DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA INTRANET DEL POLICLÍNICO DEL SUR OLAYA BOGOTÁ, BAJO LA NORMA ISO 27001.

YEINNY ANDREA BOLIVAR LEON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
BOGOTÁ D.C.
2015

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA INTRANET DEL POLICLÍNICO DEL SUR OLAYA BOGOTÁ, BAJO LA NORMA ISO 27001.

YEINNY ANDREA BOLIVAR LEON

Proyecto de Grado para Optar al título de
Especialista en Seguridad Informática

Asesor:

HENRY FERNANDO RODRÍGUEZ HERNÁNDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
DEPARTAMENTO DE INGENIERÍA ELÉCTRICA
BOGOTÁ D.C.
2015

Nota de Aceptación:

_____

_____

_____

_____

_____

_____
Firma del Presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá D.C. Septiembre 26 de 2015

RESUMEN

El presente documento tuvo como objetivo fundamental, el análisis y gestión de riesgos de la organización, el estudio de la metodología Magerit, y la norma ISO 27001.

La seguridad de la información a nivel cotidiano tiene un papel importante en las organizaciones por esta razón se busca a través de un análisis y gestión de riesgos realizar la identificación llevando a cabo las diferentes acciones que se desarrollan dentro de la metodología Magerit, como lo son el análisis de activos, amenazas, el impacto y riesgo que estos presentan dentro de la Institución, para con estos datos luego llegar a la obtención de la matriz de riesgos con la finalidad de escoger los controles y objetivos más adecuados de la norma ISO 27001.

ABSTRACT

This paper had as main objective, analysis and risk management organization, magerit study methodology, and ISO 27001.

The information security to everyday level has an important role in organizations therefore seeks through analysis and risk management make identification performing different actions developed within the Magerit methodology, as they are analysis of assets, threats, impact and risk they present within the institution, for this data then reach obtain the risk matrix in order to choose the most appropriate controls and objectives of the ISO 27001 standard

DEDICATORIA

A mi madre y mis abuelos, por acompañarme en todo momento, enseñarme a crecer y que ante las caídas uno debe levantarse con la mayor fuerza posible para continuar, por apoyarme y guiarme, por ser las bases para llegar a esta etapa de la vida.

El presente trabajo es dedicado a mi hijo el cual ha sido la parte fundamental para llevar a cabo esta meta y alcanzar este sueño.

AGRADECIMIENTOS

Quiero agradecer a todas y cada una de las personas que me enseñaron y colaboraron a la hora de realizar los diferentes análisis y recolección de la información, a mi madre porque ella estuvo en los días más difíciles de mi vida como estudiante, además por que las metas planteadas en este momento darán reconocimiento y frutos a lo largo de la vida.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE GRÁFICAS

INTRODUCCIÓN

En este proyecto se pretende demostrar que la seguridad de la información sirve como un mecanismo para dar organización a la red además de adecuar y garantizar los riesgos de la seguridad, además obtener conocimiento del manejo, funcionamiento y aplicación de las diferentes normas y estándares que son utilizados en la seguridad informática, deduciendo de esta manera cual es la norma más conveniente en la implementación del sistema de gestión de seguridad de la información en la intranet.

En este trabajo se pretende demostrar e implementar de un Sistema de Gestión de Seguridad de la Información para la Intranet del policlínico del sur Olaya Bogotá, para llevar a cabo una gestión de la red de manera organizada, adecuada y garantizando que los diferentes riesgos de seguridad de la red puedan ser disminuidos a través de la utilización de los diferentes procedimientos y tratamiento de los mimos. La información que se está tomando para la realización de este proyecto son las diferentes guías que se encuentran para colocar en práctica la Norma ISO 27001, se realizó un análisis preventivo y correctivo con el fin de llevar una mejora en la administración y gestión de la Intranet conforme a la Norma ISO 27001 identificando las vulnerabilidades presentes en la organización.

1. PLANTEAMIENTO DEL PROBLEMA

La seguridad informática es la protección que se debe dar a la información para que esta no sea tratada de forma indebida, como el ser revelada, modificada, o destruida de manera accidental o intencional, a través de las normas o medidas que son necesarias para dar la protección adecuada para que no exista el acceso no autorizado, la interferencia accidental o intencionada con operaciones normales.[1]

La intranet es una red interna de tipo área local o LAN que tiene como principal característica el uso exclusivo para la organización o empresa, esta hace uso de los protocolos HTML y TCP/IP que nos permite la interacción de la intranet con la internet, la cual tiene consigo, distintos niveles de seguridad, según el usuario. Estos niveles de seguridad, son asignados, según la relevancia del puesto dentro de la organización, del usuario. [2]

¿Puede la implementación de un SGSI en la intranet del policlínico del sur de Olaya Bogotá mejorar la seguridad del mismo?

1.1 DESCRIPCIÓN DEL PROBLEMA.

Obtener conocimiento del manejo, funcionamiento y aplicación de las diferentes normas y estándares que son utilizados en la seguridad informática, deduciendo de esta manera cual es la norma más conveniente en la implementación del sistema de gestión de seguridad de la información en la intranet del policlínico del sur Olaya Bogotá.

1.2 FORMULACIÓN DEL PROBLEMA

En la información existen cierto manejo, funcionamiento por lo cual se hace necesaria la aplicación de las diferentes normas y estándares que sean creado a lo largo de la seguridad de la información con el fin de dar lo más conveniente en la implementación del sistema de gestión de seguridad de la información en la intranet del policlínico del sur Olaya Bogotá.

1 http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf

2 http://www.misrespuestas.com/que-es-intranet.html

1.3 SUB PREGUNTAS.

- ¿Las políticas de seguridad son necesarias para establecer los procedimientos para la protección contra robo, daño o acceso no autorizado?

- ¿Es importante limitar la asignación de privilegios?

- ¿Los privilegios tienen que revisarse de forma periódica para evitar la existencia de privilegios que ya no son necesarios?

2. JUSTIFICACIÓN DEL PROYECTO

La seguridad informática adopta las diferentes herramientas, normas, estándares y procedimientos que se necesitan a la hora de llevar a cabo la implementación de un sistema de gestión de la información tanto a nivel teórico como práctico.

Con la aplicación de las metodologías se busca desarrollar la propuesta de, implementación, operación, monitorización, revisión, mantenimiento y mejora del sistema de gestión de seguridad de la información.

Realizar los análisis respectivos de la situación actual que presenta el policlínico de sur, identificar los activos, identificar las vulnerabilidades, valorar impacto, la probabilidad de ocurrencia, identificar y valorar los riesgos, para luego generar la matriz de gestión de riesgos y seleccionar los objetivos de control de acuerdo con la Norma ISO 27001. Todo esto con el fin de proponer la implementación del sistema de seguridad informática y obtener el manual de procedimientos necesarios para esta.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de la Seguridad de la Información SGSI, para la intranet del Policlínico del sur Olaya.

3.2 OBJETIVOS ESPECÍFICOS

- Revisar, analizar, evaluar la intranet para determinar los riesgos que se presentan con la información, basados en los resultados de la auditoría interna.

- Establecer las tareas a especificar para lograr el mejoramiento continuo del SGSI.

4. MARCO DEL PROYECTO

4.1 MARCO REFERENCIAL

La norma ISO 27000 fue generada por la Organización Internacional de Estandarización que es la encargada de las normas o estándares que regulan los productos y servicios que son ofrecidos a nivel de fabricación, comercio y comunicación, en todas las ramas industriales, en la actualidad se encuentra conformada por 157 instituciones de países los cuales se integran a través de una red que tiene su punto principal en la ciudad de Ginebra en Suiza, sus normas surgen del consenso de entre sus representantes.

Entre los activos más valiosos que tenemos en nuestra realidad cotidiana tanto al nivel de las empresas como todo tipo de persona o sociedad es la información la cual se puede ver afectada y amenazada en nivel de su confiabilidad y la manera en que se debe llevar a cabo su seguridad para el almacenamiento de esta misma, ya que es de carácter vital para el desarrollo de las diferentes actividades de la compañía que se encuentran en los diferentes mercados, por lo cual se hace necesario brindar el aseguramiento tanto a la información como a los diferentes sistemas que la procesan.

Para implementar un SGSI (Sistema de Gestión de la Seguridad de la Información) en la intranet del policlínico del sur Olaya, se busca disminuir el número de amenazas que se llegan a presentar con la ayuda de las diferentes vulnerabilidades existentes en la intranet pueden contribuir con las diversas formas de fraude, sabotaje o vandalismo, las acciones de establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información, se llevaran a cabo a través de un análisis de la situación que presenta el policlínico de sur, identificar los activos más importantes, observar, valorar los riesgos, para luego generar la matriz de gestión de riesgos y seleccionar los objetivos de control de acuerdo con la Norma ISO 27001.

4.2. MARCO CONTEXTUAL

4.2.1 Ubicación física

El centro policlínico del Sur es una Institución Hospitalaria de segundo nivel de atención con el objetivo de atender las necesidades de salud de los usuarios más vulnerables y de escasos recursos ubicados en el sur de Bogotá, tiene la convicción de prestación de servicios socialmente responsables, enmarcados en principios de calidad, servicio.

Actualmente, la Organización ofrece dentro de sus principales servicios: Urgencias de adultos, pediátricas, ginecológicas y obstétricas, servicios ambulatorios, consulta externa especializada, apoyo diagnóstico y terapéutico, ginecología-obstetricia, entre otros, se encuentra ubicado en la Carrera 25, No.20 -68 Sur, sus instalaciones se encuentran conformadas por 2 edificaciones cada uno de tres pisos, en la torre 2 se encuentran las oficinas administrativas.

4.2.2 Estructura de la Red LAN:

La red LAN del policlínico del sur cuenta con 4 servidores, 34 estaciones que se encuentran distribuidas en los consultorios del primer piso y en las oficinas distribuidas por departamentos, las demás estaciones se encuentran en planta baja. A continuación se detallan los cuatro servidores con los que cuenta:

a. Internet Access Server (IAS): Este software es un componente de servidor de Windows para proporcionar al usuario centralizado de autenticación, autorización y contabilidad a los usuarios tanto internos como externos.

b. Base de Datos: Utiliza como base de datos el software Oracle Data Base levantado sobre el sistema operativo Windows.

c. Internet y Correo Electrónico: Utiliza los beneficios del sistema operativo Windows, a través de internet explore y Microsoft Office Outlook.

d. Dominio: Para el servicio de Dominio se utiliza el Active Directory, del sistema operativo Windows 2008 Server.

Cuentan con cableado estructurado, lo que facilita la administración física de la red, propia de energía eléctrica para los equipos, debidamente separada del cableado de datos.

4.2.3 Estructura de la Red WAN:

La Clínica cuenta con dos enlaces a Internet:

Enlace al servicio de la línea del suscriptor Digital SDSL (sincrónico), la cual trata de una línea simétrica permanente con velocidades justamente de hasta 2.048 Kbps, contratado a la compañía UNE y que es utilizado para acceso de los prestadores de salud a las aplicaciones de planillas.

Enlace ADSL (asincrónico) servicio que es prestado por la empresa de teléfonos de Bogotá ETB de y que es utilizado para acceso a la Internet, posee dos módems en calidad de préstamo por parte de la ETB.

4.3. MARCO CONCEPTUAL

4.3.1 Seguridad informática

Define la seguridad informática como la encargada de garantizar los tres principios básicos en el manejo de la información como lo son la confidencialidad, integridad y disponibilidad utilizando para ello un conjunto de normas, métodos, herramientas y personal humano calificado para actuar ante cualquier tipo de amenaza. [3]

4.3.2 Principios de la seguridad de la información

• Integridad: la información debe ser protegida de modificaciones no autorizadas.

• Disponibilidad: la información y servicios deben estar disponibles siempre que se necesiten.

• Confidencialidad: se debe garantizar que la información es conocida únicamente por a quien le interese. [4]

3 http://g3ekarmy.com/%C2%BFque-es-la-seguridad-informatica/

4 http://auditoriadesistemas.galeon.com/productos2227783.html

4.3.3 Definición de Políticas de Seguridad Informática

Las políticas de seguridad informática son utilizadas como un medio de comunicación con cada uno de los usuarios a través del cual se da a conocer el medio de actuación que debe llevar a cabo una persona frente a los recursos y servicios de tipo informático que maneja dentro de la organización.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos. [5]

4.3.4 Normas ISO 27000

La norma ISO 27001 define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

La ISO 27001 es para la seguridad de la información lo mismo que la ISO 9001 es para la calidad: es una norma redactada por los mejores especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización. También permite que una organización sea certificada, lo cual significa que una entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible.

A raíz de la importancia de la norma ISO 27001, muchas legislaturas han tomado esta norma como base para confeccionar las diferentes normativas en el campo de la protección de datos personales, protección de información confidencial,

5 http://www.monografias.com/trabajos12/fichagr/fichagr.shtml#POLIT

protección de sistemas de información, gestión de riesgos operativos en instituciones financieras, etc.[6]

4.3.5 Documentación de la norma ISO 27001.

- El alcance del SGSI
- La política del SGSI
- Procedimientos para control de documentación, auditorías internas y procedimientos para medidas correctivas y preventivas
- Todos los demás documentos, según los controles aplicables
- Metodología de evaluación de riesgos
- Informe de evaluación de riesgos
- Declaración de aplicabilidad
- Plan de tratamiento del riesgo
- Registros.

4.3.6 Cuatro Grandes Actividades:

- Establecer el sistema.
- Implementar y operar el sistema.
- Mantener y mejorar el sistema.
- Monitorear y revisar el sistema.

4.3.7 Pasos Básicos Para Lograr La Mejora.

- Plan (planear o planificar).- En este primer paso se identifica aquello que se quiere mejorar, se recopilan los datos iníciales, se establecen los objetivos esperados y se planifican las actividades a realizar.

- Do (hacer o ejecutar).- Lo siguiente es ejecutar las actividades del plan hecho en el primer paso y documentar los resultados.

- Check (verificar).- Se comparan los resultados obtenidos versus los resultados esperados, que se definieron en el “Plan”.

- Act (actuar).- El ciclo “termina” haciendo los ajustes necesarios para que se logren, en la medida de lo posible, los objetivos planeados; se revisan las lecciones aprendidas y se reinicia el ciclo completo.[7]

6 http://www.iso27001standard.com/es/que-es-la-norma-iso-27001.

4.3.8 Análisis de Riesgos.

Análisis de riesgos de seguridad de la cadena de suministro internacional: El proceso de identificar amenazas, vulnerabilidades y debilidades de seguridad en la cadena de suministro internacional y la gestión de acciones correctivas con procedimientos de verificación para asegurar que las debilidades sean corregidas.[8]

4.3.9 Amenazas:

Una 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, en el caso de la Seguridad Informática, los Elementos de Información. Debido a que la Seguridad Informática tiene como propósitos de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.[9]

Gráfica 1. Amenazas sobre los elementos de un sistema

Fuente: Amenazas y Vulnerabilidades

4.3.10 Vulnerabilidades

La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a

---

7 http://www.magazcitum.com.mx/?p=1574

8 C-TPAT Análisis de Riesgos en 5 Pasos Guía de procedimientos. (n.d.). http://www.dian.gov.co/descargas/operador/documentos/2015/Analisis_de_Riesgo_En_5_Pasos.pdf

9 Gestión de Riesgo en la Seguridad Informática recuperado de la página web: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.[10] En la Gráfica 2 se presentan las vulnerabilidades sobre los elementos de sistema.

Gráfica 2 Vulnerabilidades sobre los elementos de un sistema

Fuente: Amenazas y Vulnerabilidades

4.3.11 Identificación de Activos

Para que el análisis de riesgos tenga un efecto positivo y real, es necesario identificar los elementos más relevantes.

Se entiende relevancia los puntos claves a considerar durante la realización del análisis de riesgos.

Dicha relevancia será de gran importancia para identificar el rumbo de las acciones del plan de Riesgos.

Este paso consiste en identificar y valorar la relevancia de los activos determinantes para el proyecto.

Los activos se evalúan sobre una escala de valor crítico donde se define que tan importantes son para cumplir con los objetivos del proyecto.
La relevancia de los activos marcara el rumbo definitivo de las acciones a seguir en el análisis del riesgo.

10 Gestión de Riesgo en la Seguridad Informática recuperado de la página web: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

Cuanta mayor relevancia tenga un activo mayor es la importancia crítica, mayor será el riesgo al que está expuesto el proyecto en caso de ocurrir un incidente que materialice una amenaza.

Para alcanzar el objetivo de identificar la relevancia de los activos, el análisis de riesgos debe proveer los datos cuantitativos y cualitativos que permiten su evaluación.[11]

4.3.12 Valoración de Activos

Una vez identificados los activos que están relacionados con el proyecto de software es necesario valor el nivel de importancia que tienen estos en el desarrollo del mismo, para ello se debe definir las dimensiones o criterios bajo los cuales se van a evaluar, como por ejemplo:

- Autenticidad: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa? Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar).

- Confidencialidad: ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.

- Integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.

- Disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.

- Trazabilidad del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿Quién hace qué y cuándo?

Nivel de importancia para el cumplimiento de los objetivos del proyecto La valoración del activo puede ser cualitativa, cuantitativa o ambas[12]

11 Caracterización, F. De. (n.d.). Índice de contenido, 1– recuperado de la página web: .http://www.udistrital.edu.co:8080/documents/276352/356568/Cap5GestionRiesgo.pdf

12 Caracterización, F. De. (n.d.). Índice de contenido, 1– recuperado de la página web: .http://www.udistrital.edu.co:8080/documents/276352/356568/Cap5GestionRiesgo.pdf

4.3.13 Identificación de Riesgos

En la identificación de riesgos se debe determinar la posibilidad de ocurrencia de riesgos potenciales, lo cual pueda entorpecer el normal desarrollo de las funciones de la Organización.

Para esto podemos elaborar un listado de los riesgos inherentes a las actividades o procedimientos que se llevan a cabo en cada proceso, priorizándolos según el grado en que estos afecten los objetivos misionales del mismo.

4.3.14 Análisis de factores de riesgo.

En el análisis de factores de riesgo es necesario tener en cuenta aquellos que pueden incrementar la probabilidad de que un riesgo ocurra. Inclusive, es posible generar riesgos nuevos como por ejemplo la integridad, la ética de las personas involucradas, el tamaño y la complejidad de las transacciones involucradas en el proceso, así como, los cambios en los sistemas o en el personal clave; adicionalmente se debe tener en cuenta los factores de carácter externo que pudieran llegar a afectar la Organización como son los económicos, sociales, legales o de cambio tecnológico.

4.3.15 Clasificación del riesgo

La clasificación del riesgo permite realizar una mejor identificación de los riesgos inherentes a los procesos de la Organización, ya que delimita los parámetros a seguir por el responsable. Esta sería una posible clasificación:

- Riesgo estratégico
- Riesgo operativo
- Riesgo de control
- Riesgo financiero
- Riesgo de tecnología
- Riesgo de incumplimiento
- Riesgo de fraude
- Riesgo de ambiente laboral13

13 http://seguridadinformacioncolombia.blogspot.com/2010/05/gestion-de-riesgos.html

- 4.3.16 Una auditoría interna

Es el proceso mediante el cual la organización evalúa el cumplimiento de la implantación del Sistema de Gestión de la Seguridad de la información en una empresa bajo una normativa. Para el caso de estudio, pues la normativa es la ISO/IEC 27001. El numeral 6 de esta normativa anuncia los aspectos y parámetros a considerar para la realización de las auditorías internas. En el número 15.3 de la normativa ISO/IEC 27002, se presentan las consideraciones de la auditoría de los sistemas de información que es necesario auditar para verificación de las medidas implementadas en los sistemas de información que la empresa posee y que están incluidos dentro del alcance del SGSI. [14]

2.4. MARCO CONCEPTUAL

4.4.1 La norma ISO/IEC 27001

Es uno de los estándares que se han establecido internacionalmente con el fin de especificar los diferentes requerimientos necesarios para formar, realizar, manejar, controlar y ayudar a mejorar un Sistema de Gestión de Seguridad de la información (SGSI). Con el fin de obtener los requerimientos necesarios para la implementación de controles a nivel de seguridad necesarios en la implementación en una organización, un sector de la misma, o un proceso, según el alcance del SGSI.

Esta nos da a conocer en sus diferentes la documentación que es requerida para una certificación de cumplimiento de todos los requisitos.

Los procesos que se pueden definir en cada paso del ciclo PHVA son los siguientes:

Planificar

- Establecer el contexto. Alcance y Limites
- Definir Política del SGSI
- Definir Enfoque de Evaluación de Riesgos
- Identificación de riesgos
- Análisis y Evaluación de riesgos
- Evaluar alternativas para el Plan de tratamiento de riesgos
- Aceptación de riesgos
- Declaración de Aplicabilidad

[14] Universidad Nacional Abierta y a distancia UNAD. Guía de implementación del SGSI recuperada de la página web: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/61_leccin_26_auditoras_internas_del_sgsi.html

Hacer

- Implementar plan de tratamiento de riesgos
- Implementar los controles seleccionados
- Definir las métricas
- Implementar programas de formación y sensibilización
- Gestionar la operación del SGSI
- Gestionar recursos
- Implementar procedimientos y controles para la gestión de incidentes de seguridad

Comprobar

- Ejecutar procedimientos de seguimiento y revisión de controles.
- Realizar revisiones regulares de cumplimiento y eficacia de los controles del SGSI.
- Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad.
- Revisión de la evaluación de riesgos periódicamente.
- Realizar auditorías internas.
- Revisión de alcance y líneas de mejoras del SGSI por la Dirección.
- Actualizar los planes de seguridad.
- Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI

Mejorar

- Implementar las mejoras identificadas para el SGSI
- Implementar las acciones correctivas y preventivas pertinentes.
- Comunicar acciones y mejoras a todas las partes involucradas.
- Asegurarse que las mejoras logren los objetivos previstos.

En la nueva versión de ISO/IEC 27001:2013 se adapta con una serie de lineamientos que sirven para el desarrollo de un sistema de gestión de la seguridad de la información, que sin importar el tipo de empresa, se pueda alinear con otros sistemas de gestión en la empresa. Esta nueva estructura propuesta, alineada con el ciclo de la Mejora Continua.

4.4.2 Deberes a cumplir respecto a la información

Legalmente que infracciones se realizan en el caso según la ley colombiana, Están trabajados como delitos informáticos generalidades y adecuación típica en el código penal colombiano, para poder comprender de mejor manera según la ley colombiana como se manejan las infracciones lo primero que debemos hacer es entender la definición de delito informático el cual comprende las conductas que incurren sobre las herramientas informáticas utilizadas como los programas, los

ordenadores, y los diferentes medios que son usados para causar lesiones a otros intereses jurídicamente tutelados como son la intimidad, el patrimonio económico y la fe pública, entre los cuales podemos encontrar Virus, Gusanos o Bombas lógicas o cronológica, el Sabotaje informático, los Piratas informáticos o hackers Acceso no autorizado a sistemas o servicios Reproducción no autorizada de programas informáticos de protección legal Manipulación de datos de entrada y/o salida Manipulación de programas Fraude efectuado por manipulación informática.

El gobierno colombiano a través de la Ley 1273 de 2009 dio origen a nuevos tipos penales relacionados con los delitos informáticos y la protección a la información y los datos con penas de prisión hasta 120 meses y multas hasta 1500 salarios mínimos legales mensuales vigentes.

Para el caso de análisis que nos concierne el artículo de esta ley que podemos aplicar es el Artículo 269ª el cual tiene como enunciado el ACCESO ABUSIVO A UN SISTEMA INFORMATICO: “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, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes..(…)”.

Otro artículo que podemos aplicar es el Artículo 269C que enuncia INTERCEPTACION DE DATOS INFORMATICOS. “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 incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses... (…)”.

El Artículo 269F VIOLACION DE DATOS PERSONALES “El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales , datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes...(…)”.

El articulo 269 H Circunstancias de agravación punitiva: “Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

5. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

6. Obteniendo provecho para sí o para un tercero.

7. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

8. Utilizando como instrumento a un tercero de buena fe.

9. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.”

5. DISEÑO METODOLÓGICO

La metodología Magerit para el análisis y gestión de riesgos fue elaborada por el Consejo Superior de Administración Electrónica, está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los usuarios; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza, es de interés para las personas que trabajan con información digital y sistemas informáticos para tratarla, permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos.

Con la metodología para análisis y gestión de riesgos Magerit se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Esta norma ayuda a implementar un sistema de gestión y análisis de Riesgos de los sistemas de información de forma organizada y está estructurada en procesos bien definidos.

Con la ayuda de esta herramienta es posible realizar las siguientes actividades

- Identificación de activos
- Determinación de amenazas
- Estimación de impactos
- Determinación del riesgo
- Determinación de las medidas de seguridad necesarias.

5.1 IDENTIFICACIÓN Y DETERMINACIÓN ANALISIS Y GESTION DE RIESGOS

5.1.1 Identificación y Valoración de Activos

Se realiza la clasificación de los activos dentro de una jerarquía, determinando para cada uno un código que refleja su posición jerárquica, un nombre y una breve descripción de las características que recoge el epígrafe, la clasificación de activos se realizó con base al "Libró II- Catálogo de elementos".

En la tabla 1 se encuentran los tipos de activos que se definen en la metodología de Magerit para su clasificación los cuales son definidos en el catálogo de elementos 2012_Magerit_v3_libro2_catálogo de elementos_es_NIPO_630-12-171-8.

Tabla 1 TIPOS DE ACTIVOS

TIPOS DE ACTIVOS	DESCRIPCION DEL TIPO
(S) servicios	Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema.
(K) Claves criptográficas	La criptografía se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos
(D) Datos/ información	Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.
(SW) aplicaciones	Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios
(HW) equipos informáticos /hardware	Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. Depositarios temporales o permanentes de los datos,
(COM) Redes de comunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.
(SI) Soportes de información	En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.
(AUX) Equipamiento auxiliar	En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
(L) Instalaciones	En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.
(P) Personal	En este epígrafe aparecen las personas relacionadas con los sistemas de información.

Los datos que se observan en la tabla 2 de Dimensiones de Activos son las características o atributos que permiten darle un valor al activo es decir son un aspecto y son utilizados para valorar las consecuencias que pueden suceder al generarse la materialización de una amenaza.

Tabla 2 DIMENSIONES ACTIVOS

DIMENSIONES
(D) DISPONIBILIDAD
(I) INTEGRIDAD
(C) CONFIDENCIALIDAD
(A)AUTENTICIDAD DE LOS USUARIOS Y DE LA INFORMACION
(T) TRAZABILIDAD DEL SERVICIO Y DE LOS DATOS

En la tabla 3 se encuentra la escala de valores que se va a utilizar con las dimensiones plasmadas anteriormente, con la finalidad de obtener la valoración de activos.

Tabla 3 PARAMETROS

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

En la tabla 4 valoración de activos nos permiten visualizar el activo y la escala de valor que lo representa dentro de cada una de las dimensiones propuestas en la tabla N° 2 las cuales son utilizadas de acuerdo a la metodología planteada para el desarrollo de Análisis de Riesgos.

Tabla 4 VALORACION DE ACTIVOS

TIPO DE ACTIVO	ACTIVO	DIMENSIONES				
		D	I	C	A	T
CAPA DE NEGOCIO						
(D) Datos/ informacion	Código fuente	10	9	9		
(D) Datos/ informacion	Documentación del proyecto	10	9	9		
SERVICIOS INTERNOS						
(S) servicios	Servidor WSUS	7	7			
(S) servicios	Servidor DNS	7				
(S) servicios	Servicio Directorio	7				
(S) servicios	Servidor de correo electrónico	4				
EQUIPAMENTO						
APLICACIONES						
(SW) aplicaciones	Servidor web	10	8	8		
(SW) aplicaciones	Software firewall		8	8		
(SW) aplicaciones	Sistema de informacion de proyectos	8	8	8	8	7
(SW) aplicaciones	Software de sistema Operativo	8	9	9	8	8
EQUIPOS						
(HW) equipos informáticos /hardware	Servidores de Base de datos	9				
(HW) equipos informáticos /hardware	Firewall externo	8				
(HW) equipos informáticos /hardware	Firewall Interno	8				
(HW) equipos informáticos /hardware	Router	8				
COMUNICACIONES						
(COM) Redes de comunicaciones	Red telefonica basica o RSDI	9				
(COM) Redes de comunicaciones	Red Wan	8				
(COM) Redes de comunicaciones	Red Lan	9				
ELEMENTOS AUXILIARES						
(AUX) Equipamento auxiliar	UPS	7				
(AUX) Equipamento auxiliar	Planta Electrica	7				
(AUX) Equipamento auxiliar	Cableado	8				
(AUX) Equipamento auxiliar	Muebles	3				
SERVICIOS SUBCONTRATADOS						
(S) servicios	Internet 9					
INSTALACIONES						
(L) Instalaciones	EDIFICIO	7				
PERSONAL						
(P) Personal	Usuarios externos				8	8
(P) Personal	Usuarios Internos				8	8
(P) Personal	Administrar de Seguridad	8			8	8

5.1.2 Identificación y Valoración de Amenazas

De acuerdo a la metodología de Magerit las amenazas se pueden clasificar en 4 tipos.

[N] Desastres Naturales.
[I] De origen industrial.
[E] Errores y fallos no intencionados.
[A] Ataque intencionados.

Se busca identificar las diferentes amenazas a las que pueden estar expuestos los activos y las consecuencias que se derivan y la probabilidad que ocurran.

Para la determinación las posibles amenazas presentes en los activos se utilizaran los siguientes valores métricos:

Esta tabla 5 se observa la escala de valores que se van a tener en cuenta durante la valoración de las amenazas.

Tabla 5 VALORACION 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

La tabla 6 establece las posibles amenazas que se pueden presentar alrededor de un activo la frecuencia de su suceso que valoración tomaría en cada una de las dimensiones planteadas para caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación).

Tabla 6 IDENTIFICACION Y VALORACION DE AMENAZAS

TIPO DE ACTIVO	ACTIVO		FREC	DIMENSIONES				
				D	I	C	A	T
CAPA DE NEGOCIO								
(D) Datos/ informacion	Código fuente			50	100	100		
		(E.1) Errores de los usuarios	10	10	10	10		
		(E.2) Errores del administrador del sistema / de la seguridad	1	20	20	20		
		(E.15) Alteración de la información	1		1			
		(E.18) Destrucción de información	1	1				
		(E.19) Fugas de información	1			10		
		(A.5)Suplantacion de la identidad del usuario	10		10	50		
		(A.6) Abuso de Privilegios de Acceso	10		10	50		
		(A.11) Acceso no autorizado	100		10	50		
		(A.15) Modificación deliberada de la información	10		100			
		(E.18) Destrucción de información	10	50				
		(A.19) Divulgación de la información	10			100		
(D) Datos/ informacion	Documentación del proyecto			50	100	100		
		(E.1) Errores de los usuarios	10	10	10	10		
		(E.2) Errores del administrador del sistema / de la seguridad	1	20	20	20		
		(E.15) Alteración de la información	1		1			
		(E.18) Destrucción de información	1	1				

TIPO DE ACTIVO	ACTIVO		FRE C	DIMENSIONES D	I	C	A	T
		(E.19) Fugas de información	1			10		
		(A.5)Suplantacion de la identidad del usuario	10		10	50		
		(A.6) Abuso de Privilegios de Acceso	10		10	50		
		(A.11) Acceso no autorizado	10		10	50		
		(A.15) Modificación deliberada de la información	10		100			
		(E.18) Destrucción de información	10	50				
		(A.19) Divulgación de la información	10			100		
SERVICIOS INTERNOS								
(S) servicios	Servidor			100	100			
		(E.1) Errores de los usuarios	1	10	10			
		(E.2) Errores del administrador	1	20	20			
		(E.10) Errores de secuencia	1		10			
		(E.15) Alteración accidental de la información	1		1			
		(E.18) Destrucción de información	1	10				
		(E.24) Caída del sistema por agotamiento de recursos	10	50				
		(A.5) Suplantación de identidad del usuario	1		50			
		(A.6) Abuso de Privilegios de Acceso	1		10			
		(A.7) Uso no previsto	1	100	10			
		(A.10) Alteración de secuencia	1		50			
		(A.11) Acceso no autorizado	1		10			
		(A,13) Repudio (Negacion de actuaizaciones)	10		100			
		(A,15) Modificacion de la informacion	10		50			
		(E.18) Destrucción de información	1		50			
		(A.24) Denegación del servicio	10		50			
(S) servicios	Servidor DNS			100				
		(N.1) Fuego	0,1	100				
		(N.2) Daño por agua	0,1	50				
		(N.*) Desastres naturales	0,1	100				
		(I1) Fuego	0,5	100				
		(I.2) Daño por agua	0,5	50				
		(I.*) Desastres Industriales	0,5	100				
		(I.3) Contaminación mecánica	0,1	50				
		(I.4) Contaminacion electormagnetica	1	10				
		(I.5) Avería de orígen físico o lógico	1	50				
		(I.6) Corte del suministro electrico	1	100				
		(I.7) Condiciones inadecuadas de temperatura o humedad	1	100				
		(E.2) Errores del administrador del sistema / de la seguridad	1	20				
		(E.23) Errores de mantenimiento /actualización de equipos (hardware)	1	10				
		(E.24) Caída del sistema por agotamiento de recursos	10	50				
		(E.25) Perdida de equipos	1	100				
		(A.23) Manipulación del hardware	0,5	50				
		(A.24) Denegación del servicio	2	100				
		(A.25) Robo de Equipos	1	100				
		(A.26) Ataque Destructivo	1	100				
(S) servicios	Servicio Directorio			50				
		(E.1) Errores de los usuarios	1	10				
		(E.2) Errores del administrador	1	20				
		(E.18) Destrucción de información	1	10				
		(E.24) Caída del sistema por agotamiento de recursos	10	50				
		(A.18) Destruccion de la informacion	1	50				
		(A.24) Denegación del servicio	10	50				
(S) servicios	Servidor de correo electrónico			100				
		(I.5) Avería de orígen físico o lógico	1	50				
		(E.1) Errores de los usuarios	1	1				
		(E.2) Errores del administrador	1	20				
		(E.8) Difusión de software Dañino	1	10				
		(E.18) Destrucción de información	1	50				
		(E.20) Vulnerabilidades de los programas (software)	1	1				
		(E.21) Errores de Mantenimiento / actualización de programas (software)	10	1				
		(A.8) Difusión de software Dañino	1	100				
		(A.18) Destruccion de la informacion	1	50				
EQUIPAMENTO								
APLICACIONES								
(SW) aplicaciones	Servidor web			100	100	100		
		(I.5) Avería de orígen físico o lógico	1	50				
		(E.1) Errores de los usuarios	1	1	10	10		
		(E.2) Errores del administrador del sistema / de la seguridad	1	20	20	20		
		(E.8) Difusión de software Dañino	1	10	10	10		
		(E.9) Errores de re-encaminamiento	1			10		
		(E.10) Errores de secuencia	1		10			
		(E.15) Alteración de la información	1		1			
		(E.18) Destrucción de información	1	50				
		(E.19) Fugas de información	1			10		
		(E.20) Vulnerabilidades de los programas (software)	1	1	20	20		
		(E.21) Errores de Mantenimiento / actualización de programas (software)	10	1	1			
		(A.5) Suplantación de identidad del usuario	1		50	50		
		(A.6) Abuso de Privilegios de Acceso	1		10	10		
		(A.7) Uso no previsto	1	100	10	10		
		(A.8) Difusión de software Dañino	1	100	100	100		
		(A.9) Re- encaminamiento de mensajes	1			100		
		(A.10) Alteración de secuencia	1		50			
		(A.11) Acceso no autorizado	1		10	50		
		(A.15) Modificación deliberada de la información	1		50			
		(A.18) Destruccion de la informacion	1	50				
		(A.19) Revelacion de informacion	1			50		
		(A.22) Manipulacion de programas	5		100	100		
(SW) aplicaciones	Software firewall			100	100			
		(E.1) Errores de los usuarios	1		10	10		

TIPO DE ACTIVO	ACTIVO		FRE C	DIMENSIONES D	I	C	A	T
		(E.2) Errores del administrador del sistema / de la seguridad	1		20	20		
		(E.8) Difusión de software Dañino	1		10	10		
		(E.9) Errores de re-encaminamiento	1			10		
		(E.10) Errores de secuencia	1		10			
		(E.15) Alteración de la información	1		1			
		(E.19) Fugas de información	1			10		
		(E.20) Vulnerabilidades de los programas (software)	1		20	20		
		(E.21) Errores de Mantenimiento / actualización de programas (software)	10		1			
		(A.5) Suplantación de identidad del usuario	1		50	50		
		(A.6) Abuso de Privilegios de Acceso	1		10	10		
		(A.7) Uso no previsto	1		10	10		
		(A.8) Difusión de software Dañino	1		100	100		
		(A.9) Re- encaminamiento de mensajes	1			100		
		(A.10) Alteración de secuencia	1		50			
		(A.11) Acceso no autorizado	1		10	50		
		(A.15) Modificación deliberada de la información			50			
		(A.19) Revelacion de informacion	1			50		
		(A.22) Manipulacion de programas	5		100	100		
(SW) aplicaciones	Sistema de informacion de proyectos			100	100	100	100	
		(I.5) Avería de orígen físico o lógico	1	50				
		(E.1) Errores de los usuarios	1	1	10	10		
		(E.2) Errores del administrador del sistema / de la seguridad	1	20	20	20		
		(E.8) Difusión de software Dañino	1	10	10	10		
		(E.9) Errores de re-encaminamiento	1			10		
		(E.10) Errores de secuencia	1		10			
		(E.15) Alteración de la información	1		1			
		(E.18) Destrucción de información	1	50				
		(E.19) Fugas de información	1			10		
		(E.20) Vulnerabilidades de los programas (software)	1	1	20	20		
		(E.21) Errores de Mantenimiento / actualización de programas (software)	10	1	1			
		(A.5) Suplantación de identidad del usuario	1		50	50	100	
		(A.6) Abuso de Privilegios de Acceso	1		10	10		
		(A.7) Uso no previsto	1	100	10	10		
		(A.8) Difusión de software Dañino	1	100	100	100		
		(A.9) Re- encaminamiento de mensajes	1			100		
		(A.10) Alteración de secuencia	1		50			
		(A.11) Acceso no autorizado	1		10	50		
		(A.15) Modificación deliberada de la información	1		50			
		(A.18) Destruccion de la informacion	1	50				
		(A.19) Revelacion de informacion	1			50		
		(A.22) Manipulacion de programas	5		100	100		
(SW) aplicaciones	Software de sistema Operativo			100	100	100	100	
		(I.5) Avería de orígen físico o lógico	1	50				
		(E.1) Errores de los usuarios	1	1	10	10		
		(E.2) Errores del administrador del sistema / de la seguridad	1	20	20	20		
		(E.8) Difusión de software Dañino	1	10	10	10		
		(E.9) Errores de re-encaminamiento	1			10		
		(E.10) Errores de secuencia	1		10			
		(E.15) Alteración de la información	1		1			
		(E.18) Destrucción de información	1	50				
		(E.19) Fugas de información	1			10		
		(E.20) Vulnerabilidades de los programas (software)	1	1	20	20		
		(E.21) Errores de Mantenimiento / actualización de programas (software)	10	1	1			
		(A.5) Suplantación de identidad del usuario	1		50	50	100	
		(A.6) Abuso de Privilegios de Acceso	1		10	10		
		(A.7) Uso no previsto	1	100	10	10		
		(A.8) Difusión de software Dañino	1	100	100	100		
		(A.9) Re- encaminamiento de mensajes	1			100		
		(A.10) Alteración de secuencia	1		50			
		(A.11) Acceso no autorizado	1		10	50		
		(A.15) Modificación deliberada de la información	1		50			
		(A.18) Destruccion de la informacion	1	50				
		(A.19) Revelacion de informacion	1			50		
		(A.22) Manipulacion de programas	5		100	100		
EQUIPOS								
(HW) equipos informáticos /hardware	Servidores de Base de datos			100	20	50		
		(N.1) Fuego	0,1	100				
		(N.2) Daño por agua	0,1	50				
		(N.*) Desastres naturales	0,1	100				
		(I1) Fuego	0,5	100				
		(I.2) Daño por agua	0,5	50				
		(I.*) Desastres Industriales	0,5	100				
		(I.3) Contaminación mecánica	0,1	50				
		(I.4) Contaminacion electormagnetica	1	10				
		(I.5) Avería de orígen físico o lógico	1	50				
		(I.6) Corte del suministro electrico	1	100				
		(I.7) Condiciones inadecuadas de temperatura o humedad	1	100				
		(I.11) Emanaciones electromagneticas	1			1		
		(E.2) Errores del administrador del sistema / de la seguridad	1	20	20	20		
		(E.23) Errores de mantenimiento /actualización de equipos (hardware)	1	10				
		(E.24) Caída del sistema por agotamiento de recursos	10	50				
		(E.25) Perdida de equipos	1	100		50		
		(A.6) Abuso de privilegios de acceso	1		10	50		
		(A.7) Uso no previsto	1	100	1	10		
		(A.11) Acceso no autorizado	1		10	50		

TIPO DE ACTIVO	ACTIVO		FRE C	DIMENSIONES D	I	C	A	T
		(A.23) Manipulación del hardware	50	50		50		
		(A.24) Denegación del servicio	2	100				
		(A.25) Robo de Equipos	1	100		50		
		(A.26) Ataque Destructivo	1	100				
(HW) equipos informáticos /hardware	Firewall externo			100	20	50		
		(N.1) Fuego	0,1	100				
		(N.2) Daño por agua	0,1	50				
		(N.*) Desastres naturales	0,1	100				
		(I1) Fuego	0,5	100				
		(I.2) Daño por agua	0,5	50				
		(I.*) Desastres Industriales	0,5	100				
		(I.3) Contaminación mecánica	0,1	50				
		(I.4) Contaminacion electormagnetica	1	10				
		(I.5) Avería de orígen físico o lógico	1	50				
		(I.6) Corte del suministro electrico	1	100				
		(I.7) Condiciones inadecuadas de temperatura o humedad	1	100				
		(I.11) Emanaciones electromagneticas	1			1		
		(E.2) Errores del administrador del sistema / de la seguridad	1	20	20	20		
		(E.23) Errores de mantenimiento /actualización de equipos (hardware)	1	10				
		(E.24) Caída del sistema por agotamiento de recursos	10	50				
		(E.25) Perdida de equipos	1	100		50		
		(A.6) Abuso de privilegios de acceso	1		10	50		
		(A.7) Uso no previsto	1	100	1	10		
		(A.11) Acceso no autorizado	1		10	50		
		(A.23) Manipulación del hardware	50	50		50		
		(A.24) Denegación del servicio	2	100				
		(A.25) Robo de Equipos	1	100		50		
		(A.26) Ataque Destructivo	1	100				
(HW) equipos informáticos /hardware	Firewall Interno			100	20	50		
		(N.1) Fuego	0,1	100				
		(N.2) Daño por agua	0,1	50				
		(N.*) Desastres naturales	0,1	100				
		(I1) Fuego	0,5	100				
		(I.2) Daño por agua	0,5	50				
		(I.*) Desastres Industriales	0,5	100				
		(I.3) Contaminación mecánica	0,1	50				
		(I.4) Contaminacion electormagnetica	1	10				
		(I.5) Avería de orígen físico o lógico	1	50				
		(I.6) Corte del suministro electrico	1	100				
		(I.7) Condiciones inadecuadas de temperatura o humedad	1	100				
		(E.2) Errores del administrador del sistema / de la seguridad	1	20				
		(E.23) Errores de mantenimiento /actualización de equipos (hardware)	1	10				
		(E.24) Caída del sistema por agotamiento de recursos	10	50				
		(E.25) Perdida de equipos	1	100				
		(A.23) Manipulación del hardware	0,5	50				
		(A.24) Denegación del servicio	2	100				
		(A.25) Robo de Equipos	1	100				
		(A.26) Ataque Destructivo	1	100				
(HW) equipos informáticos /hardware	Router			100	20	50		
		(N.1) Fuego	0,1	100				
		(N.2) Daño por agua	0,1	50				
		(N.*) Desastres naturales	0,1	100				
		(I1) Fuego	0,5	100				
		(I.2) Daño por agua	0,5	50				
		(I.*) Desastres Industriales	0,5	100				
		(I.3) Contaminación mecánica	0,1	50				
		(I.4) Contaminacion electormagnetica	1	10				
		(I.5) Avería de orígen físico o lógico	1	50				
		(I.6) Corte del suministro electrico	1	100				
		(I.7) Condiciones inadecuadas de temperatura o humedad	1	100				
		(I.11) Emanaciones electromagneticas	1			1		
		(E.2) Errores del administrador del sistema / de la seguridad	1	20	20	20		
		(E.23) Errores de mantenimiento /actualización de equipos (hardware)	1	10				
		(E.24) Caída del sistema por agotamiento de recursos	10	50				
		(E.25) Perdida de equipos	1	100		50		
		(A.6) Abuso de privilegios de acceso	1		10	50		
		(A.7) Uso no previsto	1	100	1	10		
		(A.11) Acceso no autorizado	1		10	50		
		(A.23) Manipulación del hardware	50	50		50		
		(A.24) Denegación del servicio	2	100				
		(A.25) Robo de Equipos	1	100		50		
		(A.26) Ataque Destructivo	1	100				
		(N.1) Fuego	0,1	100				
		(N.2) Daño por agua	0,1	50				
		(N.*) Desastres naturales	0,1	100				
COMUNICACIONES								
(COM) Redes de comunicaciones	Red telefonica basica o RSDI			50				
		(I.8) Fallo en el servicio de comunciaciones	1	50				
		(E.2) Errores del administrador del sistema / de la seguridad	1	20				
		(E.24) Caída del sistema por agotamiento de recursos	1	50				
		(A.7) Uso no previsto	1	10				
		(A.24) Denegación del servicio	10	50				
		(A.26) Ataque Destructivo	1	50				
(COM) Redes de comunicaciones	Red Wan			50	20	50	100	

TIPO DE ACTIVO	ACTIVO		FRE C	DIMENSIONES D	I	C	A	T
		(I.8) Fallo en el servicio de comunciaciones	1	50				
		(E.2) Errores del administrador del sistema / de la seguridad	1	20	20	20		
		(E.9) Errores de re-encaminamiento	1			10		
		(E.10) Errores de secuencia	1		10			
		(E.15) Alteracion de la informacion	1		1			
		(E.19) Fugas de Informacion	1			10		
		(E.24) Caída del sistema por agotamiento de recursos	1	50				
		(A.5) Suplantacion de la identidad del usuario	1		10	50	100	
		(A.6) Abuso de privilegios de acceso	1		10	50		
		(A.7) Uso no previsto	1	10	10	10		
		(E.9) Errores de re-encaminamiento	1			10		
		(A.10) Alteracion de secuencia	1		10			
		(A.11) Acceso no autorizado	1		10	50		
		(A.12) Analisis grafico	1			2		
		(A.14) Interceptación de información (escucha)	1			10		
		(A.15) Modificación deliberada de la información	1		10			
		(A.19) Revelacion de informacion	1			50		
		(A.24) Denegación del servicio	10	50				
		(A.26) Ataque Destructivo	1	50				
(COM) Redes de comunicaciones	Red Lan			50	20	50	100	
		(I.8) Fallo en el servicio de comunciaciones	1	50				
		(E.2) Errores del administrador del sistema / de la seguridad	1	20	20	20		
		(E.9) Errores de re-encaminamiento	1			10		
		(E.10) Errores de secuencia	1		10			
		(E.15) Alteracion de la informacion	1		1			
		(E.19) Fugas de Informacion	1			10		
		(E.24) Caída del sistema por agotamiento de recursos	1	50				
		(A.5) Suplantacion de la identidad del usuario	1		10	50	100	
		(A.6) Abuso de privilegios de acceso	1		10	50		
		(A.7) Uso no previsto	1	10	10	10		
		(E.9) Errores de re-encaminamiento	1			10		
		(A.10) Alteracion de secuencia	1		10			
		(A.11) Acceso no autorizado	1		10	50		
		(A.12) Analisis grafico	1			2		
		(A.14) Interceptación de información (escucha)	1			10		
		(A.15) Modificación deliberada de la información	1		10			
		(A.19) Revelacion de informacion	1			50		
		(A.24) Denegación del servicio	10	50				
		(A.26) Ataque Destructivo	1	50				
(AUX) Equipamento auxiliar	UPS			100	1	50		
		(N.1) Fuego	0,1	100				
		(N.2) Dañor por agua	0,1	50				
		(N.*) Desastres naturales	0,1	100				
		(I1) Fuego	0,5	100				
		(I.2) Dañor por agua	0,5	50				
		(I.*) Desastres Industriales	0,5	100				
		(I.3) Contaminación mecánica	0,1	50				
		(I.7) Condiciones inadecuadas de temperatura o humedad	5	100				
		(E.23) Errores de mantenimiento /actualización de equipos (hardware)	1	10				
		(A.7) Uso no previsto	1	50	1	1		
		(A.11) Acceso no autorizado	1		1	50		
		(A.23) Manipulación del hardware	1	50		50		
		(A.25) Robo de Equipos	1	10				
		(A.26) Ataque Destructivo	1	10				
(AUX) Equipamento auxiliar	Servicios de Energía			100	1	50		
		(N.1) Fuego	0,1	100				
		(N.2) Dañor por agua	0,1	50				
		(N.*) Desastres naturales	0,1	100				
		(I1) Fuego	0,5	100				
		(I.2) Dañor por agua	0,5	50				
		(I.*) Desastres Industriales	0,5	100				
		(I.3) Contaminación mecánica	0,1	50				
		(I.7) Condiciones inadecuadas de temperatura o humedad	5	100				
		(E.23) Errores de mantenimiento /actualización de equipos (hardware)	1	10				
		(A.7) Uso no previsto	1	50	1	1		
		(A.11) Acceso no autorizado	1		1	50		
		(A.23) Manipulación del hardware	1	50		50		
		(A.25) Robo de Equipos	1	10				
		(A.26) Ataque Destructivo	1	10				
(AUX) Equipamento auxiliar	Cableado			100	1	50		
		(N.1) Fuego	0,1	100				
		(N.2) Dañor por agua	0,1	50				
		(N.*) Desastres naturales	0,1	100				
		(I1) Fuego	0,5	100				
		(I.2) Dañor por agua	0,5	50				
		(I.*) Desastres Industriales	0,5	100				
		(I.3) Contaminación mecánica	0,1	50				
		(I.7) Condiciones inadecuadas de temperatura o humedad	5	100				
		(E.23) Errores de mantenimiento /actualización de equipos (hardware)	1	10				
		(A.7) Uso no previsto	1	50	1	1		
		(A.11) Acceso no autorizado	1		1	50		
		(A.23) Manipulación del hardware	1	50		50		
		(A.25) Robo de Equipos	1	10				
		(A.26) Ataque Destructivo	1	10				

TIPO DE ACTIVO	ACTIVO		FREC	DIMENSIONES				
				D	I	C	A	T
(AUX) Equipamento auxiliar	Muebles			100				
		(N.1) Fuego	0,1	100				
		(N.2) Daño por agua	0,1	50				
		(N.*) Desastres naturales	0,1	100				
		(I1) Fuego	0,5	100				
		(I.2) Daño por agua	0,5	50				
		(I.*) Desastres Industriales	0,5	100				
		(I.3) Contaminación mecánica	0,1	50				
		(I.7) Condiciones inadecuadas de temperatura o humedad	5	100				
		(E.23) Errores de mantenimiento /actualización de equipos (hardware)	1	10				
		(A.7) Uso no previsto	1	50				
		(A.23) Manipulación del hardware	1	50				
		(A.25) Robo de Equipos	1	10				
		(A.26) Ataque Destructivo	1	10				
SERVICIOS SUBCONTRATADOS								
(S) servicios	Internet			100	100	50	100	
		(E.1) Errores de los usuarios	1	10	10	10		
		(E.2) Errores del administrador del sistema / de la seguridad	1	20	20	20		
		(E.9) Errores de re-encaminamiento	1			10		
		(E.10) Errores de secuencia	1		10			
		(E.15) Alteración de la información	1		1			
		(E.18) Destrucción de información	1	10				
		(E.19) Fugas de información	1			10		
		(E.24) Caída del sistema por agotamiento de recursos	10	50				
		(A.5) Suplantacion de la identidad del usuario	1		50	50	100	
		(A.6) Abuso de privilegios de acceso	1		10	10		
		(A.7) Uso no previsto	1	100	10	10		
		(E.9) Errores de re-encaminamiento	1			50		
		(A.10) Alteracion de secuencia	1		50			
		(A.11) Acceso no autorizado	1		10	50		
		(A,13) Repudio (Negacion de actuaizaciones)	10		100			
		(A,15) Modificacion de la informacion	10		50			
		(E.18) Destrucción de información	1	50				
		(A.19) Revelacion de informacion	1			50		
		(A.24) Denegación del servicio	10	50				
INSTALACIONES								
(L) Instalaciones	EDIFICIO			100	50	50		
		(N.1) Fuego	1	100				
		(N.2) Daño por agua	1	100				
		(N.*) Desastres naturales	0,5	100				
		(I1) Fuego	1	100				
		(I.2) Daño por agua	1	100				
		(I.*) Desastres Industriales	1	100				
		(I.11) Emanaciones electromagneticas	0,1			1		
		(E.15) Alteración de la información	1		1			
		(E.18) Destrucción de información	1	100				
		(E.19) Fugas de información	1			10		
		(A.7) Uso no previsto	1	10	50	50		
		(A.11) Acceso no autorizado	5		10	10		
		(A,15) Modificacion de la informacion	1		50			
		(E.18) Destrucción de información	1	100				
		(A.19) Revelacion de informacion	1			50		
		(A.26) Ataque Destructivo	0,1	100				
		(A.27) Ocupacion enemiga	1	100		50		
PERSONAL								
(P) Personal	Usuarios externos							
(P) Personal	Usuarios Internos							
(P) Personal	Administrador de Seguridad			10				
		(A.28) Indisponibilidad del personal	0,5	10				
		(A.29) Extorsión	0,9	10				
		(A.30) Ingeniería Social (picaresca)	0,5	10				

5.1.3 Estimación Estado de Riesgo

Es la manera de desarrollar el análisis de las amenazas que presenta la organización, por esto se deben cumplir con las siguientes actividades:

- Estimación del Impacto
- Estimación del Riesgo

Y así obtener los niveles de exposición al riesgo de cada uno de los activos.

Para la elaboración de esta tabla se tomaron los siguientes niveles de criticidad

NIVELES DE CRITICIDAD	
10	CRITICO
8--9	MUY ALTO
6--7	ALTO
4--5	MEDIO
1--3	BAJO
0	DESPRECIABLE

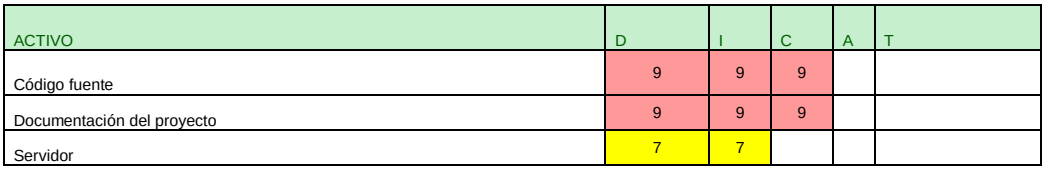
En la tabla 7 se observa el Impacto Acumulado o potencial el cual se evalúa sobre los activos inferiores, es calculado el valor acumulado y la degradación causada por la amenaza.

Tabla 7 IMPACTO ACUMULADO

	DIMENSIONES				
	D	I	C	A	T
ACTIVO	10	9	9	8	
CAPA DE NEGOCIO	9	9	9		
Código fuente	9	9	9		
Documentación del proyecto	9	9	9		
SERVICIOS INTERNOS	7	7			
Servidor	7	7			
Servidor DNS	7	7			
Servicio Directorio	6				
Servidor de correo electrónico	4				
EQUIPAMENTO	10	9	9	8	
APLICACIONES	10	9	9	8	
Servidor web	10	8	8		
Software firewall		8	8		
Sistema de informacion de proyectos	10	9	9	8	
Software de sistema Operativo	10	9	9	8	
Servidores de Base de datos	10	7	8		
Firewall externo	10	6	7		
Firewall interno	10	6	7		
Router	10	6	7		
Red telefonica basica o RSDI	8				
Red Wan	9	6	7		
Red Lan	9	6	7		
UPS	10	3	8		
Servicios de Energía	10	3	8		
Cableado	10	3	8		
Muebles	3				
SERVICIOS SUBCONTRATADOS	10	8	7		
Internet	10	8	7		
INSTALACIONES	10	8	8		
EDIFICIO	10	8	8		
PERSONAL	5				
Administrador de Seguridad	5				

En la gráfica 3 se visualiza e impacto acumulado por cada uno de los activos de la organización.

Gráfica 3 Impacto Acumulado



ACTIVO	D	I	C	A	T
Código fuente	9	9	9		
Documentación del proyecto	9	9	9		
Servidor	7	7			

Servidor DNS	7	7			
Servicio Directorio	6				
Servidor de correo electrónico	4				
Servidor web	10	8	8		
Software firewall		8	8		
Sistema de informacion de proyectos	10	9	9	8	
Software de sistema Operativo	10	9	9	8	
Servidores de Base de datos	10	7	8		
Firewall externo	10	6	7		
Firewall interno	10	6	7		
Router	10	6	7		
Red telefonica basica o RSDI	8				
Red Wan	9	6	7		
Red Lan	9	6	7		
UPS	10	3	8		
Servicios de Energía	10	3	8		
Cableado	10	3	8		
Muebles	3				
Internet	10	8	7		
EDIFICIO	10	8	8		
Administrador de Seguridad	5				

En la tabla 8 se estima en función del valor de cada uno de los activos y las dependencias para lo cual se toma como base el impacto del activo tanto a nivel directo como a nivel indirecto.

Tabla 8 RIESGO ACUMULADO

	DIMENSIONES				
	D	I	C	A	T
ACTIVO	{7,4}	{7,1}	{7,5}	{5,7}	
CAPA DE NEGOCIO	{7,2}	{7,1}	{7,5}		
Código fuente	{7,2}	{7,1}	{7,5}		
Documentación del proyecto	{7,2}	{7,1}	{7,5}		
SERVICIOS INTERNOS	{5,4}	{5,9}			
Servidor	{5,4}	{5,9}			
Servidor DNS	{5,4}				
Servicio Directorio	{5,4}				
Servidor de correo electrónico	{3,3}				

EQUIPAMENTO	{7,4}	{6,9}	{6,9}	{5,7}	
APLICACIONES	{6,8}	{6,9}	{6,9}		
Servidor web	{6,8}	{6,3}	{6,3}		
Software firewall		{6,3}	{6,3}		
Sistema de informacion de proyectos	{6,8}	{6,9}	{6,9}	{5,7}	
Software de sistema Operativo	{6,8}	{6,9}	{6,9}	{5,7}	
Servidores de Base de datos	{7,2}	{5,0}	{5,7}		
Firewall externo	{7,2}	{4,4}	{5,1}		
Firewall interno	{7,2}	{4,4}	{5,1}		
Router	{7,2}	{4,4}	{5,1}		
COMUNICACIONES	{7,2}	{4,4}	{5,1}		
Red telefonica basica o RSDI	{6,6}				
Red Wan	{7,2}	{4,4}	{5,1}		
Red Lan	{7,2}	{4,4}	{5,1}		
UPS	{7,4}	{2,7}	{5,7}		
Servicios de Energía	{7,4}	{2,7}	{5,7}		
Cableado	{7,4}	{2,7}	{5,7}		
Muebles	{3,3}				
SERVICIOS SUBCONTRATADOS	{7,2}	{6,5}	{5,1}		
Internet	{7,2}	{6,5}	{5,1}		
INSTALACIONES	{6,8}	{5,7}	{5,7}		
EDIFICIO	{6,8}	{5,7}	{5,7}		
PERSONAL	{3,8}				
Administrador de Seguridad	{3,8}				

La grafica 4 de riesgo acumulado nos indica la medida en que las amenazas afectan los activos de orden superior al igual a los que depende de dicho activo.

Gráfica 4 Riesgo Acumulado

ACTIVO	D	I	C	A	T
Código fuente	{7,2}	{7,1}	{7,5}		
Documentación del proyecto	{7,2}	{7,1}	{7,5}		
Servidor	{5,4}	{5,9}			
Servidor DNS	{5,4}				
Servicio Directorio	{5,4}				
Servidor de correo electrónico	{3,3}				
Servidor web	{6,8}	{6,3}	{6,3}		
Software firewall		{6,3}	{6,3}		
Sistema de información de proyectos	{6,8}	{6,9}	{6,9}	{5,7}	
Software de sistema Operativo	{6,8}	{6,9}	{6,9}	{5,7}	
Servidores de Base de datos	{7,2}	{5,0}	{5,7}		
Firewall externo	{7,2}	{4,4}	{5,1}		
Firewall interno	{7,2}	{4,4}	{5,1}		
Router	{7,2}	{4,4}	{5,1}		
Red telefónica básica o RSDI	{6,6}				
Red Wan	{7,2}	{4,4}	{5,1}		
Red Lan	{7,2}	{4,4}	{5,1}		
UPS	{7,4}	{2,7}	{5,7}		
Servicios de Energía	{7,4}	{2,7}	{5,7}		
Cableado	{7,4}	{2,7}	{5,7}		
Muebles	{3,3}				
Internet	{7,2}	{6,5}	{5,1}		
EDIFICIO	{6,8}	{5,7}	{5,7}		
Administrador de Seguridad	{3,8}				

En la tabla número 9 se puede observar que los activos se relacionan unos con otros, de forma que el efecto de una amenaza en un activo tiene consecuencias indirectas en los activos que dependen del activo directamente dañado, El impacto repercutido mide el daño en los activos superiores.

El impacto repercutido se calcula tomando en cuenta:

- el valor propio del activo superior
- la degradación causada por la amenaza en el activo inferior
- el grado de dependencia del activo superior del activo inferior

Básicamente, la degradación del activo inferior repercute sobre el activo superior en la medida indicada por el grado de dependencia:

Impacto repercutido = valor * degradación * grado [15]

Tabla 9 IMPACTO REPERCUTIDO

	DIMENSIONES				
	D	I	C	A	T
ACTIVO					
CAPA DE NEGOCIO					
Código fuente	10	9	9		
Documentación del proyecto	10	9	9		
SERVICIOS INTERNOS					
Servidor	7	7			
Servidor DNS	7				
Servicio Directorio	7				
Servidor de correo electrónico	4				
EQUIPAMENTO					
APLICACIONES					
Servidor web	10	8	8		
Software firewall		8	8		
Sistema de informacion de proyectos	8	8	8	8	
Software de sistema Operativo	8	9	9	8	
EQUIPOS					
Servidores de Base de datos	9				
Firewall externo	8				
Firewall interno	8				
Router	8				
Red telefonica basica o RSDI	9				
Red Wan	8				
Red Lan	9				
UPS	7				
Servicios de Energía	7				
Cableado	8				

15 Glosario de términos de la Herramienta Pilar –Magerit recuperada de la página web: http://www.ar-tools.com/es/glossary/index.html

Muebles	3				
SERVICIOS SUBCONTRATADOS					
Internet	9				
INSTALACIONES					
EDIFICIO	7				
PERSONAL					
Usuarios externos					
Usuarios Internos					
Administrador de Seguridad	5				

En la gráfica 5 se visualiza e impacto repercutido por cada uno de los activos de la organización.

Gráfica 5 Impacto Repercutido

ACTIVO	D	I	C	A	T
Código fuente	10	9	9		
Documentación del proyecto	10	9	9		
Servidor	7	7			
Servidor DNS	7				
Servicio Directorio	7				
Servidor de correo electrónico	4				
Servidor web	10	8	8		
Software firewall		8	8		
Sistema de informacion de proyectos	8	8	8	8	
Software de sistema Operativo	8	9	9	8	
Servidores de Base de datos	9				
Firewall externo	8				
Firewall interno	8				
Router	8				
Red telefonica basica o RSDI	9				
Red Wan	8				
Red Lan	9				
UPS	7				
Servicios de Energía	7				
Cableado	8				
Muebles	3				
Internet	9				
EDIFICIO	7				
Administrador de Seguridad	5				

En la tabla 10 se muestra el valor que se calcula teniendo en cuenta los diferentes valores de cada uno de los activos sin considerar las dependencias.

Tabla 10 RIESGO REPERCUTIDO

ACTIVO	D	I	C	A	T
Código fuente	{7,4}	{7,1}	{7,5}		
Documentación del proyecto	{7,4}	{7,1}	{7,5}		
Servidor	{5,7}	{5,9}			
Servidor DNS	{5,4}				
Servicio Directorio	{5,7}				
Servidor de correo electrónico	{3,3}				
Servidor web	{7,4}	{6,5}	{6,3}		
Software firewall		{6,3}	{6,3}		
Sistema de informacion de proyectos	{6,3}	{6,3}	{6,3}	{5,7}	
Software de sistema Operativo	{5,7}	{6,9}	{6,9}	{5,7}	
Servidores de Base de datos	{6,9}				
Firewall externo	{6,3}				
Firewall interno	{6,3}				
Router	{6,3}				
Red telefonica basica o RSDI	{6,9}				
Red Wan	{6,3}				
Red Lan	{6,9}				
UPS	{5,7}				
Servicios de Energía	{5,7}				
Cableado	{6,3}				
Muebles	{3,3}				
Internet	{6,9}				
EDIFICIO	{5,1}				
Administrador de Seguridad	{3,8}				

En la tabla 11 Se plasman los diferentes controles que puede implementar la organización con la finalidad de minimizar los riesgos que visualizaron en el análisis anterior.

Tabla 11 CONTROLES PARA APLICAR

ACTIVOS	TIPOS DE CONTROL	ACCIONES CONTROL A IMPLEMENTAR
DATOS		
DATOS	PREVENCIÓN	Asignar Roles y Responsabilidades
		Ofrecer seguridad a través de la definición del trabajo y los recursos
	DETENCION	Responsabilidades y procedimientos
		Proteger los diferentes registros de la institución
	RECUPERACION	Protección de los datos y de la privacidad de la información personal del cliente
		Seguridad de oficinas, despachos y recursos
PERSONAL		
EMPLEADOS	PREVENCION	Términos y condiciones de las relaciones laborales
		Controles de confidencialidad
	DETENCION	Procesos de tipo disciplinario dentro de la entidad
		Responsabilidades de tipo administrativo
	RECUPERACION	Administración de incidentes y las continuas mejoras dentro de la seguridad de la información
		Conocimiento de la educación y entrenamiento de la seguridad de la información
TECNOLOGIA		
HARDWARE PORTATIL	PREVENCION	Seguridad de los equipos fuera de la institución
		Requerimientos para el control de acceso
	DETENCION	Controles para acceder al sistema operativo
		Procedimientos de conexiones de terminales
	RECUPERACION	Mantenimiento de Equipos
		Compra de seguros para cada uno de los equipos
PC DE OFICINA	PREVENCION	Utilización de Contraseñas
		Equipo informático de usuarios desentendidos
	DETENCION	Conocimiento de la educación y entrenamiento de la seguridad de la información
		Seguridad en los equipos
	RECUPERACION	Copias no autorizadas de software o información propietaria

ACTIVOS	TIPOS DE CONTROL	ACCIONES CONTROL A IMPLEMENTAR
		Controles de tipo físico tanto para la entrada y salida de los equipos
SERVIDORES	PREVENCION	Monitoreo de red
		Control acceso a la red
	DETENCION	Protección a puertos de diagnóstico remoto
		Control de conexión a las redes
	RECUPERACION	Identificación y autenticación de movimientos en la red
		Administración de incidentes y recuperación de Backus
PAQUETES DE SOFTWARE ESTANDAR	PREVENCION	Seguridad en los procesos de desarrollo y soporte
		Seguridad en la definición del trabajo y los recursos
	DETENCION	Gestión de acceso a los usuarios
		Gestión interna de respaldo
	RECUPERACION	Recuperación de la información
		Control de vulnerabilidades técnicas
SISTEMAS OPERATIVOS	PREVENCION	Revisión Técnica de los cambios en el sistema operativo
		Procedimientos de conexiones de terminales
	DETENCION	Documentación de procedimientos operativos
		Control de cambios operaciones
	RECUPERACION	Recuperar Backus, puntos de restauración
		Control de acceso al sistema operativo
MEDIOS Y SOPORTES	PREVENCION	Autenticación de usuarios para conexiones externas
		Autenticación de nodos de la red
	DETENCION	Administración de incidentes y mejoras de la seguridad
		Monitorización del uso del sistema
	RECUPERACIÓN	Analizar el registro de fallas
		Protección a puertos de diagnóstico remoto
INFRAESTRUCTURA		
ESTABLECIMIENTOS	PREVENCION	Requerimientos para el control de acceso
		Monitorear el control de acceso de personal
	DETENCION	Establecer de controles de detención de sismos, incendios
		Monitoreo del cableado estructurado de la infraestructura
	RECUPERACION	Reemplazar las redes de cableado defectuosas
		Establecer plan de continuidad de la institución
SISTEMAS DE INFORMACION		
SISTEMAS WEB	PREVENCION	Protección contra software maliciosos
		Gestión de vulnerabilidades técnicas
	DETENCION	Gestión de acceso a los usuarios
		Restricciones de los cambios en el sistema operativo
	RECUPERACION	Recuperación de la información
		Revisión Técnica de los cambios en el sistema operativo
PROCESOS		
SERVICIO DE COREO ELECTRONICO	PREVENCION	Monitoreo de las posibles suplantación de identidad
		Controles de Red
	DETENCION	Revisión de registros de usuarios
		Revisión de derechos de acceso a los usuarios
	RECUPERACION	Políticas de uso de los controles criptográficos
		Gestión de Servicios externos
SISTEMAS DE TRAMITE	PREVENCION	Realizar mantenimiento periódicamente
		Tener los datos actualizados
	DETENCION	Revisión de los usuarios privilegiados
		Verificar el desvió de la información
	RECUPERACION	Realizar la actualización de los datos
		realizar copias de Backus periódicamente
SISTEMAS DE COMUNICACIÓN	PREVENCION	uso de contraseñas
		Protección contra amenazas externas y ambientales
	DETENCION	Monitorizar y revisar los servicios de terceras partes
		Controles físicos de entrada
	RECUPERACION	Gestión de servicios externos
		Degradación del servicio y equipo

En la gráfica 6 se puede evidenciar toda la información resumida el análisis y gestión de riesgos

Gráfica 6 Matriz de Riesgo

ANALISIS DE RIESGOS										EVALUACION DE RIESGOS					RIESGO RESIDUAL			TRATAMIENTO			
TIPO DE ACTIVO	ACTIVO	RIESGO	DESCRIPCION	CLASIFICACION	GENERADOR	CAUSAS	CONSECUENCIAS	VALOR	IMPACTO	CONTROL	TIPO DE CONTROL	APLICACION	EFICACIA DEL CONTROL	FRECUENCIA DE MONITOREO	VALOR	IMPACTO	ACCION TRATAMIENTO	TIEMPO DE IMPLEMENTACION	COSTO	RESPONSABLE
(D) Datos/ informacion	Código Fuente	Almacenamiento de datos no protegidos Documentación no actualizada Falta de controles para el establecimiento de contratos Falta de atención del personal Perdida de información	Existe la posibilidad que se tenga acceso a la información, además que no se encuentre actualizada, sea destruida, modificada	RIESGO CONFIDENCIAL	INTERNO	mínimo nivel de acceso a la información , falta de conocimiento de la políticas de información , daños por parte de terceros , daños mal intencionados por parte de terceros	perdida de confianza por la parte externa de la organización, perdida de información	9	MUY ALTO	Asignar Roles y Responsabilidades Ofrecer seguridad a través de la definición del trabajo y los recursos Responsabilidades y procedimientos Proteger los diferentes registros de la institución Protección de los datos y de la privacidad de la información personal del cliente Seguridad de oficinas, despachos y recursos	PREVENCIÓN DETENCION RECUPERACION	SI	ALTO	DIARIA	10	MUY ALTO	Reasignación de Roles en el sistema, implementación de mas niveles de seguridad, socialización de las políticas de manejo de información	Según la ocurrencia	MEDIO	Los procesos que se encuentra involucrados con la información de la organización
	Documentación del proyecto							9	MUY ALTO			SI	ALTO		10	MUY ALTO				
(S) servicios	Servidor WSUS	Ingresar código malicioso Falta de monitoreo en los servidores No plan de continuidad del negocio No hay protección en los archivos de registro contraseñas no seguras	se pueden generar errores por caida del sistema debido a la falta de fluido electrico o mal funcionamiento de las maquinas.	RIESGO TECMOLOGICO	INTERNO /EXTERNO	1. Se pierda la disponibilidad del servicio por parte del proveedor 2. Falta de mantenimiento de los equipos y redes 3. Deterioro de las redes 4. Manejo adecuado y operación de los usuarios y técnicos 6. Falla en las comunicaciones. 7. Fluctuaciones en el fluido electrico. 8. Falta de protección ante picos de voltajes y/o interrupción del fluido electrico no planificado	demora en los procesos, información que se extravia, la imagen de la entidad se puede ver afectada ante el publico, no genera sus procesos de manera oportuna, la operación no realiza sus labores de manera normal alteración de la operación.	7	ALTO	Seguridad en los equipos Copias no autorizadas de software o información propietaria Controles de tipo físico tanto para la entrada y salida de los equipos Monitoreo de red Control acceso a la red Protección a puertas de diagnóstico remota Control de conexión a las redes Identificación y autenticación de terminales en la red Administración de incidentes y recuperación de Backup	PREVENCIÓN DETENCION RECUPERACION	SI	ALTO	SEMANAL		ALTO	se tiene que realizara la capacitacion correspondiente al uso adecuado, , lograr un sistema redundante para la institucion	según la ocurrencia	ALTO	Departamento de sistemas
	Servidor DNS							7	ALTO			SI	ALTO		7	ALTO				
	Servicio Directorio							6	ALTO			SI	ALTO		7	ALTO				
	Servidor de correo electrónico							4	MEDIO			SI	MEDIO		4	MEDIO				
(SW) aplicaciones	Servidor web	Amenazas phishing Amenazas de hackers compra de software licenciados	Esta se genera debido al acceso no autorizado del personal, suplantacion de identidad, falta de respaldos de información, recursos compartidos con redes no protegidos o no confiables					10	CRITICO	Protección contra software malicioso Gestión de vulnerabilidades técnicas Gestión de acceso a los usuarios Restricciones de los cambios en el sistema operativo Recuperación de la información Revisión Técnicas de los cambios en el sistema operativo	PREVENCIÓN DETENCION RECUPERACION	SI	ALTO	SEMANAL	10	CRITICO	Robustecer la seguridad mejorando los cortafuegos. Instalación de un IDS y un WIDS Aplicar buenas practicas en el desarrollo de sistemas de información seguros.	Diariamente	MEDIO	Departamento de sistemas
	Softwares firewall	información, vulnerabilidades de los programas,	Bajo nivel de seguridad en el acceso a la información							Protección contra software malicioso Gestión de vulnerabilidades técnicas Gestión de acceso a los usuarios Restricciones de los cambios en el sistema operativo Recuperación de la información Revisión Técnicas de los cambios en el sistema operativo	PREVENCIÓN DETENCION RECUPERACION	SI								
	Sistema de información de proyectos	información, vulnerabilidades de los programas,	alteracion o daño de la información, se presentan varios errores de los usuarios					10	CRITICO			SI	ALTO		8	MUY ALTO				
	Softwares de sistema Operativo	falta de documentacion del sistema, falta de	Esta se genera por la poca capacitacion a los usuarios de la organización					10	CRITICO			SI	ALTO		8	MUY ALTO				

ANALISIS DE RIESGOS										EVALUACION DE RIESGOS					RIESGO RESIDUAL			TRATAMIENTO		
TIPO DE ACTIVO	ACTIVO	RIESGO	DESCRIPCION	CLASIFICACION	GENERADOR	CAUSAS	CONSECUENCIAS	VALOR	IMPACTO	CONTROL	TIPO DE CONTROL	APLICACIÓN	EFICACIA DEL CONTROL	FRECUENCIA DE CONTROL	VALOR	IMPACTO	ACCION TRATAMIENTO	TIEMPO DE IMPLEMENTACION	COSTO	RESPONSABLE
(HW) equipos informaticos Hardware	Servidores de Bases de datos	Gran numero de puertos abiertos y la no se conoce el manejo correcto de	alta controles en la seguridad de la red y capacitacion para el manejo de la aplicacion.	RIESGO TECNOLOGICO	INTERNO (EXTERNO	1.El mantenimiento en los equipos es minimo o casi nulo 2.Recurso a nivel de tecnologia no cuentan con la mejor calidad 3. no utilizan las recursos tecnologicos necesarios 4. El personal no tiene la capacitacion adecuada para su utilizacion en los diferentes recursos a nivel de tecnologia . 5. Falta de proteccion de los recursos tecnologicos.6. Factores ambientales	Estaos equipos en malas condiciones y dañados, la tecnologia no se aprovecha de la mejor manera, el personal varias veces no sabe como desarrollar sus labores, perdida de datos	10	CRITICO	Monitoreo de red Control acceso a la red Protección a puertas de diagnóstico remoto Control de conexión a las redes Identificación y autenticación de movimientos en la red Administración de incidentes y recuperación de Backus	PREVENCIÓN DETENCION RECUPERACION	SI	ALTO	SEMANAL	9	MUY ALTO	Contratar servicio de personas expertas para el manejo y adecuacion de los mismo	Según la ocurrencia	BAJO	Departamento de Sistemas
	Firewall externo							10	CRITICO			SI	ALTO	MENSUAL	8	MUY ALTO				
	Firewall Interno	Daños, deterioro o pérdida de los recursos						10	CRITICO			SI	ALTO	MENSUAL	8	MUY ALTO				
	Routes		Posibilidad de que se presentes daños, fallas o perdidas de los recursos tecnologicos, en su uso, y/o almacenamiento					10	CRITICO			SI	ALTO	MENSUAL	8	MUY ALTO				
(COM) Redes de comunicaciones	Red telefonica basica o RSDI	Fallas en los servicios de comunicaciones que puedan generar perdida de informacion	Posibilidad de que se presentes fallas en las telecomunicaciones			1. Falta de disponibilidad del servicio por parte del proveedor 2. Falta de mantenimiento de los equipos y redes 3. Deterioro de las redes 4. Manejo adecuado y operación de los usuarios y tecnicos	Perdida de información, demora en los procesos,perdidad de la imagen de la entidad ante el publico, información inoportuna, incumplimiento del proceso, alteración de la operación.	8	MUY ALTO	uso de contraseñas Protección contra amenazas externas y ambientales Monitorizar y revisar los servicios de terceras partes Controles físicos de entrada Gestión de servicios externos Degradación del servicio y equipo	PREVENCIÓN DETENCION RECUPERACION	SI	ALTO	MENSUAL	9	MUY ALTO				
	Red Wan							9	MUY ALTO			SI	ALTO	SEMANAL	8	MUY ALTO				
	Red Lan							9	MUY ALTO			SI	ALTO	SEMANAL	9	MUY ALTO				
(AUX) Equipamiento auxiliar	UPS	Daños, deterioro o pérdida	Posibilidad de que se presentes daños, fallas o perdidas de los recursos	SGO LOCAT	INTERNO	Falla en las comunicaciones, Fluctuaciones en el fluido electrico.Falta de protección ante pico de voltajes y/o interrupción	Perdida de información, demora en los procesos,perdidad de la imagen de la entidad ante el publico, información inoportuna, incumplimiento del proceso, alteración de la operación.	10	CRITICO	Requerimientos para el control de acceso Monitorear el control de acceso de personal Establecer de controles de detección de sismos, incendios	PREVENCIÓN DETENCION RECUPERACION	SI	ALTO	MENSUAL	7	ALTO	solicitar verificacion por parte del area encargada para la realizacion de las diferentes	Según la ocurrencia	MEDIO	Servicios Generales Locativos
	Planta Electrica							10	CRITICO			SI	ALTO	MENSUAL	7	ALTO				
	Cableado							10	CRITICO			SI	ALTO	MENSUAL	8	MUY ALTO				
	Muebles							3	BAJO			SI	BAJO	MENSUAL	3	BAJO				
(S) servicios	Internet 3	falta de control de servicios externos	Bajo relevancia al mal desempeño, falta y/o deficiencia	RIESGO TECNOLOGICO	INTERNO (EXTERNO	Falta de disponibilidad del servicio por parte del proveedor	genera perdida de informacion y retraso en las actividades	10	CRITICO	uso de contraseñas Protección contra amenazas externas y ambientales Monitorizar y revisar los servicios de terceras partes		SI	ALTO	MENSUAL	9	MUY ALTO	Controlar la prestacion del servicio y su efectividad por parte del	gún la ocurrencia	MEDIO	comunicaciones
(I) Instalaciones	EDIFICIO	Perdida de información y falta de proteccion fisica adecuada, contra los desastres naturales.	las instalaciones de la organizacion no se encuentran en debida forma	RIESGO LO	INTERNO	falta de la infraestructura adecuada para el funcionamiento de la organización	genera perdida de informacion y retraso en las actividades	10	CRITICO	Requerimientos para el control de acceso Monitorear el control de acceso de personal Establecer de controles de detección de sismos, incendios		SI	ALTO	MENSUAL	7	ALTO	solicitar verificacion por parte del area encargada para la realizacion de las diferentes	gún la ocurrencia	MEDIO	Servicios Generales Locativos
(P) Personal	Usuarios externos										PREVENCIÓN DETENCION RECUPERACION	SI		MENSUAL						
	Usuarios Internos											SI		MENSUAL						
	Administrador de Seguridad	Falta de conocimiento y oportuno entrenamiento	falta de capacitacion	RIESGO HU	INTERNO	al ejecucion de sus labor	genera perdida de informacion y retraso en las actividades	5	MEDIO	Términos y condiciones de las relaciones laborales Controles de confidencialidad Procesos de tipo disciplinario dentro de la entidad Responsabilidades de tipo administrativo Administración de incidentes y las continuas mejoras dentro de la seguridad de la información Conocimiento de la educación y entrenamiento de la seguridad de la información		SI	MEDIO	MENSUAL	5	MEDIO	Dirrigir charlas y capacitacion del mismo	gún la ocurrencia	BAJO	Procesos involucrados

En la Tabla 12 se encuentran los costos totales para el desarrollo de la implementación estarían calculados aproximadamente de la siguiente manera:

Tabla 12 Costos

DETALLE	**VALOR ANUAL**
SOFTWARE	11.473.395
APLICACIONES	50.000.000
PERSONAL CAPACITADO	81.000.000
HARDWARE	200.000.000
EQUIPAMENTO AUXILIAR	30.000.000
ADECUACIONES INSTALACIONES	15.000.000
ENERGIA ELECTRICA	10.000.000
GASTOS DE FORMACION	30.000.000
GASTOS VARIOS	40.000.000
COSTO	467.473.395
5% MARGEN DE ERROR	23.373.670
COSTO TOTAL DEL PROYECTO	490.847.065

Los valores están calculados a septiembre de 2015 pero pueden variar de acuerdo a la tasa de cambio representativa para el mercado (TRM) en el periodo que se desee realizar la implementación además se calculó un 5% de margen de error.

5.1.4 Políticas de seguridad de la información

Desde la seguridad informática se define la información como un recurso necesario por la organización al igual que sus activos, razón por la cual se busca su protección integrando sus tres principios básicos confidencialidad, integridad y disponibilidad, utilizando para ello un conjunto de normas, métodos, herramientas y personal humano calificado, con el fin de minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo.

Finalidad

Brindar la protección a los recursos de la información que son propiedad de la institución al igual que la tecnología que emplea para cada uno de sus procedimientos ante eventuales amenazas de carácter interno o externo, deliberado o accidental, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la

información. Esto se puede establecer o llevar a cabo manteniendo dentro de la organización las políticas de seguridad en un estado de actualización constante lo cual lo efectúa el profesional certificado en las norma ISO 27001 para asegurar su vigencia y nivel de eficacia.

Alcance

Esta Política se pretende implementar al diferente recurso que posee la institución, así como en los procesos internos y externos relacionados a la entidad por medio de contratos o intervención a través de acuerdos con terceros.

Documento de Política de Seguridad de la Información:

A través de este documento se quiere dar a conocer a los empleados del policlínico la política de seguridad, para que de esta manera se minimicen los errores de los empleados y los problemas que podrían ocurrir al igual que los daños que pueden producir, además se refleja el entrenamiento y los controles necesarios que asegurarán que los empleados pueden comprender la mala utilización de la información, así como sus consecuencias a nivel legal.

5.1.5 Aspectos a desarrollar a nivel Organizativos para la Seguridad.

En el desarrollo de los aspectos correspondientes a nivel organizativo para ofrecer la seguridad se hace necesaria la creación o definición de un marco que sirva para gestionar las diferentes tareas como la aprobación de las políticas necesarias, las funciones y responsabilidades que van a ser asignadas a cada uno de los empleados para dar la eficiencia necesaria en la administración de la seguridad de la información, teniendo en cuenta que en varias ocasiones los terceros deben tener acceso a la diferentes datos de la información que es manejada por la institución, sea necesaria la tercerización de algunas de las funciones del procesamiento de información.

Finalidad

Buscar la forma de llevar a cabo la administración de la seguridad de la información en la sociedad con el fin de establecer la manera como se va a determinar como de parte de la gerencia se va a iniciar, controlar y llevar a cabo la

implementación así como la distribución de las diferentes funciones y responsabilidades

Se necesita aprobar la aplicación de las diferentes medidas de seguridad para que los terceros puedan acceder a la información de la entidad. Conformar un comité de seguridad de la información que nos permita obtener las propuestas para ser llevadas a la Gerencia para su aprobación y así poder generar la definición y asignación de las responsabilidades que surjan en las funciones

Otra parte que puede ser muy importante para la seguridad de la información es la de poder definir el proceso que se va a utilizar para otorgar la autorización de los nuevos recursos Tanto para el procesamiento de información como para los requerimientos de Seguridad en contratos con Terceros, los principales puntos que se deben considerar serían los siguientes:

a) Buscar los diferentes mecanismos necesarios para dar cumplimiento a las Políticas de seguridad de la información en la Institución.

b) Dar la protección necesaria a cada uno de los activos de la institución teniendo en cuenta lo siguiente:

   - Fomentando procedimientos que nos colaboren en el cuidado y protección de los activos entre los que abarque los activos físicos, información y el software.

   - Procedimiento a través del cual se pueda obtener la información necesaria para determinar si ha ocurrido algún evento que llegue a comprometer algunos de los bienes de la organización como por ejemplo la pérdida o modificación de los datos.

   - Controles que no s colaboren tanto en la garantía de la recuperación o la destrucción de los activos o información al tener la terminación de uso de un contrato o por la por la terminación de la vigencia de uso del mismo.

c) Dar una descripción de tipo detallado de cada uno de los servicios disponibles.

d) Mostrar los niveles de servicio tanto al que puede ser esperado y los que deben ser aceptables.

e) Permisos que necesarios para la transferencia de personal de un lugar a otro cuando sea necesario.

f) Dar a conocer las diferentes obligaciones que son partes del acuerdo y las diferentes responsabilidades legales.

g) Definiciones que se encuentran íntegramente relacionadas con la protección de los datos.

h) Generar medios que nos permitan llevar a cabo la revisión o control de la protección física requerida y los mecanismos necesarios.

i) Métodos y procedimientos en los que se defina la forma en que se va originar el entrenamiento de los usuarios y los diferentes administradores en materia de la seguridad.

j) Generar controles que nos permitan garantizar la protección contra el software de tipo malicioso.

La Organización de tipo interno.

Realizar la asignación de responsabilidades sobre seguridad de la información
Efectuar un entrenamiento de tipo adecuado para cada uno de los empleados con el fin de dar una mejora en la cultura de la seguridad de la información en la institución a través de lo que se puede llegar a la reducción de los errores de los empleados y también limitara los problemas que podrían ocurrir al igual que los impactos.

5.1.6 Procesos de autorización de los diferentes recursos.

Para el tratamiento de la información esto con el fin de llevar a cabo la implementación de los controles que nos permitan reducir el riesgo de acceso a los recursos de información de manera autorizada, por lo que hace necesario la creación de responsabilidades para la seguridad.

5.1.7 Los Dominio de gestión en los activos de la red de información:

Se utiliza el conocimiento sobre los diferentes activos que posee la institución y que de acuerdo a su clasificación son parte importante en la administración de riesgos, los cuales deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o de acuerdo con la funcionalidad que cumple con el objeto de señalar como ha de ser tratada y protegida dicha información.

Finalidad

Proporcionar un apropiado nivel de protección con el fin de dar la clasificación de la información para señalar la sensibilidad y creatividad con la finalidad de definir los niveles de protección y medidas de tratamiento especial en acorde a su clasificación.

- La Responsabilidad que se debe generar sobre los activos

Como propietarios de la información debemos encargarnos de dar la clasificación de acuerdo a su sensibilidad y criticidad con la finalidad de llevar acabo la documentación y mantener actualizada la clasificación que se efectuó. La persona que se encuentra responsable de la seguridad de la información es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de la información con el fin de llevar a cabo la contemplación de los diferentes requerimientos de la seguridad que se deben establecer de acuerdo a la criticidad de la información que procesan.

Se debe realizar la supervisión de los procesos de clasificación y dar la rotulación correspondiente en cada una de las áreas por cada uno de los propietarios de la información para dar el cumplimiento establecido de la política de la información.
Al realizar la identificación de los activos más importantes que se encuentran asociados con cada uno de los sistemas de información y cada uno de los propietarios los cuales colaborar en el inventario con la información de cada uno de ellos, el cual tendrá una actualización o modificación de la información que se encuentra almacenada con una periodicidad de 4 meses para lo cual habrá una persona en cargada en cada una de las unidades de la Organización.

- Responsabilidad sobre los activos.

A través del inventario de activos se trata de controlar que estos no se desaparezcan o sean robados esto se permite realizar a través de la asignación de los diferentes propietarios y con lo que también se tendría identificado todos los activos de la institución.

- Propiedad sobre los diferentes recursos

En este punto lo que se busca desarrollar es un control sobre los diferentes activos que se encuentran dentro de la institución para lo cual se realiza la asignación de propietarios a cada uno de ellos para su respectiva identificación.

- El uso de manera responsable de los recursos

Con el fin de colocar en el más mínimo riesgo los recursos se debe realizar la utilización de cada uno de los activos a través de guías teniendo en cuenta las diferentes premisas de la institución.

5.1.8 Dominio de seguridad de los recursos humanos:

Para ofrecer la seguridad de la información nos debemos basar en la capacidad para dar la conservación de la integridad, confidencialidad y disponibilidad de los activos.

Para poder desarrollar lo que anteriormente descrito lo que se efectuar la educación e información al personal de manera constante tanto desde su ingreso a la organización acerca de las diferentes medidas de seguridad que se van incrementando y aumentando en el desarrollo de sus funciones y las expectativas que se tienen con el fin de desarrollar las expectativas depositadas en ellos en materia de seguridad, por lo cual es necesario para definir las diferentes sanciones que se deberán realizar cuando no se cumpla las políticas de seguridad.

Finalidad

La idea es obtener la reducción de los posibles riesgos de error a nivel humano, al utilizar de manera inadecuada de las instalaciones y los diferentes recursos además del manejo no autorizado de la información.

Otro punto importante es el de las responsabilidades que en materia de seguridad en la etapa deben ser incluidas en la incorporación del personal e incluirlas en los diferentes acuerdos que deben ser firmados y verificados para su cumplimiento en el desempeño del individuo como empleado.

Dar a conocer de manera constante a los usuarios el conocimiento de las amenazas que se presentan en la seguridad de la información esto con el fin de que se dé respaldo a la política de seguridad de la institución en el transcurso de las tareas cotidianas.

Establecimiento de compromisos de Confidencialidad con todas las personas de las instalaciones de procesamiento de información de la institución, a través del establecimiento de herramientas y mecanismos necesarios para promover la comunicación de las diferentes debilidades existentes en materia de la seguridad al igual que los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir que se vuelvan a presentar.

Seguridad en la definición del trabajo y los recursos

Al momento de realizar la descripción de las responsabilidades en los puestos de trabajo se debe incorporar las funciones y responsabilidades en materia de

seguridad, las cuales deberán tener las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad además de las responsabilidades que se vinculan o tienen que ver con cada una de las protecciones que son necesarias para los activos, ejecución de procesos para las actividades de seguridad determinadas.

Se debe llegar a especificar el procedimiento a través del cual se va a seleccionar el personal.

Control de Seguridad en la definición del trabajo y los recursos.

Roles y responsabilidades

Al implementar estos diferentes controles para hacer que los empleados se encuentren conscientes de su responsabilidad esto con el fin de colaborar en la reducción del riesgo con eso el impacto seguirá siendo alto, este riesgo no puede reducirse más allá.

Lo que se busca es la reducción del riesgo, si se escoge de manera oportuna a los empleados por esta razón se debe plantear una política de selección del personal a través de la cual se definirán los diferentes roles y responsabilidades.

Selección y política del personal

La necesidad de realizar este proceso es la reducir el riesgo para lo cual se hace muy importante la selección del personal de manera oportuna para lo cual se llevara a cabo el establecimiento de una política para la selección de personal.

Términos y condiciones de la relación laboral

Se busca reducir el riesgo del mal uso de los activos al hacer que los empleados comprenden sus responsabilidades, y sus roles con respecto a la seguridad de información.

Responsabilidades de administración

Es necesario realizar las respectivas verificaciones del conocimiento apropiado de los empleados de las amenazas de seguridad y como se puede reducir el riesgo y los posibles impactos, otra parte importante es el conocimiento de los roles y responsabilidades que posee el empleado para de esta manera disminuir el mal uso de cada uno de los activos además de ofrecerles conocimiento, educación e información de cómo llevar a cabo la seguridad de la información dentro de su institución.

Todo esto con el fin de reducir el riesgo y sus posibles impactos, lo cual reducirá los errores de los empleados y también limitará los problemas que podría ocurrir y sus impactos.

Proceso disciplinario

Los empleados deben tener conocimiento claro y específico de los riesgo que surgen en el momento de ejecutar un código malicioso desconocido y qué consecuencias que nos puede generar esta acción dentro del proceso interno de manejo de información , al igual del proceso de tipo disciplinario que le puede acarrear por desconocimiento.

5.1.9 Dominio de seguridad física y del entorno:

La seguridad física y del entorno ambiental busca la minimización de los riesgos de daños e interferencias a la información y las diferentes operaciones de la institución con la finalidad de evitar el mayor riesgo posible de acceso físicos no autorizados, mediante el establecimiento de parámetros de seguridad, lo que nos va permitir aumentar y mejorar el funcionamiento de los procesamientos y así obtener la más mínima interrupción del servicio.
En las oficinas también se encuentra una gran cantidad de información que es almacenada en papel por lo que se haría bastante necesario establecer pautas de seguridad para la conservación de dicha documentación.

Finalidad

Lo que se busca a través de este punto de desarrollo es el de Prevenir e impedir accesos no autorizados, para que se efectuaran daños e interferencia en las sedes, instalaciones e información de la entidad.

En la parte de la información crítica lo que se busca es la protección de sus equipos los cuales se deben ubicar en zonas protegidas y que se encuentren resguardadas en un perímetro de seguridad que debe promover las diferentes medidas de seguridad y los controles de tipo apropiado para su manejo al igual que contemplar las medidas necesarias cuando estos necesiten ser trasladados o permanezcan fuera de las áreas que están destinadas para su protección y cuidado. Otro punto importante al que se deben generar controles es a los factores de tipo ambiental que podrían perjudicar el correcto funcionamiento de los equipos informáticos en los que se lleva a cabo el almacenamiento de la información de la institución esto antes de recurrir a la implementación de un control de seguridad física por lo cual es necesario realizar el levantamiento de información de la situación en la que se encuentra la institución respecto a su seguridad de tipo físico con el fin de determinar las vulnerabilidades y las soluciones que se deben originar.

Seguridad en las áreas

Perímetro de seguridad física

A través de la aplicación de los diferentes controles se busca ofrecer una adecuada protección con el fin de evitar un ataque de tipo destructivo, suministrando la protección física adecuada para cada uno de los activos de la institución. Con aplicación de los diferentes controles se busca ofrecer a los empleados los recursos necesarios en el manejo de la documentación o registro para que este sea de la manera correcta.

1. Colocar bajo llave la información más sensible.

2. Controles físicos de entrada a los diferentes activos para evitar el acceso no autorizado, mediante una protección física adecuada.

3. Seguridad de oficinas, despachos y recursos.

Seguridad en los equipos.

Las utilidades de apoyo se basaran en evitar la interrupción de los diferentes servicios que ofrecen los activos con la aplicación de estos controles.
En el Mantenimiento de equipos.

Este riesgo se minimiza a través de un mantenimiento de los equipos de la institución.

Mantener la seguridad de los equipos tanto dentro como fuera de la organización. Buscando el aseguramiento de que los equipos que se encuentre protegidos ante las posibles amenazas físicas y del ambiente.

5.1.10 Dominio gestión de comunicaciones y operaciones:

Los diferentes peligros existentes entre los cuales tenemos el software malicioso, virus, troyanos, etc. Es de suma importancia acoger controles para prevenir cualquier tipo de amenazas.

Se deben generar ambientes de pruebas y de operaciones, lo que se busca que los procedimientos den la garantía la calidad en los procesos a nivel operativo con la finalidad de evitar incidentes que se lleguen a generar por la manipulación de manera incorrecta de la información.

Las comunicaciones que se establecen para permitir el intercambio de la información se tienen que establecer a través de diferentes controles que permiten

ofrecer garantía a las condiciones de confidencialidad, integridad y disponibilidad de la información que es emitida o recibida a través de los diferentes canales de comunicación.

Finalidad

Se busca dar garantía al funcionamiento de manera correcta y segura a las instalaciones de procesamiento de la información y las comunicaciones con lo cual se desea establecer las diferentes responsabilidades y procedimientos que permitan su respectiva gestión y operatividad los cuales deben llegar a incluir las diferentes instrucciones de tipo operativo.

Para lo cual el administrador de la red al igual que el encargado a nivel legal de la institución además de los contratos y los diferentes acuerdos que son pactados por los terceros se hace necesario dar la certificación de que se encuentran incorporadas las consideraciones de manera relativa a la seguridad de la información que se encuentre involucrada en la gestión de los productos o servicios que se encuentran prestados.

Alcance

A través de la definición de una política de control de acceso que se aplica a los usuarios tanto a nivel interno como externo para se generen los diferentes permisos para acceder a los sistemas de información, red de la institución, además de las bases de datos.

De la misma manera se aplica al personal de tipo técnico la definición, instalación, administración al igual que el otorgamiento de los permisos de acceso, conexiones a la red y todos aquellos que administran su seguridad.

Los procedimientos y demás responsabilidades que se tiene durante la operación.
Documentación de los diferentes procedimientos de tipo operativo.

Se debe efectuar la documentación de los diferentes procedimientos de actualización con el fin de que no ocurra en una errónea actualización y por consiguiente no generar inconvenientes graves durante la prestación del servicio o al igual que su perdida, a través de la utilización de este control se puede reducir el riesgo ya que se documentaria únicamente los procedimientos de tipo operativo que son permitidos y necesarios durante la ejecución del sistema.

Control de cambios operacionales

Se debe generar la documentación adecuada de los procedimientos de actualización además de la pérdida del servicio.

Gestión de servicios externos.

Entrega del servicio

A través de este control lo que se busca llevar a cabo la reducción de las fallas en los acuerdos en los diferentes niveles de servicio con partes externas, donde la institución debe mantener un nivel en el que la seguridad y revisa la implementación de los diferentes acuerdos.

Llevar los controles necesarios de terceras partes a través de la revisión y monitorización de sus servicios.

Esto nos colabora con la reducción de los riesgos y fallos en los diferentes servicios que son entregados a las terceras partes teniendo una buena definición de los acuerdos y se toman en cuenta aspectos relacionados a la seguridad.
Planificar y aceptar el sistema
Planificación de la capacidad

A través de una planificación adecuada se evitara que el servicio se vea amenazado por delitos de tipo informático de extrema gravedad.
Aceptación del sistema

A través de una planificación adecuada se evitara que el servicio se vea amenazado por delitos de tipo informático de extrema gravedad.
Protección contra software malicioso.

El sistema debe contar con una protección contra el software malicioso.
Los controles que fueron elegidos nos permiten dar una probabilidad muy alta para que los problemas ocurran, pero se debe tener en cuenta que es posible que la presencia de un nuevo código malicioso genere un nuevo riesgo, lo que los controles se encargan de reducir la probabilidad de que este problema ocurra mediante la implementación de procedimientos que son lo mejor y más apropiado para la protección contra el sistema de software malicioso.

La Gestión de tipo interno para generar un respaldo.
La recuperación de la información

Por medio de este controla se busca llevar a cabo la reducción de cada uno de los riesgos con la ayuda de las políticas de respaldo y la restauración de manera oportuna

La gestión en la seguridad de la red

Controles a aplicar en la red

A través de la aplicación de cada uno de los controles se busca llevar al máximo la reducción del riesgo de no prestar el servicio con una adecuada gestión en la red, con el fin de mantener la confidencialidad de los datos, evitando el acceso no autorizado en la red, información y servicio.

Seguridad prestada en los servicios de Red.

Crear estos controles con la finalidad de sostener la confidencialidad de cada uno de los datos y de esta forma evitar el acceso de tipo no autorizado a la red, información y servicio.

Utilización de los medios de información.

Gestión de medios removibles

Con los controles se busca tener un procedimiento de manipulación de la información para protegerla del mal uso o divulgación no autorizada de la información.

Los procedimientos de la información con el establecimiento de los controles buscan un procedimiento de la manipulación de información para protegerla del mal uso o divulgación no autorizada.

Intercambio de la información

Mensajería electrónica
Se busca la minimización de la transmisión del sistema de software de tipo Malicioso a través del uso de comunicaciones electrónicas.

Con los controles se busca tener un aseguramiento de intercambio de información de tipo seguro.

Sistemas de información de tipo comerciales

Se trata de minimizar la transmisión de sistema de Software de tipo malicioso a través del uso de comunicaciones electrónicas.

Registro de auditoria

Se monitorización a través de una apropiada detención en su tiempo adecuado para brechas de seguridad que permiten reducir con este objetivo se ha implementado en la institución a través herramientas de administración de redes para realizar una adecuada monitorización y detectar a tiempo huecos de seguridad.

Registros generados por el administrador y el operador.

A través de la monitorización se puede generar la detención de brechas de seguridad y la reducción de impactos que pueden generar o causar las brechas de seguridad.

Registro de fallas

Se busca con la Monitorización realizar las detenciones a tiempo las brechas de seguridad y así reducirá los impactos que puede causar las brechas de seguridad

5.1.11 Dominio de control de acceso:

Requerimiento de negocios para control de acceso

Política de control de acceso

Se generan las políticas de seguridad de control de acceso que se necesita para permitir el ingreso para permitir el ingreso a las oficinas aso como el procedimiento para eliminar los permisos de personas que han salido de la empresa, si bien el riesgo no va a desaparecer el objetivo es disminuirlo.

Se llevan a cabo la realización de las políticas de seguridad de control de acceso que son necesarios para el ingreso a las oficinas así como el procedimiento para eliminar los permisos de las personas que no se encentran ya en la institución.

Las políticas de control de acceso buscan las responsabilidades y obligaciones de las personas que tienen el acceso a modificar información de las empresas y los controles necesarios para proteger información crítica.

Se hace necesaria la utilización de políticas de control para el acceso con el fin de justificar y dar a conocer las responsabilidades y obligaciones que tienen cada uno de los usuarios que posee las facultades necesarias para generar modificaciones a la información de la institución además de los controles que se deben utilizar de manera necesaria para dar protección a la información de tipo crítico, como el riesgo no va desaparecer nuestro fin si es ayudar con su disminución.

Gestión para el acceso de los usuarios

Registro de los usuarios

Se hace necesaria la utilización de un procedimiento en el cual generemos un registro de los usuarios tanto al ingreso como en la salida con el fin de dar una garantía para el acceso a los sistemas y servicios de información.

Gestión de los diferentes privilegios

Para realizar este control necesitamos un procedimiento a través del que se pueda llevar a cabo la revisión continua de los privilegios que nos permitan dar al usuario la garantía para el uso del acceso a los servicios de información al igual que realizar su respectiva revocación para de esta manera lograr la disminución de los cambios no autorizados en la información de tipo crítico.

Generar las revisiones de los derechos de acceso a cada uno de los usuarios.
Para lo cual se hace útil la creación de un control de acceso tanto para los datos como para los servicios de información, por lo cual se necesita efectuar una revisión de tipo periódica para los derechos de acceso a los usuarios.

Las responsabilidades de los usuarios.

El Uso de Contraseñas

Es útil para los usuarios la utilización de las contraseñas y estar informados sobre su uso al igual que sus responsabilidades y la manera en la cual se debe mantener la reserva para de esta forma conservar la reserva con el fin de evitar los accesos de información de tipo confidencial para las personas ajenas.

Los equipos de tipo informático de los usuarios desatendidos

Por lo cual es necesario y útil que cada uno de los usuarios adquiera los conocimientos para la protección de los equipos, con el fin de evitar el acceso de las terceras personas o pérdidas de la información, las políticas de limpieza de la pantalla y el escritorio es necesario establecer las políticas de la limpieza de escritorio para evitar papeles y unidades extraíbles que puedan contener la información que requiera la protección.
El Control de acceso a la red

Se debe generar una Política para los servicios de la red, se utiliza asegurar que el acceso de los usuarios de la red y cada uno de los servicios que no comprometan la seguridad de dichos servicios.

Se busca la Autenticación de cada uno de los usuarios para conexiones externas
Se necesario que asegurar el acceso de los usuarios a las redes y sus servicios que no comprometen a la seguridad de dichos servicios, se busca mantener un control sobre los sistemas críticos que almacenan información importante de la institución.
Se debe realizar la Autenticación de nodos de la red.

Se hace necesario tener la seguridad del acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios, una de las alternativas para evitar conexiones falsas es la autenticación de los nodos permitidos para la red.

Se busca la creación de la protección a puertos de diagnóstico remoto.
Se hace necesaria la utilización de un control sobre los puertos para que estos no puedan ser una puerta de entrada para la información no autorizada en la información de la institución, por lo cual se deben definir los puertos necesarios y bloquear los demás.

Control de conexión a las redes

La política de control de acceso para redes compartidas los cuales ejercen la restricción de las capacidades de conexión de los usuarios, con el fin de evitar la congestión dentro de los servicios por las peticiones de información de tipo falso, lo indispensable de mantener un monitoreo sobre la red para detectar las posibles brechas de seguridad y disminuirlas.

Se busca el Control de enrutamientos en la redes

La que se busca es que la conversión de cada una de las direcciones de la red lo cual es un mecanismo que de manera útil genera el aislamiento de las redes y evitar las rutas de propagación de problemas de seguridad en las redes.

El Control de acceso al sistema operativo

Identificación y autenticación del usuario

Lo que se busca a través de esto es que los usuarios puedan disponer de un identificador único que se debe utilizar de forma personal y exclusiva, lo que se puede posteriormente seguir la pista de las siguientes actividades de cada uno de los responsables en particular.
El Control de acceso a las diferentes aplicaciones

La Restricción de acceso a la información

Se debería generar el acceso a la información y las funciones del sistema de las aplicaciones de cada uno de los usuarios de este, además se encuentra incluido el apoyo, para generar un mejor control de cada una de las personas que tienen acceso para la auditoria.

5.1.12 Factibilidad de los controles de dominio adquisición, desarrollo y mantenimiento de sistemas de información:

A través de control debe revisar las aplicaciones en los puntos críticos de las vulnerabilidades, es básico para esto tener una adecuada infraestructura con una adecuada administración de la base, Sistemas Operativos y software de base, en las diferentes plataformas, para asegurar la correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Finalidad

A través de este control se puede promover el cubrimiento de varios puntos de la seguridad, entre los principales objetivos se tienen:

Definición de la documentación de las normas y procedimientos que se deben aplicar durante el ciclo de vida de los aplicativos en la infraestructura de base en la cual se apoya.

Se busca la definición de los métodos de protección de la información de tipo crítico o sensible.

Alcance

Los diferentes controles que se dan a conocer se aplican dentro de los sistemas informáticos al igual que los sistemas operativos que integran los ambientes por el organismo de donde residen los mismos.

Con el fin de efectuar un mejor control para la información de tipo confidencial o importante de los diferentes departamentos de la institución.

Podemos tomar como información confidencial a todo tipo de información que se refiera a los planes del negocio, la tecnología no anunciada, información financiera no pública; e información personal como son tarjetas de crédito, contraseñas.

La institución debe contar con un procedimiento de cambios aprobados por la gerencia y los diferentes cambios los cuales deben ser documentados además de comunicados a los empleados que se encuentren involucrados, en los resultados se llevan a la especificación el proceso en el que se efectúa un cambio.

Se efectúa la Revisión técnica de los cambios en el sistema operativo
Cada vez que sea necesaria la elaboración de un cambio en el Sistema Operativo, los sistemas deben ser revisados con el fin de asegurar que no se produzca impacto en su funcionamiento o seguridad.

El administrador de la red debe poseer un procedimiento en el cual se debe incluir:

- Se debe inspeccionar cada uno de los procedimientos dentro de la integridad y control de las aplicaciones para garantizar que no hayan sido comprometidas por el cambio.

- Se busca que se de garantía a los cambios que se van a efectuar dentro del sistema operativo deben ser informados con anterioridad a la ejecución. Por lo tanto el administrador debe efectuar la planificación de los días en los que se realizara el cambio para que este sea informado a los usuarios y de la misma forma coordinar con cada uno de los responsables del área en el caso de que la actualización o cambio necesite llevar a cabo la suspensión de las actividades por parte de los usuarios del área, como recomendación estos cambios deben programarse para fines de semana donde no haya impacto en los usuarios.

- Se debe llevar con seguridad el cumplimiento de la actualización del Plan de Continuidad de las Actividades de la institución.

Limitaciones que se realizan durante el cambio de paquetes de Software.

Se debe llevar a cabo el análisis si es necesario efectuar las modificaciones de paquetes en el software que son suministrados por los diferentes proveedores y que con previa autorización de cada uno de los responsables del área informática, por esto se debe:

Lo que se busca es que se lleve a cabo un Análisis de términos y las diferentes condiciones para que las licencias tienen como fin de buscar las determinaciones de las modificaciones que se encuentran las autorizaciones.

- Se busca realizar la determinación de la convivencia de que la modificación se lleve a cabo por la institución, por el tercero o proveedor encargada.
-
- La evaluación del impacto que se produce en la institución en la cual se hace cargo del mantenimiento.

- Se debe generar una copia de software original para sobre esta efectuar los cambios que se buscan identificar perfectamente, documentada de manera completa y detalla por si se hace rotundamente necesario la aplicación durante las nuevas versiones.

Para desarrollar este punto es necesario que se analice por los responsables de cada uno de las áreas y los administradores de la red, porque ellos son los que deben generar o aprobar el cambio cuando este implique varios procedimientos que impliquen la utilización de recursos a nivel legal, financiero, recursos, etc.

Canales encubiertos y código

A través de un canal oculto se puede exponer la información a que sea enviada a por medios de tipo indirecto y desconocido, debido a que los diferentes códigos maliciosos son los que se encuentran en la capacidad de afectar al sistema en forma no autorizada o no requerida por el usuario, por esto sería necesario que en cada una de las máquinas de los empleados de la institución se contara con un software de tipo adecuado, al igual que poseer las medidas que son necesarias como lo son el antivirus, por todas estas razones antes de la instalación del software dentro de la institución se debe analizar lo siguiente:

Los controles a realizar de tipo criptográficos

Las Política en el uso de los controles criptográficos.

Se debe efectuar el desarrollo de la política en la cual se especifique el uso de las medidas de tipo criptográfico que se deben tener en cuenta para la protección de la información.

Seguridad en los procesos de desarrollo y soporte

Procedimientos de control de cambios

Correspondería requerir los diferentes procedimientos de tipo formales de los controles de cambios con la finalidad de dar pruebas a la seguridad y los procedimientos de control que no se alteran con la finalidad de no ocasionar problemas en el funcionamiento de la aplicación.

La Revisión de tipo técnico de los cambios en el sistema operativo
Se efectúa la revisión y aprobación de las aplicaciones del sistema cuando estas sufran cambios para asegurar los impactos no sean de manera adversa dentro del funcionamiento y la seguridad.

Las Restricciones en los cambios a los paquetes de software

Se hace básica la utilización de los paquetes de software vendidos por los proveedores sin efectuar cambios a este en la medida en lo que sea posible con el fin de evitar que los servicios se efectúen y lleven en la manera correcta.

Canales encubiertos y código troyano

Se hace básica la utilización de los paquetes de software vendidos por los proveedores sin efectuar cambios a este en la medida en lo que sea posible con el fin de evitar que los servicios se efectúen y lleven en la manera correcta y las diferentes puertas sean aprovechadas por hackers o intrusos.

Gestión de vulnerabilidad técnica

Control de vulnerabilidades técnicas

Para esto se debe ofrecer la información de manera oportuna de las vulnerabilidades de tipo técnico dentro de los sistemas de información que se utilizan dentro de los sistemas de información contenidos dentro de la organización y la evaluación de las mismas. A fin de evitar brechas de seguridad que pueden ser fácilmente explotadas. Permitiendo el acceso a la red de intrusos.

5.1.13 Gestión de incidentes de seguridad de la información

La Divulgación de los eventos y las debilidades de la seguridad de la información

Divulgación de eventos de la seguridad de la información

Se hace necesaria la realización de los procedimientos de la divulgación de los diferentes acontecimientos de la seguridad de la información al igual que la respuesta generada al incidente y el procedimiento a escala con la finalidad de que los usuarios lleven a cabo las medidas correctivas necesarias.

Administración de incidentes y mejoras de la seguridad de la información

Responsabilidades y procedimientos

Es preciso definir las responsabilidades y los diferentes procedimientos que se deben establecer con el fin de dar una respuesta de manera rápida, eficaz y ordenada a los diferentes incidentes en la seguridad en la información.

5.1.14 Gestión de Continuidad del Negocio:

Lo más importante para la institución es la administración de forma adecuada y ordenada de las actividades necesarias dentro de la continuidad del negocio el procedimiento en el que se debe involucrar a todos los empleados de la institución.
El plan de continuidad debe generarse y al mismo tiempo se debe tener actualizado además de estar integrado en los diversos procesos dentro de cada uno de los departamentos de la institución.

Finalidad.

El control se realiza con la finalidad de cubrir en los puntos críticos de la institución esto basado para efectuarlo durante los casos de desastre, lo cual se basaría en los siguientes objetivos:

Realizar el análisis respectivo de las consecuencias que puede generar la interrupción del servicio y de esta manera tomar las medidas necesarias para las prevenciones de los casos que se puedan volver a repetir en el futuro.

Generar la propagación de la efectividad de cada una de las operaciones de contingencia de la institución con la finalidad de los establecimientos de planes que incluían las siguientes etapas:

- Realizar la detección y determinación del daño y activar el plan para su mejora.
-
- Efectuar la restauración de tipo temporal de las operaciones y la recuperación de dicho daño que se produjo al sistema original.
-
- Realizar la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.
-
- Asignar las funciones para las diferentes actividades que se encuentran definidas.

Alcance

Estos controles se deben aplicar en los puntos críticos de la institución.

Los diferentes aspectos de la gestión de continuidad del negocio.

Los proceso de gestión de la continuidad del negocio.

La consideración de la gestión de la continuidad del negocio tiene la necesidad de realizar controles que permitan la identificación y la reducción de los riesgos, limitar las consecuencias de incidencias que sean dañinas y tener de manera segura la reanudación de las operaciones en el menor tiempo posible.

El Desarrollo e implantación de los planes de contingencia

A través de este control se busca tener la seguridad de la disponibilidad de la información en niveles aceptables y de acuerdo al nivel crítico en el negocio cuando se presenta alguna falla pueda afectar los servicios.

5.1.15 Dominio de cumplimiento

Todos los controles que sean nombrados en los puntos que se trataron con anterioridad los cuales deben ser complementados a través de las regularidades y disposiciones a nivel legal y de contrato que se encuentran legalmente rigiendo en la actualidad en el estado colombiano. Se hace necesaria la definición en forma clara los requisitos normativos y contractuales pertinentes a cada sistema de información de la institución.

Finalidad

Los puntos más primordiales para tener en cuenta son:

El cumplimiento de las disposiciones de tipo normativo y contractual a fin de Cumplir con las disposiciones normativas y contractuales a fin de impedir las sanciones de tipo administrativo de la institución o de los empleados que incurran en la responsabilidad civil o penal como resultado de su incumplimiento.

Avalar que la política, normas y los procedimientos para la seguridad sean cumplidos por la institución.

Alcance

El control se debe aplicar a todo el personal de la institución.

Los Cumplimientos con los requisitos legales

Los Derechos de propiedad intelectual

Se deben realizar los procedimientos adecuados para dar el cumplimiento necesario al uso del material protegido como lo son los derechos de autor y los productos de software propietario.

Dar la conservación necesaria a los registros de la institución.

Es necesaria la protección de los registros de carácter importante para la institución que estos sean protegidos frente a la perdida, destrucción y falsificación, lo que se busca es tener guardada de forma segura los registros con

la finalidad de cumplir los requisitos legales o regulatorios el cual soporta las actividades que son esenciales dentro del negocio.

La Protección de los datos y de la privacidad de la información personal
Lo que se busca es basarse en las leyes para dar la protección necesaria a los datos personales para de esta forma evitar los problemas de tipo legal en los que pueden verse involucrados la institución.

Evitar el mal uso de los recursos de tratamiento de la información.

La capacitación a los usuarios es indispensable para que los usuarios tengan conciencia que el uso de los computadores con fines no autorizados pueden llegar a ser un delito penal.

Revisiones de la política de seguridad y de la conformidad técnica

Conformidad con la política de seguridad

Se hace necesario que los empleados de la institución como gerentes, jefes de las áreas y todos los altos cargos de la parte administrativa tienen que velar por que se estén cumpliendo de manera correcta los diferentes procedimientos de la seguridad dentro de su área de responsabilidad con el fin de evitar los problemas de tipo legal.

6 PLAN DE AUDITORIA INTERNA PARA APLICAR EN LA MEJORA CONTINUA

Con la finalidad de realizar la auditoria a nivel interno en cuanto a la seguridad de la información se ha generado el siguiente formato o lista de chequeo el cual verifica a los aspectos auditables basados los controles, procesos y procedimientos concordes a la familia de estándares ISO 27001 e ISO 27002.

Formato de gestión documental: A través de este formato se busca que el auditor pueda realizar la revisión de lo relacionado con la documentación del SGSI de la institución, con el fin de revisar y comprobar los objetivos de control, controles, procesos y procedimientos acordes a la familia de estándares ISO 27001 e ISO 27002. Ver anexo (1).

Formato de gestión revisión del sistema: Obtener a través de este formato se busca verificar que la entidad se encuentre realizando lo que expresa la norma la ISO 27001, Ver anexo (2).

Evaluación de registros, Ver anexo (3).

Formato de análisis de red: Este formato permite al auditor evaluar todo lo relacionado con la red LAN en la institución, como conocer las IP´s, los host y servidores, según la metodología OSSTMM. Ver anexo (4).

Análisis De Servidores: Este le permitirá al auditor revisar lo relacionado con los servidores y su función principal, según la metodología OSSTMM. Ver anexo (5).

7 CONCLUSIONES

El Sistema de Gestión de Seguridad se establece para cada una de las organizaciones con el fin de obtener los riesgos a los que se encuentran expuestos la información que se maneja en el sistema para establecer la forma estructurada, sistemática y metódica de cómo evitarlo.

En la seguridad informática es necesario realizar la definición de los roles que va tener cada uno de las personas que utilizan la acceso a la información, para así colocar las restricciones en cada uno de los usuarios de acuerdo a sus permiso y limitaciones.

Lo primero que se debe tener en cuenta para evitar los accesos de tipo no autorizado y los diferentes daños en el sistema es el generar las diferentes medidas de protección, además de dar a conocer la información necesaria para conocer lo que debe contener un área segura.

El SGSI no es necesario que abarque toda la organización sino se debe buscar que sea aplicado a los procesos principales de la organización donde se ubique la mayoría de las actividades que se encuentren relacionadas con la gestión de la información.

Tener clara la forma en la que se va actuar y responder ante un episodio de seguridad, por lo que se hace necesario que los diferentes empleados de la organización tengan claro cómo se debe actuar con la finalidad de minimizar la probabilidad de recurrencia del problema.

Dentro de las políticas de seguridad se deben tener en cuenta las políticas que se deben considerar para los medios de almacenamiento, determinando los procedimientos necesarios para la protección contra robo, daño o acceso no autorizado o para su destrucción o borrado total cuando no vayan a ser utilizados de nuevo.

Es fundamental dar un límite a los privilegios que se le van asignar a cada uno de los usuarios para su acceso con el fin de llevar a cabo un control de acceso esto con el fin de evitar controles de acceso estándar por esto se debe utilizar un identificador de usuario distinto al de uso habitual, Los privilegios tienen que revisarse de forma periódica para evitar la existencia de privilegios que ya no son necesarios.

8 RECOMENDACIONES

Lo que se debe llevar a cabo la identificación de los activos para de esta forma brindarles un grado de protección según su criticidad y así dar una adecuada protección.

Se deben efectuar análisis periódicos de los riesgos y que nos permitan analizar de forma periódica los riesgos para de esta manera poder verificar y monitorear continuamente la situación, se necesita proporcionar un SGSI permanente para generar un proceso continuo, mas no de acciones puntuales.

Se debe realizar la documentación de cada uno de los procedimientos operativos sin importar el tipo de cada uno de ellos, detallando para cada una de sus tareas para tener claro sus requerimientos tanto en la interdependencia de los otros sistemas, tareas de mantenimiento pronosticadas y procedimientos de recuperación ante incidentes.

Es necesario que el SGSI respete y cumpla las normas y leyes que se encuentren vigentes en el País como por ejemplo el derecho.

9 BIBLIOGRAFÍA

Caracterización, F. De. (n.d.). Índice de contenido, 1– recuperado de la página web: http://www.udistrital.edu.co:8080/documents/276352/356568/Cap5GestionRiesgo.pdf

Gestión de Riesgo en la Seguridad Informática recuperado de la página web: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

Guía de procedimientos, autor C-TPAT Análisis de Riesgos en 5 Pasos. (n.d.). http://www.dian.gov.co/descargas/operador/documentos/2015/Analisis_de_Riesgo_En_5_Pasos.pdf

Libro I - Método., autor Amutio, M. A., Candau, J., & Mañas, J. A. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministerio de Hacienda y Administraciones Públicas.

Post o artículo generado dentro de un foro, autor Héctor Acevedo Juárez, ISO-27001: ¿Qué es y para qué sirve? (parte 1) CISSP, CISA, CGEIT, ITIL y MCSE • 08/11/2011 disponible en: http://www.magazcitum.com.mx/?p=1574

Post o artículo generado dentro del foro INGTUX, Ingeniero en Computación de la UNAM, especialista en seguridad informática, administración y seguridad de servidores GNU/Linux y pruebas de penetración o hacking ético, linuxero de corazón. @tuxcomp en twitter, ¿Qué es la Seguridad Informática? De fecha 28 de noviembre de 2011. Disponible en http://g3ekarmy.com/%C2%BFque-es-la-seguridad-informatica/

Post o artículo generado dentro del foro, autor anónimo, Seguridad informática disponible en: http://auditoriadesistemas.galeon.com/productos2227783.html.

Post o artículo generado dentro del foro, autor KOSUTIC Dejan 27001 academy Que es la norma 27001 disponible en: http://www.iso27001standard.com/es/que-es-la-norma-iso-27001.

Que es intranet, mis respuestas punto.com block disponible en: http://www.misrespuestas.com/que-es-intranet.html.

Riesgo vs. Seguridad de la información. (n.d.), 1–7.recuperada de la página web:http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf

Trabajo de grado. Monografía o tesis JEREZ, Carlos Augusto. Seguridad para lograr Confiabilidad y Calidad de los Servicios Digitales en Internet. Tesis profesional Cholula, Puebla, México a 6 de mayo de 2004, Capítulo 1 de seguridad informática conceptos básicos disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo_1.html o http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf

Trabajo escrito o monografía COITE Angélica, ROMERO Hugo Auditoría de Sistema y políticas de Seguridad Informática, Auditoria informática (AUD). Políticas de seguridad informática (SEG). Privacidad en la red y control de intrusos (PRIV). Detección de intrusos. Virus y antivirus (v/a). Seguridad. Disponible en: http://www.monografias.com/trabajos12/fichagr/fichagr.shtml#POLIT publicado el día lunes 10 de febrero de 2003.

Universidad Nacional Abierta y a distancia UNAD. Guía de implementación del SGSI recuperada de la página web: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/61_leccin_26_auditoras_internas_del_sgsi.html.

10 ANEXOS

ANEXO 1. FORMATO DE GESTIÓN DOCUMENTAL

ORGANIZACIÓN		FECHA		REVISADO POR	
EMPRESA					
VERSIÓN		ESTÁNDAR APLICADO		ISO 27001	
DESCRIPCIÓN DE LA AUDITORIA				Revisión preliminar de controles para el procedimiento de Auditoría Externa del SGSI	
DOCUMENTOS DEL SGSI		CUMPLIMIENTO			OBSERVACIONES
		SI	NO	NA	
¿En la institución existe una política de seguridad con un enfoque estratégico de riesgos y controles informáticos?					
¿La revisión y aprobación del documento de la política del SGSI fue aprobado por la alta dirección?					
¿Existe documentación del SGSI es de tipo formal que incluya las políticas, objetivos de control, procedimientos y lineamientos?					
¿La política de seguridad para los usuarios de los empleados de la institución?					
¿Es formal la definición del alcance del SGSI?					
¿La institución posee un documento que evalúe los riegos informáticos que los a los que se encuentra expuesto el sistema de información?					
¿Existe un documento en el que se establezcan los controles informáticos o plan de tratamiento ante los posibles riesgos a los que se está expuesto?					
¿Hay un documento donde se ve reflejada el compromiso de la alta dirección con la seguridad de la información?					

ANEXO 2 FORMATO DE GESTIÓN REVISIÓN DEL SISTEMA

DOCUMENTOS DEL SGSI	CUMPLIMIENTO			OBSERVACIONES
	SI	NO	NA	
POLÍTICA DE SEGURIDAD				
Documento de la política de seguridad de la información				
Revisión de la política de seguridad de la información				
ORGANIZACIÓN DE LA SEGURIDAD DE INFORMACIÓN				
Comité de gestión de seguridad de información				
Responsabilidades y roles de la seguridad de información				
Autorización de recursos para el tratamiento de la información				
Acuerdos de confidencialidad				
Contacto con autoridades				
Tratamiento de la seguridad en relación con clientes				
Tratamiento de seguridad en contrato con terceros				
GESTIÓN DE ACTIVOS DE INFORMACIÓN				
Inventario de activos				
Responsabilidades y responsables sobre los activos				
Acuerdos sobre el uso responsable sobre activos				
RECURSOS HUMANOS				
Inclusión de la seguridad en las responsabilidades laborales				
Selección de personal				
Términos y condiciones de la relación laboral				
Asignación de permisos y privilegios				
Cancelación de permisos de acceso cuando finaliza o cambia el puesto de trabajo				
SEGURIDAD FÍSICA Y DEL ENTORNO				
Áreas seguras				
Perímetro de seguridad física				
Controles de acceso a áreas restringidas				
Seguridad en oficinas, despachos, recursos				
Protección contra amenazas externas y del entorno				
Trabajo en áreas seguras				
Seguridad en equipos				
Instalación y protección de equipos				
Suministro eléctrico				
Seguridad del cableado				
Seguridad en equipos fuera de las instalaciones de la empresa				
Seguridad en la reutilización o eliminación de equipos.				
Traslado de activos				
GESTIÓN DE COMUNICACIONES				
Documentación de procesos operativos				
Control de cambios operacionales				
Segregación de tareas				
Separación de los recursos para desarrollo y producción				
Planificación y aceptación del sistema				

Planificación de capacidades.				
Aceptación del sistema.				
Medidas y controles contra software malicioso.				
Medidas y controles contra código móvil.				
Gestión interna de soportes y recuperación				
Recuperación de información				
Gestión de redes				
Controles de red				
Seguridad en los servicios de red				
Utilización y seguridad de los soportes de información.				
Gestión de soportes extraíbles.				
Eliminación de soportes				
Procedimientos para la utilización de la información				
Intercambio de información y software				
Políticas de acceso e intercambio de información				
Acuerdos de intercambio con terceros – convenio				
Soportes físicos				
Correo electrónico				
Seguridad en comercio electrónico				
Seguridad en transacciones en línea				
Registro de incidencias				
Protección de los registros de incidencias				
CONTROL DE ACCESO				
Política de control de acceso				
Gestión de accesos de usuario				
Registro de usuarios				
Gestión de privilegios				
Gestión de contraseñas de usuario				
Revisión de los derechos de acceso de los usuarios				
responsabilidades del usuario				
Uso de contraseñas				
Equipo informático de usuario desatendido				
Políticas para CPU y monitores sin uso				
Control de acceso en red				
Política de uso de servicios de red				
Autenticación de usuario para conexiones externas				
Autenticación de nodos de la red				
Protección a puertos de diagnóstico remoto				
Control de conexión a redes				
Control de encaminamiento de red				
Control de acceso a sistemas operativos				
Autenticación del usuario				
Gestión de contraseñas				
Uso de servicios del sistema				
Desconexión automática de terminales				
Control de acceso a aplicaciones				
Restricción en el acceso a la información				
Aislamiento de aplicaciones sensibles				
SISTEMAS DE INFORMACIÓN				
Seguridad en aplicaciones del sistema				
Validación de datos de entrada				
Control de acceso interno				
Autenticación de mensajes				
Validación de datos de salida				
Controles criptográficos.				
Política de uso de los controles criptográficos.				

Cifrado				
Seguridad de archivos del sistema				
Control de software en explotación				
Protección de los datos de prueba del sistema				
Control de acceso a librerías y código fuente de programas				
Seguridad en los procesos de desarrollo y soporte				
Procedimientos de control de cambios.				
Canales encubiertos y código troyano				
Gestión de vulnerabilidades técnicas				
Control de las vulnerabilidades técnicas.				
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN				
Comunicación de eventos y debilidades en la seguridad				
Gestión de incidentes y mejoras en la seguridad				
Identificación de responsabilidades y procedimientos				
Evaluación de incidentes en seguridad.				
Recogida de pruebas.				

ANEXO 3 EVALUACIÓN DE REGISTROS

DOCUMENTOS DEL SGSI	CUMPLIMIENTO			OBSERVACIONES
	SI	NO	NA	
Registros de capacitaciones, habilidades, experiencias				
Resultados de auditorias				
Revisión de actas por parte de dirección				
Acciones correctivas				
Registro Capacitaciones en la política de seguridad informática				
Registro sobre actividades de usuarios, excepciones y eventos de seguridad				

ANEXO 4 FORMATO DE ANÁLISIS DE RED

ORGANIZACIÓN		FECHA		REVISADO POR	
EMPRESA					
VERSIÓN		ESTÁNDAR APLICADO		ISO 27001	
DESCRIPCIÓN DE LA AUDITORIA				Revisión preliminar de controles para el procedimiento de Auditoría Externa del SGSI	

Elementos	CARACTERÍSTICA	DETALLE
Rangos de IP a testear y detalle de rangos		
Información de dominios y su configuración		

Servidores	IP	Sistema Operativo

ANEXO 5 ANÁLISIS DE SERVIDORES

ORGANIZACIÓN		FECHA		REVISADO POR	
EMPRESA					
VERSIÓN		ESTÁNDAR APLICADO		ISO 27001	
DESCRIPCIÓN DE LA AUDITORIA				Revisión preliminar de controles para el procedimiento de Auditoría Externa del SGSI	

NOMBRE DEL SERVIDOR	
DIRECCIÓN IP	
FUNCIÓN	
DOMINIO	

PUERTO	PROTOCOLO	SERVICIO	DETALLES DEL SERVICIO

SECUENCIAS TCP
PREDICCIÓN DE SECUENCIA TCP: _____
NÚMEROS DE SECUENCIA ISN TCP: _____
TIEMPO OPERACIONAL: _____
VULNERABILIDADES DETECTADAS:

VULNERABILIDAD	EJEMPLO	SOLUCIÓN