones se debe proteger de interceptación, interferencia o daño.**

Tabla 23. (Continuación)

12.3.1 Respaldo de la información	**Control para mantener la información disponible cuando se necesite.**	**SI**	**Realizar copias de respaldo de la información, software e imágenes de los sistemas y establecer pruebas de acuerdo con políticas de copias de respaldo.**
12.6.2Restricciones en la instalación de software	**Control del Uso de los Recursos Tecnológicos.**		**Políticas de seguridad relacionadas con el uso de los Recursos Tecnológicos.**
			Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.
12.7.1 Controles de auditorías de sistemas de información	**Controlar y revisar la ejecución de auditorías de Sistemas de Información.**		**Políticas de seguridad en relación a las auditorias que se realizan.**
EVALUACION DE SEGURIDAD DE LAS COMUNICACIONES			
13.1.1.Controles de redes	**Realizar la gestión para los equipos activos monitoreando el comportamiento del tráfico de la red con Wireshark.**	**SI**	**Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.**
13.1.2 Seguridad de los servicios de red	**Documentar la Seguridad de los servicios de red.**		**Identificar los mecanismos de seguridad y los niveles de servicio de todos los servicios de red para incluirlos en los acuerdos de los servicios de red.**
13.2.4Acuerdos de confidencialidad o de no divulgación	**Realizar acuerdos de confidencialidad para los empleados.**		**Se deben identificar, revisar y documentar los requisitos para los acuerdos de confidencialidad o de no divulgación para la protección de la información.**
EVALUACION DE CUMPLIMIENTO			
18.1.3 Protección de registros	**Proteger los registros**	**SI**	**Proteger contra pérdida, destrucción y de acceso no autorizado de acuerdo con las leyes y reglamentoscontractuales de GED.**
18.1.4 Privacidad y protección de información de datos personales	**Ley 1588 de Protección de datos personales.**		**Asegurar la privacidad y protección de la información de datos personales, como estipula en la legislación.**
18.2.2 Cumplimiento con las políticas y normas de seguridad	**Realizar actas de comité de calidad del proceso gestión de recursos informáticos.**		**Revisar con regularidad el cumplimiento del procesamiento de la información a través de auditoría interna.**

11 RECOMENDACIÓN

Se debe socializar las vulnerabilidades y el análisis de riesgos de seguridad para la empresa GED para que se pueda ejecutar los controles de acuerdo a la norma ISO 27002 para definir las políticas y procedimientos de seguridad.

Para el diseño del Sistema de Gestión de Seguridad de la Información es necesariocapacitara los colaboradores en temas de seguridad informática y a quienes estén involucrados con GED.
Se debe evaluar y aprobar las políticas concebidas dentro de este proyecto.
Los controles de seguridad de acuerdo al resultado del análisis de riesgos deben ser realizados en la mayor brevedad posible.
Los directivos deben tener en cuentala seguridad informática, e incluir los recursos necesarios para su diseño.
Los colaboradores de la empresa deben recibir capacitación sobre el desarrollo del proyecto para el conocimiento y adaptación a la política de cambio sobre la seguridad informática.
Se deben realizar auditorías a los activos de información para actualizar los controles que permitan la mejora de prácticas que estén relacionadas con la seguridad de la información.

12 DIVULGACION

El proyecto DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA GED (GESTION ESTRATEGIA Y DESARROLLO) tendrá como medio de divulgación el repositorio de la universidad, en donde se podrá consultar por personas externas y los estudiantes de los programas académicos de la Universidad Nacional Abierta y a Distancia “UNAD”.

CONCLUSIONES

El presente proyecto cumplio con los objetivos propuestos para el Diseño de un sistema de gestion de seguridad de la información en GED, se realizó la identificación de los activos de información mediante entrevistas, cuestionarios y listas de chequeo, se determinó las vulnerabilidades, amenazas y riesgos donde se identificaron los activos críticos y que requieren de atención y de controles y políticas de seguridad.

Se reviso y verifico la existencia de controles para definir cuales son los adecuados para fortalecer y asegurar la información que es parte del desarrollo de las labores de la organización.
GED es una organización que tiene contratos con diferentes empresas de la ciudad y debe establecer políticas que protejan y garanticen la seguridad de la información de cualquier tipo de amenazas.

El diseño del sistema de gestión de la seguridad de la información permite el desarrollo de gestión de cada proceso de la empresa por medio de estándares, técnicas y metodologías como la ISO 27001-27002 para lograr mitigar los riesgos que puedan presentar, además de reducir el riesgo, aumentar la confiabilidad, integridad y disponibilidad de la información lo cual se logra con el apoyo de las directivas y de todos los colaboradores.
También el SGSI es muy beneficioso para la Organización en cuanto a las mejoras continuas de los procesos para realizar las auditorías internas y lo importante de incrementar la confianza y mejora de su imagen frente a sus clientes.

BIBLIOGRAFÍA

AGUIRRE CARDONA. Juan David y BETANCOURT ARISTIZABAL, Catalina. “Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda”Internet:(http://repositorio.utp.edu.co/dspace/bitstream/11059/4117/1/0058A284.pdf.)

ALVAREZ BASALDUA, Luis Daniel. Seguridad en Informática Auditoría de SistemasInternet:(http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf.)

_____.”Concepto de virus informático”Internet:(http://spi1.nisu.org/recop/al01/salva/definic.html)

_____.”Fundamentos de Seguridad Informática” Internet: (http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Estandares.php)

GUERRON ERAS, Jorge Catulo. “Elaboración de un plan para la implementación del sistema de seguridad de la información” Internet: (http://openaccess.uoc.edu/webapps/o2/bitstream/10609/19067/24/jguerronTFM0113memoria.pdf)

GUZMÁN GARCÍA, Alexander y TABORDA BEDOYA, Carlos Alberto. “Diseño de un sistema de gestión de la seguridad informática – SGSI–, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C., a través de la auditoría” Internet: (http://hdl.handle.net/10596/3448)

_____.”Implementación de un SGSI etapa 3” Internet: (http://www.pmg-ssi.com/2014/02/implementacion-de-un-sgsi-etapa-3-ejecucion/)

_____.”Lección 1: Conceptos de Vulnerabilidad, Riesgo y Amenaza” Internet: (http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html)

_____.”Lección 23: Provisión de recursos” Internet: (http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/53_leccin_23_provisin_de_recursos.html)]

_____.”Ley 1273 DE 2009” Internet:(http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492)

_____.”Recursos requeridos para el desarrollo del proyecto” Internet: (http://www.virtual.unal.edu.co/cursos/agronomia/2007841/lecciones/03_07.htm)

_____."¿Sabes diferenciar la ISO 27001 y la ISO 27002?" Internet: (http://www.redseguridad.com/opinion/articulos/sabes-diferenciar-la-iso-27001-y-la-iso-27002)

_____."Seguridad Informática" Internet: (http://carrmen.jimdo.com/riesgo-informatico/)

_____."Sistema de Gestión de la Seguridad de la Información" Internet: (http://www.iso27000.es/download/doc_sgsi_all.pdf)

_____."Sistema de Gestión de Seguridad de la Información ISO 27001" Internet: (http://www.dnvba.com/es/Certificacion/Sistemas-de-Gestion/Seguridad-de-la-Informacion/Pages/Sistema-de-Gestion-de-Seguridad-de-la-Informacion-ISO-27001.aspx)

_____."Tema 1- Seguridad Informática"Internet: (http://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA)

ANEXOS

ANEXO A

Cuestionario sobre Seguridad Informática

Seguridad General

1. ¿Los computadores de su empresa tienen instalado un antivirus?
   __Si
   __No
   __NS/NR
2. ¿El antivirus instalado, está actualizado con las últimas definiciones?
   __Si
   __No
   __NS/NR
   3. ¿Se realiza mantenimiento periódico a los computadores de la empresa?
   __Si
   __No
   __NS/NR
4. ¿Cuántos computadores tiene su empresa?
   __1 - 5
   __5 - 10
   __+ 10
5. La empresa tiene conexión WIFI, ¿Cuenta con las medidas de seguridad pertinentes para proteger esta conexión?
   __Si
   __No
   __NS/NR
6. ¿Se tiene definida una política para la realización de copias de seguridad de los datos?
   __Si
   __No
   __NS/NR
7. ¿Se realizan copias de seguridad de los datos de la empresa?
   __Si
   __No
   __NS/NR
8. ¿Con qué frecuencia se realizan las copias de seguridad en la empresa?
   __Diaria
   __Semanal
   __Mensual
9. ¿El personal de su empresa ha sido informado sobre la LEY 1273 DE 2009?
   __Si
   __No
   __NS/NR
10. ¿Los programas que se utilizan en su empresa, que almacenan datos, cumplen con las características de seguridad de su empresa?
    __Si
    __No
    __NS/NR

Cuestionario sobre Seguridad Informática

Seguridad General

1. ¿Los computadores de su empresa tienen instalado un antivirus?
   X Si
   __No
   __NS/NR
2. ¿El antivirus instalado, está actualizado con las últimas definiciones?
   __Si
   __No
   X NS/NR
3. ¿Se realiza mantenimiento periódico a los computadores de la empresa?
   __Si
   __No
   X NS/NR
4. ¿Cuántos computadores tiene su empresa?
   __1 - 5
   __5 - 10
   X + 10
5. La empresa tiene conexión WIFI, ¿Cuenta con las medidas de seguridad pertinentes para proteger esta conexión?
   X Si
   __No
   __NS/NR
6. ¿Se tiene definida una política para la realización de copias de seguridad de los datos?
   X Si
   __No
   __NS/NR
7. ¿Se realizan copias de seguridad de los datos de la empresa?
   X Si
   __No
   __NS/NR
8. ¿Con qué frecuencia se realizan las copias de seguridad en la empresa?
   X Diaria
   __Semanal
   __Mensual
9. ¿El personal de su empresa ha sido informado sobre la LEY 1273 DE 2009?
   __Si
   X No
   __NS/NR
10. ¿Los programas que se utilizan en su empresa, que almacenan datos, cumplen con las características de seguridad de su empresa?
    __Si
    __No
    X NS/NR

ANEXO B

RESUMEN ANÁLITICO RAE.

Título de Documento.	Diseño De Un Sistema De Gestión De Seguridad Informática Para La Empresa GED (Gestión Estrategia Y Desarrollo) De La Ciudad De Bogotá
Autor	MENDOZA PENAGOS Lina Patricia
Palabras Claves	Activo, SGSI, riesgo, ISO27001:2013, Magerit, Amenazas.
Descripción El proyecto es desarrollado en GED donde se aplicara el SGSI basado en la norma ISO 27001, efectuando diferentes procesos entre las cuales se encuentran políticas para controlar y garantizar la seguridad de los activos.	
Fuentes Bibliográficas	AGUIRRE CARDONA. Juan David y BETANCOURT ARISTIZABAL, Catalina. "Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda"Internet:(http://repositorio.utp.edu.co/dspace/bitstream/11059/4117/1/0058A284.pdf.) ALVAREZ BASALDUA, Luis Daniel. Seguridad en Informática Auditoría de Sistemas Internet:http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf.) _____."Concepto de virus informático" Internet: (http://spi1.nisu.org/recop/al01/salva/definic.html) _____."Fundamentos de Seguridad Informática" Internet: (http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Estandares.php) GUERRON ERAS, Jorge Catulo. "Elaboración de un plan para la implementación del sistema de seguridad

	de la información" Internet: (http://openaccess.uoc.edu/webapps/o2/bitstream/10609/19067/24/jguerronTFM0113memoria.pdf)

Contenido: El objetivo general del proyecto:
Diseñar un Sistema de Gestión de Seguridad de la Información que ayuda a reducir las amenazas de seguridad en que se encuentra la empresa GED en la ciudad de Bogotá.

Objetivos Específicos

Identificar los activos informáticos mediante la aplicación de instrumentos de recolección de información para establecer los dominios del estándar ISO 27001 en GED.

Determinar las vulnerabilidades amenazas y riesgos de seguridad a los que pueda estar expuesta la información aplicando la metodología MAGERIT.

Revisar y verificar la existencia de controles de acuerdo a la norma ISO 27002 que ayude a definir la existencia de políticas y procedimientos de seguridad en GED.

Diseñar un sistema de gestión de seguridad de la información y sus respectivas normas de acuerdo a los resultados de la evaluación realizada.

Metodología Se utilizó metodología MAGERIT, Análisis y gestión de riesgos.

El presente proyecto cumplio con los objetivos propuestos para el Diseño de un sistema de gestion de seguridad de la información en GED, se realizó la identificación de los activos de información mediante entrevistas, cuestionarios y listas de chequeo, se determinó las vulnerabilidades, amenazas y riesgos donde se identificaron los activos críticos y que requieren de atención y de controles y políticas de seguridad.

Se reviso y verifico la existencia de controles para definir cuales son los adecuados para fortalecer y asegurar la información que es parte del desarrollo de las labores de la organización.
GED es una organización que tiene contratos con diferentes empresas de la ciudad y debe establecer políticas que protejan y garanticen la seguridad de la información de cualquier tipo de amenazas.

El diseño del sistema de gestión de la seguridad de la información permite el desarrollo de gestión de cada proceso de la empresa por medio de estándares, técnicas y metodologías como la ISO 27001-27002 para lograr mitigar los

riesgos que puedan presentar, además de reducir el riesgo, aumentar la confiabilidad, integridad y disponibilidad de la información lo cual se logra con el apoyo de las directivas y de todos los colaboradores.
También el SGSI es muy beneficioso para la Organización en cuanto a las mejoras continuas de los procesos para realizar las auditorías internas y lo importante de incrementar la confianza y mejora de su imagen frente a sus clientes.

Recomendaciones.

Se debe socializar las vulnerabilidades y el análisis de riesgos de seguridad para la empresa GED para que se pueda ejecutar los controles de acuerdo a la norma ISO 27002 para definir las políticas y procedimientos de seguridad.

Para el diseño del Sistema de Gestión de Seguridad de la Información es necesario capacitara los colaboradores en temas de seguridad informática y a quienes estén involucrados con GED.
Se debe evaluar y aprobar las políticas concebidas dentro de este proyecto.
Los controles de seguridad de acuerdo al resultado del análisis de riesgos deben ser realizados en la mayor brevedad posible.
Los directivos deben tener en cuenta la seguridad informática, e incluir los recursos necesarios para su diseño.
Los colaboradores de la empresa deben recibir capacitación sobre el desarrollo del proyecto para el conocimiento y adaptación a la política de cambio sobre la seguridad informática.
Se deben realizar auditorías a los activos de información para actualizar los controles que permitan la mejora de prácticas que estén relacionadas con la seguridad de la información.