ANALISIS PARA LA IMPLEMENTACION DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION SEGÚN LA NORMA ISO 27001 EN LA EMPRESA SERVIDOC S.A.

ING. LUIS ENRIQUE GIRALDO CEPEDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI, VALLE DEL CAUCA
2016

ANALISIS PARA LA IMPLEMENTACION DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION SEGÚN LA NORMA ISO 27001 EN LA EMPRESA SERVIDOC S.A.

ING. LUIS ENRIQUE GIRALDO CEPEDA

PROYECTO TRABAJO DE GRADO

Directora: YINA ALEXANDRA GONZÁLEZ SANABRIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI, VALLE DEL CAUCA
2016

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Santiago de Cali, marzo de 2016

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

Las Tecnologías de la Información y la Comunicación TIC han llevado a las organizaciones a estar a la vanguardia con los adelantos tecnológicos, la información se convierte entonces en un recurso primordial para lograr ser competitivos, esta es la razón por la cual debe ser protegida de diferentes formas, con el uso de las nuevas tecnologías, las compañías se han vuelto más vulnerables ante ataques informáticos.

Para proteger la información es necesario confeccionar un estudio muy detallado que permita identificar los riesgos a los que se encuentra expuesta la empresa, de esta forma se puede establecer cuál es la forma correcta de implementar medidas para contrarrestar esta deficiencia y salvaguardar los activos, una forma eficaz para realizar estos procesos es un análisis para la implementación de un Sistema de Gestión de Seguridad Informática y esto es exactamente lo que aborda este trabajo de grado, un análisis concienzudo de todas las vulnerabilidades a las que está expuesta la empresa Servidoc S.A. en temas relacionados con seguridad informática.

El análisis se realizó por medio de fases, donde se incluyeron entrevistas, observación directa y la aplicación de la metodología de análisis de riesgos Magerit entre otras, esta metodología permitió realizar un análisis para la implementación de un SGSI que permita identificar amenazas, vulnerabilidades y riesgos que pueden afectar la organización específicamente en las áreas de contabilidad, facturación e Historias clínicas, el resultado final permitió la identificación de los riesgos y la forma de mitigar esos riesgos, para ello se hicieron recomendaciones y se sugirieron proyectos que la empresa debe implementar para cubrir estas debilidades, adicionalmente se logró identificar el nivel en el que se encuentra la organización en cuanto a seguridad informática y el resultado fue muy negativo, puesto que falta mucho por hacer para proteger los activos de la empresa.

Abstract

Technologies of Information and Communication ICT have led organizations to be at the forefront with technological advances, information then becomes a key to be competitive resource, this is the reason why it must be protected from different However, with the use of new technologies, companies have become more vulnerable to attacks.

To protect information is necessary to make a detailed study to identify the risks to the company, this way is exposed can be established what is the proper way to implement measures to address this deficiency and to safeguard assets, a form effective for these processes is an analysis for the implementation of a

Management System Computer Security and this is exactly what addresses this degree work, a thorough analysis of all vulnerabilities to which the company is exposed Servidoc SA, on issues related to computer security.

The analysis was performed through phases where interviews, direct observation and application of the methodology of risk analysis Magerit among others were included, this methodology allowed an analysis for the implementation of an ISMS to identify threats, vulnerabilities and risks to which is exposed the organization specifically in the areas of accounting, billing and medical records, the end result allowed the identification of risks and how to mitigate those risks, for that recommendations were made and projects suggested that the company should implemented to cover these weaknesses, additionally it was possible to identify the level at which the organization in terms of security and the result was very negative, since much remains to be done to protect the assets of the company is

1. DEFINICION DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Actualmente la empresa Servidoc S.A. no posee ningún método o control que le permita identificar vulnerabilidades, riesgos y ataques a los que puede ser sometida, no existe documentación que evidencia procedimientos que puedan ayudar a solventar estas deficiencias poniendo en riesgo los activos de la organización.

1.2 FORMULACION DEL PROBLEMA

¿Cuenta la empresa Servidoc S.A. con un plan que ayude a realizar un análisis para implementar un Sistema de Gestión de Seguridad de la Información que proporcione la identificación y gestión del riesgo?

1.3 DESCRIPCION DEL PROBLEMA

La empresa Servidoc S.A. desea tener una propuesta que permita gestionar el riesgo al que se encuentra expuesta, contando con un modelo de Gestión de Seguridad de la Información que permita identificar y mitigar el riesgo.

Esta propuesta será de gran importancia para la organización, teniendo en cuenta que la organización no ha definido políticas que tengan que ver con seguridad informática, otro aspecto inexistente es la asignación de responsabilidades en materia de seguridad, no se cuenta con procedimientos en materia de seguridad física y desastres de origen natural que afecten los activos de la empresa, entre los problemas más graves se encuentra el uso inadecuado de los recursos tecnológicos, falta de control en navegación y uso de correo electrónico.

1.4 JUSTIFICACION

Las constantes reformas a la salud que día a día realiza el Gobierno Nacional obligan a las Instituciones Prestadoras de Salud (IPS) a que se preocupen más por invertir en tecnologías que apoyen la prestación del servicio, esto representa un incremento en la administración del recurso tecnológico, redes, almacenamiento, acceso a la información, etc., todo esto se traduce en que

la seguridad de la información sea un poco más compleja de administrar por parte del personal encargado.

La Empresa Servidoc S.A ubicada en la ciudad de Cali, es una empresa dedicada a la prestación de servicios de salud. Cuenta con tres sedes y 70 computadores distribuidos en sus diferentes oficinas, la conexión a internet de los puestos de trabajo es permanente, cada una de las sedes se conecta de manera independiente.

Para la Compañía, la información que se maneja en los equipos de cómputo es muy valiosa por cuanto ahí reposa información de historias clínicas, información contable entre otras que por ley Servidoc S.A, debe resguardar y proteger. Esta es la razón por la cual se ha decidido que el proyecto determine y garantice que se cumplan las premisas de la seguridad informática que son confidencialidad, integridad y disponibilidad.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Realizar un análisis para la Implementación de un Sistema de Gestión de Seguridad de la información ISO-27001 en la compañía Servidoc S.A, con el fin de identificar y proponer soluciones de seguridad informática a las estaciones de trabajo que son críticas para la prestación de servicios específicamente en las áreas de contabilidad, facturación e historias clínicas de la empresa.

2.2 OBJETIVOS ESPECÍFICOS

- Identificar fortalezas y debilidades que tiene la empresa Servidoc S.A. en las áreas de facturación, contabilidad e historias clínicas en cuanto a seguridad informática se refiere.
- Evaluar los riesgos de seguridad en la información de Servidoc S.A y conocer las medidas que los pueden contrarrestar.
- Identificar las vulnerabilidades que posee la empresa.
- Crear y entregar un documento con políticas de seguridad de la información y asignación de responsabilidades al personal.

3. MARCO REFERENCIAL

3.1 **ESTADO DEL ARTE**

FERNÁNDEZ, Raúl José Gil (2.011) en la ciudad de Barquisimeto (Venezuela), desarrolló un trabajo de grado con el nombre de "**sistematización de la gestión de riesgos de La seguridad de la información en la red de la universidad Centroccidental Lisandro Alvarado".**

El desarrollo de la investigación se centró en diseñar un sistema de gestión de riesgos de la seguridad de la información específicamente en la red de la universidad "Lisandro Alvarado", tomando como referencia el estándar internacional ISO/IEC 27001:2005. Esta investigación concluyó que la Universidad cuenta con controles de seguridad informática que cubren de forma parcial aspectos de seguridad, razón por la cual es necesario implementar la norma ISO/IEC 27001:2005 con el fin de reducir las vulnerabilidades y amenazas que afectan a la organización.

Lo expuesto anteriormente se relaciona directamente con la presente investigación, puesto que el autor utiliza la norma ISO/IEC 27001:2005 como apoyo para el análisis y gestión de riesgos de la información.

En el año 2013 NIETO, Juan Pablo en la ciudad de Barcelona (España), realizo una investigación llamada "**Plan de implementación de la ISO/IEC 27001:2005"** para optar al título de Master Interuniversitario en la Seguridad de las TIC, dentro de esta implementación de la norma ISO/IEC27001:2005, se contempla el estado de madurez, análisis y definición de riesgos.

Las conclusiones generadas arrojaron como resultado que las amenazas y riesgos más representativos se encuentran en el factor humano, mostrando un resultado del 73%, además se hallan amenazas relacionadas con la infraestructura de la empresa y errores de programación; para reducir estas amenazas y riesgos, el autor sugiere unas salvaguardas para mitigar estos riesgos, adicionalmente presenta una serie de proyectos que permitirán reducir el riesgo a su nivel mínimo.

La exploración realizada por el autor, aporta mucho al desarrollo del presente trabajo, puesto que despliega la investigación apoyada de la norma ISO/IEC 27001:2005 y se utiliza MAGERIT como metodología de análisis de riesgo.

MATALOBOS VEIGA, Juan Manuel en el año 2009 en la ciudad de Madrid (España), realizo una investigación llamada "**Análisis de Riesgos de la**

Seguridad de la Información", el desarrollo de esta se basa en un análisis de riesgos de la organización, definiendo los controles que se deben implementar en la organización; se utilizaron diferentes metodologías de análisis de riesgo, en la cual el autor concluye que una vez identificados los activos de la empresa que presentan falencias en cuanto a seguridad informática, es posible definir controles de forma apropiada para mitigar el riesgo de una forma oportuna.

El aporte es de gran relevancia, ya que aborda diferentes metodologías de análisis de riesgo, además se apoya en la norma ISO/IEC 27001:2005.

En la ciudad de Machala (Ecuador), VÁSQUES, Karina del Rocío en el año 2013 realizo una investigación llamada "**Aplicación de la Metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicada a la empresa pesquera e industrial Bravito S.A.",** el trabajo consiste en la realización de un análisis de riesgos para definir un ambiente seguro de la información de la organización, estableciendo mecanismos de protección para los riegos encontrados en los diferentes activos.

El autor concluye que la situación en cuanto a seguridad informática de la empresa Pesquera e Industrial Bravito S.A. es preocupante, pues nunca se habían realizado estudios y la empresa se encuentra muy vulnerable, al realizar el análisis de la situación actual, se encontraron muchas falencias, para lo cual se definen unas serie de salvaguardas para reducir el riesgo.

Lo anterior aporta mucho al desarrollo del presente trabajo, puesto que desarrolla la investigación apoyada de la metodología de análisis de riesgos MAGERIT.

PEREIRA, Hose Aurela, en el año 2013 en la ciudad de Barcelona (España), realizo una investigación llamada "**Plan de implementación de la ISO/IEC 27001:2005"** para optar al título de Master Interuniversitario en la Seguridad de las Tecnologías de la información y las comunicaciones, la investigación tiene como finalidad establecer un estado de madurez de la organización en cuanto a seguridad informática, además realizar un análisis de riesgo para determinar los controles y salvaguardas que se deben aplicar.

Con la realización del trabajo presentado por el autor, se logró establecer un plan de trabajo para la implementación de la norma ISO/IEC 27001:2005, se realizó un estudio del estado actual de la organización en el cumplimiento de la norma, mostrando que aunque existen controles en la organización, faltan muchos controles por implementar, además se definen algunas salvaguardas y se sugieren proyectos que se deben implementar para reducir el riesgo.

La investigación realizada por el autor, aporta mucho al desarrollo del presente trabajo, si se tiene en cuenta que desarrolla la investigación apoyada de la norma ISO/IEC 27001:2005 y se utiliza MAGERIT como metodología de análisis de riesgo.
En el 2009 BUENAÑO QUINTA, José Luis; GRANADA LUCES, Marcelo Alfonso, en la ciudad de Guayaquil (Ecuador), elaboraron una investigación titulada "**Planeación y Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 – 27002",** en este proyecto se realiza un análisis de riesgos de la Universidad Politécnica Salesiana sede Guayaquil, el análisis se enfoca en los riesgos que afectan la prestación del servicio y la continuidad de las operaciones.

Los autores concluyeron que a raíz del crecimiento tecnológico que ha tenido la universidad, se ha vuelto muy vulnerable a ataques informáticos, la intención con este análisis es reducir el riesgo, para ello se ha definido la implementación de controles principalmente en la parte de infraestructura y documentación.

Este trabajo representa un aporte teórico significativo para la presente investigación, puesto que se utiliza la metodología de análisis de riesgo MAGERIT y la aplicación de la norma ISO/IEC 27001 – 27002.

CUCHIMBA, PERAFÁN RUIZ, John Jairo; CAICEDO, Mildred en la ciudad de Popayán (Colombia), desarrollo una investigación titulada "**Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca",** la finalidad de esta investigación es realizar un análisis de riesgos detallado con el propósito de realizar la implementación del sistema de Gestión Seguridad de la Información de la IUCMC.

Los autores concluyen que la universidad presenta muchos problemas de seguridad, estos problemas identificados pueden ser solucionados implementado un SGSI, el cual permitirá reducir el riesgo en que se encuentra la universidad actualmente a un nivel más bajo, además optimizar los procesos para que se cumplan los objetivos de la organización. Esta investigación representa un gran aporte teórico al presente trabajo ya que utiliza MAGERIT como metodología de análisis de riesgo.

En la ciudad de Montevideo (Uruguay), MEGA, Gustavo Pallas en el año 2009 realizó una investigación para optar al título de Maestría en Ingeniería de Computación, con el nombre de "**Metodología de Implantación de un SGSI en un grupo empresarial jerárquico",** esta investigación abarca la implementación de un SGSI con un enfoque mixto para un grupo empresarial, lo que pretende el autor es que la dirección sea centralizada, pero las operaciones se realizan de forma local, es decir en cada una de las empresas que conforma el grupo empresarial. El autor concluye que el enfoque mixto

permitirá unificar criterios y optimizar recursos cuando los riesgos deban afrontarse en forma conjunta.

PEREZ PÉREZ ,Yesica María; OSORIO RIVERO, Yenis Pineda en la ciudad de Ocaña, desarrollaron una investigación para optar al título de Especialistas en Auditoría Informática con el título "**Diseño de una Política de Gestión de Riesgo de la Información para la dependencia de Admisiones Registro y control de la Universidad Francisco de Paula Santander Ocaña",** esta investigación se centra en la identificación y valoración de riesgos de la Universidad, con el fin de implementar una política que permita reducir los riesgos en la oficina de admisiones y registro de dicha universidad.

Los autores concluyen que con el análisis realizado y la implementación de la política de riesgos se cree conciencia para que los encargados de los procesos reconozcan los riesgos a que se enfrentan y tomen decisiones en busca de los objetivos planteados por la organización. La metodología utilizada para el análisis de riesgos fue MAGERIT, lo que sirve de apoyo teórico al presente trabajo.

SALCEDO, Robin J. en la ciudad de Barcelona, desarrolló una investigación con el nombre de **"plan de implementación del SGSI basado en la norma ISO/IEC 27001:2013"**. La investigación se centra en la implementación de un SGSI en la empresa ISAGXXX para solucionar problemas de seguridad en los servicios de información con la finalidad de llevar el riesgo a un nivel tolerable. El autor concluye que el apoyo de la gerencia es vital para el desarrollo de proyecto y que se deben realizar auditorías periódicamente, por otro lado es necesario aumentar el presupuesto para la implementación de estrategias de seguridad informática en la organización.

El aporte teórico de esta investigación al desarrollo del presente trabajo, es el apoyo que el autor hace de la norma ISO/IEC 27001:2013.

3.2 **MARCO TEÓRICO**

Magerit: Metodología de análisis y gestión de riesgos, su iniciativa se centra particularmente en que todas las organizaciones dependen directamente del uso de las tecnologías de la información para su rápido y correcto crecimiento, pero esto genera algunos riesgos que se deben llevar a un nivel bajo, para ello Magerit proporciona procedimientos de medición que permite saber el valor de los activos, identificar de forma detallada el riesgo al que se encuentran expuestos y la forma de mitigar este riesgo.

Esta metodología cuenta con tres libros donde se documenta de forma detallada la forma de analizar y gestionar el riesgo de los sistemas de información de las organizaciones.

Sistema de Información: Dice ALARCÓN, Vicenç Fernández (2.006) que es un conjunto de componentes que interaccionan entre sí para lograr un objetivo común, satisfacer las necesidades de información de una organización, la mayoría están conformados por cinco componentes básicos: elementos de entrada, elementos de salida, sección de transformación, mecanismos de control y objetivos.

Según OZ, Effy en una organización un sistema de información está compuesto por hardware, software, personas y procedimientos, todos interconectados entre sí para producir excelentes resultados.
Sistema de gestión de la seguridad de la información SGSI: Un sistema de gestión, en general abarca una estructura, unos recursos, unos procesos y unos procedimientos que tienden a poner en práctica los objetivos y las políticas de una organización.

AREITIO BERTOLÍN, Javier [1] dice que un buen SGSI puede verse como un ciclo cerrado, que comienza con la prevención de amenazas, la reducción de las mismas, la detección de incidentes y la contención de los mismos. Los daños ocasionados se corrigen y se pasa a la recuperación, seguida de la evaluación de nuevo y se vuelve al comienzo con la prevención de amenazas.

La implantación de un SGSI, ayuda a establecer la forma más adecuada de tratar los aspectos de seguridad, mediante la conjugación de los recursos humanos y técnicos, respaldados por medios administrativos, que garanticen la instauración de controles efectivos para lograr el nivel de seguridad necesario, en correspondencia con los objetivos de la organización, de tal forma que se mantenga el riesgo por debajo del nivel asumible por la organización.

El SGSI, proporciona a los directivos una herramienta que ofrece una visión global, sobre el estado de sus sistemas informáticos.

Seguridad de la información
Son las medidas que toda organización debe adoptar con el fin de proteger la información, cumpliendo con los objetivos de la seguridad informática como son la disponibilidad, confidencialidad e integridad.

---

[1] AREITIO BERTOLÍN, Javier. Seguridad de la Información – Redes, informática y sistemas de información. Disponible en: https://books.google.com.co/books?id=_z2GcBD3deYC&pg=PA201&dq=sistema+gestion+seguridad+informatica&hl=es&sa[1] GOBIERNO DE ESPAÑA. Familia de Normas ISO 27000. Disponible en: =X&ei=3gNcVd_wKYOpNvbigUg&ved=0CCQQ6wEwAA#v=onepage&q=sistema%20gestion%20seguridad%20informatica&f=false

Estándares de Gestión de Seguridad
Según GOBIERNO DE ESPAÑA las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrónica Internacional (IEC) que proporcionan un marco para la gestión de la seguridad de la información.

- **Norma ISO/IEC 27001**

Es un estándar para la seguridad de la información, y fomenta la importancia de entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información, implementar y operar controles para manejar los riesgos de la seguridad de la información, monitorear y revisar el desempeño y la efectividad de SGSI y mejoramiento continuo en base a la medición de los objetivos.[2]

- **Norma ISO/IEC 27002**

Código de buenas prácticas para la gestión de la seguridad de la información, esta norma recomienda las medidas que se deben implementar para asegurar los sistemas de información de las organizaciones.

Esta norma contiene 39 objetivos de control y 133 controles, todos estos agrupados en 11 dominios.

- **Norma ISO/IEC 27003**

Proporciona métricas para la gestión de la seguridad de la información, da las directrices para la implementación de un SGSI, esta norma sirve de soporte a la ISO/IEC 27001.

En esta norma se describe de forma detalla todos los procesos hasta la puesta en marcha, además muestra el proceso de cómo se logra la aprobación por parte de la dirección para la implementación de un Sistema de Gestión de Seguridad de la Información.

Kali Linux
Es un programa Linux de libre distribución, su función principal es realizar tareas de auditoria en temas relacionados con seguridad informática, esta distribución contiene gran cantidad de herramientas entre las que se incluyen: escaneo de puertos, pruebas de seguridad de redes inalámbricas, herramientas para averiguar contraseñas entre muchas otras.

[2] Aguilera López., Purificación., Seguridad Informática. Disponible en: books.google.com. Obtenido de https://books.google.com.co/books?id=Mgvm3AYIT64C&pg=PA9&dq=concepto+seguridad+informatica&hl=es&sa=X&ei=jf9bVcWxMYW1sAS9z4CQDg&ved=0CC0Q6AEwAA#v=onepage&q=concepto%20seguridad%20informatica&f=true

El programa es de fácil instalación, además viene en versiones para 32 bits y 64 bits.

Nmap

Es una potente herramienta de código abierto que permite escanear puertos de grandes redes, es ideal para el desarrollo de labores de auditoría, permite identificar que equipos se encuentran accediendo una red, además es posible identificar los servicios que están utilizando, indicando el sistema operativo y su respectiva versión, es una herramienta ideal en labores de monitorización de redes.

Ethical hacking

El avance de las Tecnologías de la información y la comunicación ha generado muchos beneficios para la humanidad, de igual forma con este crecimiento, los equipos cada vez se vuelven más vulnerables ante ataques por parte de piratas informáticos que buscan atacar los sistemas y comprometer la información de las organizaciones, para contrarrestar estos ataques, nace el Ethical Hacking, su función principal es monitorear y explorar las vulnerabilidades a los que son susceptibles los sistemas, evaluando tanto la parte física como lógica de los sistemas, intentando encontrar esas vulnerabilidades para que puedan ser corregidas a tiempo y así evitar ataques que puedan comprometer la seguridad.

En algunas ocasiones se les conoce como hackers de sombrero blanco, inspirados en las películas del oeste, donde el bueno portaba el sombrero blanco y los malos el sombrero negro.

Las pruebas de penetración que realizan los Ethical hacking permiten evaluar vulnerabilidades, clasificar las debilidades y finalmente realizar recomendaciones, priorizando las necesidades de las empresas.

Wireshark

Herramienta Linux de libre distribución encargada de analizar protocolos en una red, es posible analizar una red y las aplicaciones que viajan por ella, wireshark tiene la capacidad de analizar más de 480 protocolos entre los que se encuentran TCP, DNS, ICMP, HTTP.

Esta aplicación se encuentra disponible en versiones Windows y Linux, permite realizar filtros del escaneo realizado, es fácil de usar y permite una interfaz gráfica.

Dnsenum
Esta herramienta permite recopilar información de dominios, es de libre distribución, dentro de los datos que obtiene Dnsenum se pueden encontrar el nombre del servidor, la dirección del host, muestra subdominios y cuentas de correo, muestra el registro MX, datos importantes que serán de gran ayuda en el momento de realizar una penetración al sistema.

TheHarvester
Esta herramienta Linux de libre distribución consigue datos de puertos abiertos, subdominios, hosts, correos entre otros, para conseguir los datos, se vale de motores de búsqueda, LinkedIn y la potente base de datos Shodan, estas datos que se obtienen con TheHarvester son de gran apoyo para realizar un ataque.

Análisis de Riesgos
Es el estudio que debe realizar toda organización con el fin de identificar las vulnerabilidades a las que se encuentran expuestos sus activos, así como identificar cuáles son esas amenazas que se podrían desencadenar a raíz de estas vulnerabilidades, esta es la razón por la cual se debe tener identificado los riesgos a los que se enfrenta la compañía y así establecer medidas que permitan una correcta seguridad de la información.

3.3 MARCO CONCEPTUAL

Activos: Se puede decir que los activos son todos los elementos que hacen parte de un sistema de información, estos pueden ser hardware, software, instalaciones, los servicios prestados.

Amenaza: Son problemas que pueden afectar los activos de la organización, esas pueden ser origen humano que a su vez pueden ser sin intención como las causadas por negligencia y las malintencionadas que pueden ser internas o externas, el otro tipo de amenazas son las causadas por fenómenos de origen natural.

Vulnerabilidad: Se considera como vulnerabilidad la debilidad que posee un bien y que puede ser aprovechada por una amenaza para materializarse, esta es la razón por la cual se debe trabajar bastante en aspectos de seguridad informática.

Impacto: Son las consecuencias que sufre un activo cuando una amenaza se materializa.

Riesgo: Es la probabilidad de que ocurra un evento y sus consecuencias negativas ocasionando daños o perdidas.

Disponibilidad: La información siempre está disponible, es caso de presentarse alguna falla, debe estar en capacidad de recuperarse rápidamente

Confidencialidad: La información solo puede ser consultada y modificada por personal autorizado.

Integridad: Que la información no haya sido modificada, es decir que sea igual a los datos de origen.

Desastres de origen natural: Accidentes causados por fenómenos naturales (terremotos, inundaciones,…)

Desastres de origen industrial: Accidentes causados por desastres industriales (contaminación, fallos eléctricos,…)

Errores y fallos no intencionados: Estos accidentes normalmente son causados por personal con permisos para acceder al sistema y causan fallas en el sistema por error o por omitir algunos procesos.

Ataques intencionados: Este tipo de ataques es causado por personal con acceso a la información y atacan el sistema con intenciones de conseguir un beneficio propio.

3.4 **MARCO NORMATIVO**

La legislación colombiana ha avanzado bastante en cuantos delitos informáticos se refiere, hoy en día existen varias leyes que abarcan aspectos relacionados con el uso de las Tecnologías de la Información y la Comunicación (TIC). Estas leyes constituyen un aporte al desarrollo del presente trabajo, algunas de estas son:

- Ley 1273 del 2009 (Colombia)

En el año 2009, se modificó el código penal, para dar paso a algunos artículos relacionados al uso y protección de la información y de los datos, además artículos para preservar el uso de las TIC.[3]

Algunos artículos relacionados en esta ley son:

- Acceso abusivo a un sistema informático.

[3] MINTIC. El Congreso de Colombia Decreta. Disponible en: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

- Uso de software malicioso.
- Suplantación de sitios web para capturar datos personales.
- Interceptación de datos informáticos.
- Daño informático.
- Violación de datos personales.
- Hurto por medios informáticos y semejantes.
- Transferencia no consentida de activos.

- Ley 1288 de 2009

En el año 2.009 DIARIO OFICIAL, publicó la expedición de normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, además se dictan otras disposiciones.

Algunos artículos contemplados en esta ley son:

- Reserva de información en inteligencia y contrainteligencia.
- Coordinación y cooperación en las actividades de inteligencia y contrainteligencia.
- Los miembros de la Comisión Legal Parlamentaria de Seguimiento a las Actividades de Inteligencia y Contrainteligencia serán sometidos a estudios periódicos de seguridad y confiabilidad.
- Controlar el ingreso y la salida de información a las bases de datos y archivos de inteligencia y contrainteligencia, garantizando de manera prioritaria su reserva constitucional y legal.

4. DISEÑO METODOLÓGICO

4.1 **ALTERNATIVA DE GRADO:**

Monografía

4.2 **LÍNEA DE INVESTIGACIÓN:**

Cadena de formación de sistemas, línea de gestión de sistemas

El análisis para la implementación del SGSI de la empresa Servidoc S.A. se llevara a cabo siguiendo una serie de fases que permitirán cumplir con los objetivos planteados. Según SALCEDO, Robin J, un SGSI debe cumplir con 6 fases.

Figura 1. Fases para implementar un SGSI

Fuente:http://openaccess.uoc.edu/webapps/o2/bitstream/10609/41002/4/rsalcedobTFC1214memoria.pdf

En cada una de las fases se detallan los procedimientos y actividades que se deben realizar, estos son:

- **FASE 1: Situación actual:** En esta fase se analiza cómo se encuentra la organización en el cumplimiento de los controles de la norma ISO/IEC 27001:2013, se realiza un análisis diferencial y se definen cuáles son las fortalezas y debilidades de la empresa en cuanto a seguridad informática.

- **FASE 2: Sistema de Gestión Documental:** Elaboración de la Política de Seguridad, declaración de aplicabilidad y documentación del SGSI.
- **FASE 3: Análisis de riesgos:** Se define cual será la metodología de análisis de riesgos que se implantará, esta debe permitir identificar las vulnerabilidades, amenazas y el riesgo al cual se enfrenta la organización.
- **FASE 4: Propuesta de Proyectos:** Se sugieren una serie de proyectos para que la organización pueda alcanzar los objetivos planteados
- **FASE 5: Auditoría de Cumplimiento** de la ISO/IEC 27001:2013: Esta fase permite definir el cumplimiento de los controles de la norma que tiene la organización.
- **FASE 6**: **Presentación de Resultados y entrega de Informes:** Se presentan los resultados del proyecto y las conclusiones.

4.3 **RECURSOS DISPONIBLES**

Se dispone del apoyo de los directivos de la empresa Servidoc S.A., el material y documentación necesaria para el desarrollo de este proyecto va a ser proporcionado por la empresa.

Se cuentan con los recursos disponibles para realizar el análisis de este proyecto, se dispone con Conexión a internet por fibra óptica, además de un computador con procesador Core I5 y un Disco Duro de 1 Tera, configuración suficiente para el desarrollo de este proyecto, los insumos como papelería, DVD, memorias, fotocopias y todos los que se deriven de este, serán asumidos por la empresa.

También se cuenta con el acceso a todos los equipos de cómputo de las áreas de contabilidad, facturación e historias clínicas, por órdenes de la gerencia, se cuenta con el total apoyo y disposición de los empleados, incluso aprobación de tiempos extras cuando sea necesario, para ello sólo es necesario enviar un correo electrónico a la gerencia informando.

4.4 **TÉCNICAS DE RECOLECCION DE INFORMACION, POBLACIÓN Y MUESTRA**

TÉCNICAS DE RECOLECCION DE INFORMACION

Para el desarrollo del proyecto se realización las siguientes técnicas de recolección de información:

- Revisión de Documentos: Permite tener una visión clara de donde se encuentra la organización actualmente y para donde se dirige. Los documentos a revisar pueden ser cuantitativos como consultas, manuales de procedimientos, política, el otro tipo de documentos son los cualitativos como reportes, registros de captura de información.

- Entrevistas: En esta técnica se utilizan preguntas y respuestas, están son de tipo abiertas o cerradas, se deben realizar siguiendo una serie de pasos como: realizar una lectura previa del cuestionario, es necesario que se establezcan los objetivos a alcanzar, luego se debe realizar una selección del personal, indicarle al entrevistado cual es el objeto de esta.

POBLACIÓN: La población estuvo representada por los funcionarios de la empresa Servidoc S.A.

MUESTRA: Después de haber definido la población, se tomó una muestra de 25 empleados de la organización.

4.5 TECNICAS DE PROCESAMIENTO Y ANALISIS DE DATOS

Una vez se tiene toda la información necesaria suministrada por las entrevistas realizadas al personal de la organización, se procede a realizar una serie de procedimientos para lograr los resultados deseados.

Es necesario que las entrevistas cumplan con lo que se estableció inicialmente, además es importante verificar que las encuestas hayan sido diligenciadas en su totalidad, si las preguntas realizadas fueron comprendidas realmente por los entrevistados, y otros factores que permitan un resultado real y eficiente, el siguiente paso es ingresar la información a una hoja electrónica o programa de propósito específico para tal fin, por último se realiza la respectiva tabulación de los resultados obtenidos.

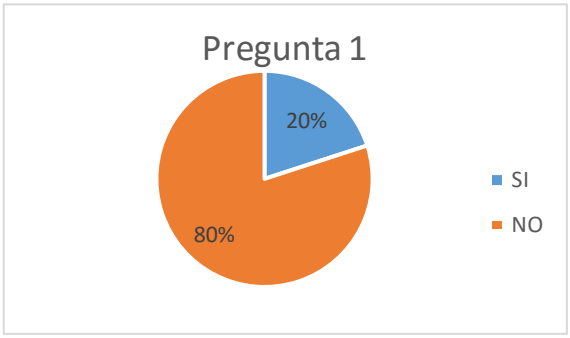
Para analizar la situación actual de la empresa Servidoc S.A. se realizó tabla de frecuencia en un solo sentido, la cual indica en cada tabla el porcentaje de aquellos entrevistados que dieron una respuesta a cada pregunta. Así mismo, se exponen representaciones gráficas con estadísticas las cuales a través de imágenes ilustran los resultados de la investigación. (Véase el Anexo A).

4.6 **DESARROLLO DEL PROYECTO**

Los resultados arrojados por la encuesta realizada al personal de Servidoc S.A. son los siguientes:

Pregunta 1

Figura 2. ¿El computador asignado para el desarrollo de sus funciones recibe mantenimiento periódicamente?



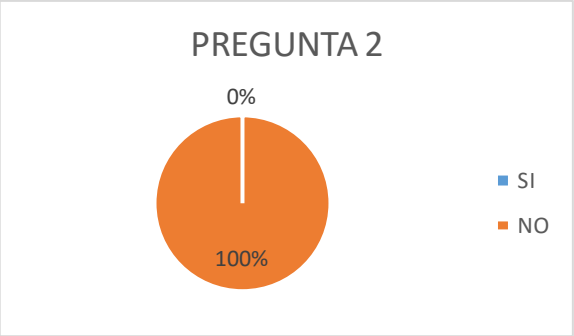
No.	ITEM	FRECUENCIA	%
1	SI	5	20,00%
2	NO	20	80,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, 5 mencionaron que se realizaba mantenimiento cada tres meses, 20 dicen que no se realiza mantenimiento periódicamente.

Pregunta 2

Figura 3. ¿Existe un Sistema de Gestión de Seguridad Informática en la Empresa?



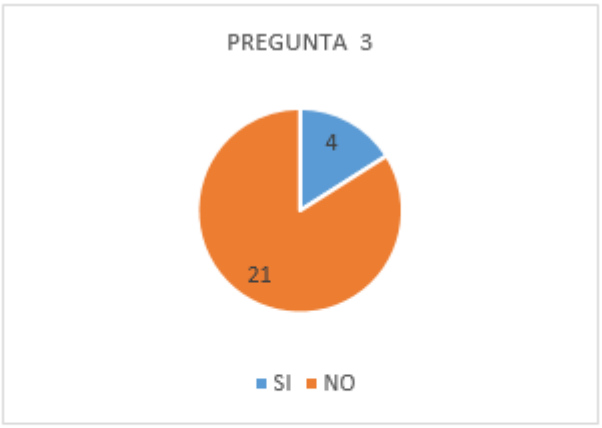
No.	ITEM	FRECUENCIA	%
1	SI	0	0,00%
2	NO	25	100,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, 25 mencionaron que no existe un Sistema de Gestión de Seguridad de la Información.

PREGUNTA 3

Figura 4. ¿La compañía capacita al personal en temas de seguridad informática?



No.	ITEM	FRECUENCIA	%
1	SI	4	16,00%
2	NO	21	84,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, 25 mencionaron que nunca se realiza capacitación en aspectos relacionados con seguridad informática.

PREGUNTA 4

Figura 5. ¿Existe alguna política para el cambio regular de las contraseñas?

No.	ITEM	FRECUENCIA	%
1	SI	2	8,00%
2	NO	23	92,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, 23 mencionaron que han sido informados de manera verbal, pero no se aplican con regularidad, 2 empleados afirman que si hay políticas de cambio de contraseñas.

PREGUNTA 5

Figura 6. ¿Existe un manual de funciones y responsabilidades de seguridad de la información?

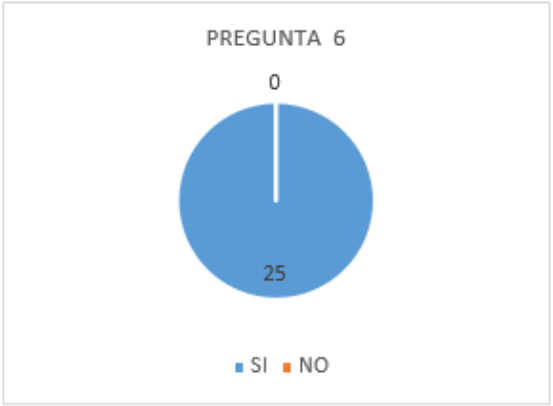
No.	ITEM	FRECUENCIA	%
1	SI	0	0,00%
2	NO	25	100,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, 25 mencionaron no conocer manuales de funciones y responsabilidades de seguridad de la información.

PREGUNTA 6

Figura 7. ¿Cuándo ocurre un evento relacionado con seguridad de la información sabe a quién reportarlo?



No.	ITEM	FRECUENCIA	%
1	SI	25	100,00%
2	NO	0	0,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, 25 mencionaron que cuando ocurre un evento relacionado con seguridad informática, se debe reportar al ingeniero de sistemas.

PREGUNTA 7

Figura 8. ¿Realiza copias de los datos?

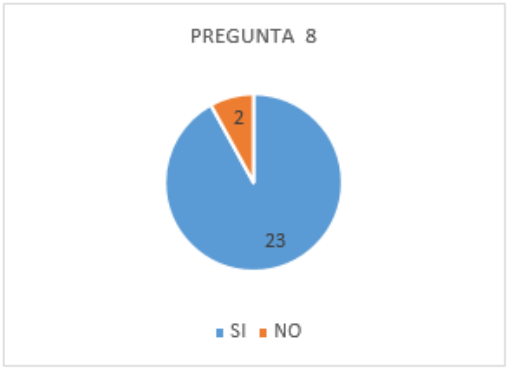
No.	ITEM	FRECUENCIA	%
1	SI	6	24,00%
2	NO	19	76,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, 6 mencionaron que realizan copias de seguridad en algunas ocasiones, los 19 restantes, correspondientes al 76% mencionaron nunca realizar copias de seguridad.

PREGUNTA 8

Figura 9. ¿Considera necesario que la compañía invierta en el análisis para la implementación de un Sistema de Gestión de Seguridad de la Información?



No.	ITEM	FRECUENCIA	%
1	SI	23	92,00%
2	NO	2	8,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, 23 mencionaron que sería muy importante una inversión de este tipo, dos empleados contestaron que ese dinero se podría invertir en otras cosas.

PREGUNTA 9

Figura 10. ¿Posee antivirus el computador?

No.	ITEM	FRECUENCIA	%
1	SI	7	28,00%
2	NO	18	72,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.
Interpretación**:**

De 25 empleados encuestados, 7 mencionaron que el computador si cuenta con programa antivirus, los 18 restantes afirman que no se cuenta con programa antivirus.

PREGUNTA 10

Figura 11. ¿La compañía posee software legal en su totalidad?

No.	ITEM	FRECUENCIA	%
1	SI	4	16,00%
2	NO	21	84,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, 4 afirman que se tiene software legal, los 21 restantes dicen que la empresa no tiene licencias legales

PREGUNTA 11

Figura 12. ¿Existen zonas restringidas de acceso de personal?

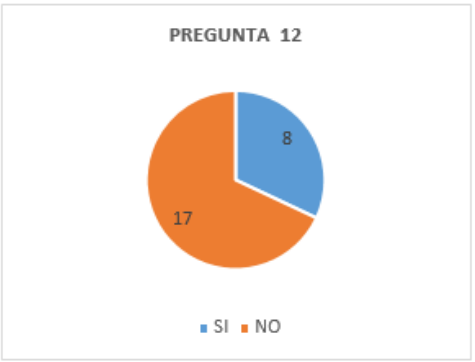
No.	ITEM	FRECUENCIA	%
1	SI	4	16,00%
2	NO	21	84,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, 4 afirman que la empresa si cuenta con zonas restringidas, los 21 restantes dicen que no se cuenta con sitios restringidos.

PREGUNTA 12

Figura 13. ¿Se realiza mantenimiento preventivo y correctivo a la UPS?



No.	ITEM	FRECUENCIA	%
1	SI	8	32,00%
2	NO	17	68,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, 8 afirman que se realiza de forma periódica mantenimiento a la UPS, los 17 restantes dicen que no se realiza ningún mantenimiento.

PREGUNTA 13

Figura 14. ¿Existen sistemas de seguridad que impidan el acceso a lugares restringidos?

No.	ITEM	FRECUENCIA	%
1	SI	0	0,00%
2	NO	25	100,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, los 25 afirman que no se poseen dispositivos de control de acceso.

PREGUNTA 14

Figura 15. ¿Se cuenta con sistemas de alarma como detectores de humo y humedad?

No.	ITEM	FRECUENCIA	%
1	SI	0	0,00%
2	NO	25	100,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, los 25 afirman que no se poseen dispositivos de este tipo.

PREGUNTA 15

Figura 16. ¿Existe vigilancia en la entrada del edificio?

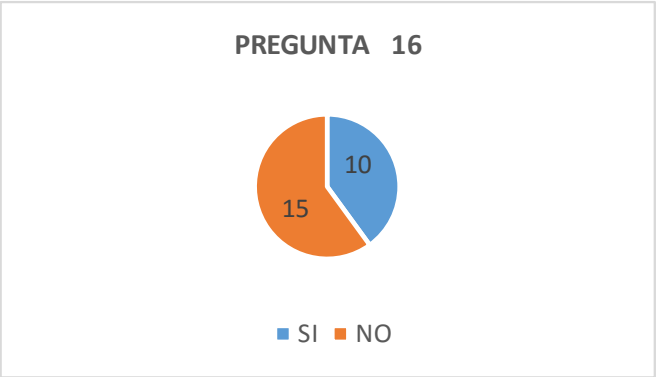
No.	ITEM	FRECUENCIA	%
1	SI	0	0,00%
2	NO	25	100,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, los 25 afirman que no se cuenta con vigilancia al ingreso de la organización.

PREGUNTA 16

Figura 17. ¿Los sitios donde están los equipos de cómputo cuentan con aire acondicionado?



No.	ITEM	FRECUENCIA	%
1	SI	20	80,00%
2	NO	5	20,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, 20 afirman que se cuenta con airea condicionado donde funcionan los equipos, los 5 restantes dicen que no tienen aire acondicionado.

PREGUNTA 17

Figura 18. ¿Se encuentra asegurados mediante pólizas los equipos de cómputo?

No.	ITEM	FRECUENCIA	%
1	SI	4	16,00%
2	NO	21	84,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, 4 afirman que se cuenta con pólizas de protección, los 21 restantes dicen que no se cuenta con ninguna póliza de protección para los equipos de cómputo.

PREGUNTA 18

Figura 19. ¿Existe algún control para navegar en internet?

No.	ITEM	FRECUENCIA	%
1	SI	3	12,00%
2	NO	22	88,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, 3 mencionan que se cuenta con controles para navegación, los 22 restantes dicen que no se cuenta con ninguna restricción.

PREGUNTA 19

Figura 20. ¿Existe control sobre el uso del correo electrónico?

No.	ITEM	FRECUENCIA	%
1	SI	25	100,00%
2	NO	0	0,00%
	TOTAL	**25**	**100,00%**

Fuente: El autor.

Interpretación**:**
De 25 empleados encuestados, los 25 mencionan la inexistencia de controles para el uso del correo electrónico.

5. FASES PARA IMPLEMENTAR UN SGSI

5.1 FASE 1: SITUACION ACTUAL

En esta fase se relaciona la situación actual de la compañía, y el análisis diferencial

5.1.1 Situación actual.

Para Servidoc S.A, como para las demás empresas del sector, la Seguridad Informática ya no es un problema de los profesionales o del proceso de sistemas de una organización, sino que ha salido de los centros de cómputo para instalarse en el escritorio del usuario, en donde verdaderamente nacen los problemas de Seguridad.

El hecho de que Servidoc S.A. sea una empresa dedicada a la prestación de servicios, significa que la sobrecarga de información es representativa, esta situación se traduce en que personas no autorizadas puedan robar, alterar, acceder o vulnerar la información.

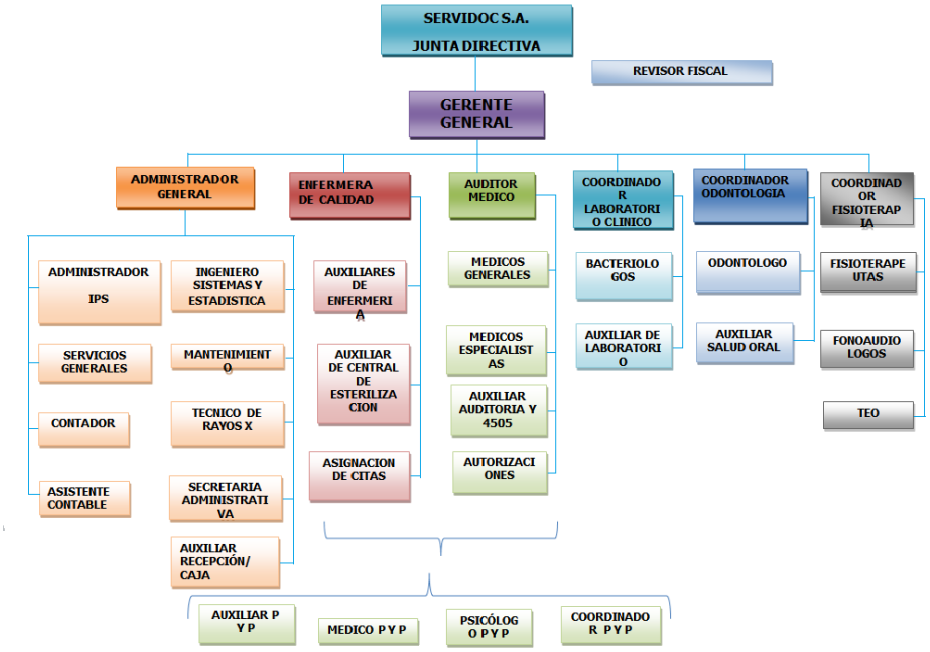
La anterior situación conlleva a realizar permanentemente tareas que permitan reducir riesgos que pongan en peligro la información de las áreas de facturación, contabilidad e historias clínicas de la empresa Servidoc S.A.

La información de la organización, los procesos que la apoyan, así como los sistemas y las redes, son bienes muy importantes para Servidoc S.A, por lo que requieren ser protegidos frente a amenazas que puedan poner en riesgo la disponibilidad, integridad, confidencialidad de la información y la estabilidad de los procesos la compañía.

De ahí la importancia del análisis para la implementación de un Sistema de Gestión de la Seguridad Informática basados en los requisitos de la norma ISO-27001.

5.1.2 Organigrama

Figura 21. Organigrama Servidoc S.A.



Fuente: Servidoc S.A.

5.1.3 **Activos que posee servidoc s.a.**

La empresa Servidoc S.A. cuenta con una sede ubicada en la ciudad de Cali, específicamente en la Avenida 3AN No. 23DN 08, es un edifico que consta de cuatro pisos. En el primer piso funciona la barra de servicios y consultorios de médico general y especialistas, en el segundo piso funcionan laboratorio, administración, además se encuentra ubicado el cuarto técnico, donde están todos los equipos de comunicaciones como rack, swichet, routers, entre otros, en el tercer piso funcionan odontología y rayos X, en el cuarto piso consultorios médicos. Es de aclarar que la sede no es de propiedad de la empresa, es un edifico tomado en alquiler.

Inventario de Activos

Un activo[4] Es todo lo que una empresa posee para llevar a cabo el tratamiento de la información, entre estos están (hardware, software, recurso humano entre otros), esta clasificación se realiza como se plantea en la siguiente tabla.

[4] SALCEDO, Robin J. Sistema de gestión de la seguridad de la información. Disponible en http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/321_paso_1_inventario_de_activos.html

Tabla 1. Activos de Servidoc S.A.

Tipo de Activo	Descripción	Valor Activo	Valor en Millones de $	Criticidad
Personal Personal	Personal Directivo	Muy alto	250	Crítico
	Administradora	Alto	150	Crítico
	Jefes enfermería	Alto	90	Alto
	Personal barra de servicios	Alto	50	Bajo
	Auxiliares enfermería	Medio	50	Bajo
	Auxiliares laboratorio	Medio	50	Bajo
	Médicos Generales	Alto	50	Bajo
	Médicos especialistas	Alto	50	Alto
	Servicios generales	Medio	50	Bajo
	Contadora	Alto	100	Alto
	Asistente contable	Medio	50	Medio
	Revisor fiscal	Alto	100	Medio
	Secretaria gerencia	Medio	50	Bajo
	Secretaria asignación citas	Bajo	10	Bajo
	Ingeniero sistemas	Alto	100	Critico
	Bacteriólogas	Alto	100	Alto
	Mensajero	Alto	3	Muy bajo
	Auditores médicos	Alto	100	Alto
	Electro médico	Alto	100	Medio
	Electricista	Bajo	10	Bajo
	Mantenimiento	Bajo	10	Bajo
Hardware	Portátiles	Bajo	10	Medio
	Equipos de cómputo	Medio	50	Crítico
	Impresoras	Medio	40	Alto
	Servidor Aplicaciones	Muy Alto	200	Critico
Red	Acces Point	Medio	50	Crítico
	Swichet	Medio	50	Crítico
	Routers	Medio	50	Crítico
	firewalls	Medio	50	Crítico
Instalación	cableado estructurado	Muy alto	250	Crítico
	Instalaciones eléctricas	Muy alto	250	Crítico
Servicios	Conectividad a internet	Muy alto	250	Crítico

Tabla 1. (Continuación)

Tipo de Activo	Descripción	Valor Activo	Valor en Millones de $	Criticidad
Equipamiento Auxiliar	Planta eléctrica	Medio	60	Bajo
Software o aplicación	Windows server 2010	Medio	50	Crítico
	CgUno	Medio	50	Alto
	Windows	Medio	50	Alto
	Ofimática	Bajo	10	Muy bajo
Activo de información	Contratos de trabajo personal	Bajo	10	Bajo
	Pólizas mantenimiento	Bajo	10	Bajo
	BD usuarios EPS	Medio	50	Crítico
	BD proveedores	Medio	50	Crítico
	contabilidad	Muy alto	200	Crítico
	Mercadeo	Alto	100	Medio

Fuente: El Autor

5.1.4 **Análisis diferencial.**

En esta etapa se establece un paralelo entre los controles que tiene implementados la Cía. frente a los controles que contempla la norma ISO 27001:2013, con el objeto de realizar un análisis para la implementación de un sistema de Gestión de Seguridad de la Información (SGSI), además permitirá establecer un análisis de la documentación.

El autor NIETO, Juan Pablo [5] en su trabajo de maestría en seguridad de las TIC, realizo un análisis diferencial, afirmando que el resultado que debe generar este es la identificación de las áreas que poseen falencias y sus respectivos planes para mejorar la seguridad en estas. El análisis de los controles se hace teniendo en cuenta el estado actual, para ello se le asigna una calificación de acuerdo a la siguiente tabla.

[5] NIETO, Juan Pablo Plan de implementación de la ISO/IEC 27001:2005. Disponible en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23054/1/Nieto_WP2013_PlanImplementacionISO2007.pdf

Tabla 2. Nivel de cumplimiento

NIVEL DE CUMPLIMIENTO		
Valor	**Nombre**	**Descripción**
0	No existente	No existe evidencia del estándar o practica en la compañía.
1	Inicial	La organización tiene practicas hechas a la medida pero inconsistentes.
2	Repetible	La organización tiene un enfoque coherente pero no documentado.
3	Definido	Se tiene un enfoque coherente y documentado pero no medido.
4	Administrado	Los procesos son medidos frecuente mente y se realizan mejoras.
5	Optimizado	La organización ha refinado su cumplimiento con el nivel de las mejores prácticas

Fuente: El Autor

En el Anexo B. se realiza un análisis diferencial de la compañía, se observa la situación actual de la organización, para ello es necesario tomar cada uno de los controles de la norma ISO/IEC 27001:2013, donde se analiza control por control, identificando su responsable, el nivel de cumplimiento de acuerdo a los valores definidos en la Tabla 2. Se asigna una calificación de 0 a 5, además se cuenta una columna descripción donde se menciona si el control existe actualmente o no, por último se encuentra la columna cumple/no cumple, en la cual se han definido valores como si - no. (Véase el Anexo B).

5.1.5 **Fortalezas y debilidades**

Fortalezas

- Algunos funcionarios son conscientes de los roles que tienen
- Comprobación de antecedentes de los empleados
- Se cuenta con inventario de asignación de activos por empleado para el desarrollo de sus funciones
- Existen algunos procedimientos sobre cambios de contraseñas sin documentar
- Existen controles criptográficos solamente para presentación de informes a la Supe salud

- Existen algunos controles sobre sitios restringidos pero no están bien definidos
- Existen algunos controles sobre el mantenimiento de los equipos de cómputo
- Existen algunos extintores contra incendios
- Se cuenta con procedimientos de sincronización de relojes
- Se tiene algún conocimiento sobre la legislación y derechos de autor

Debilidades

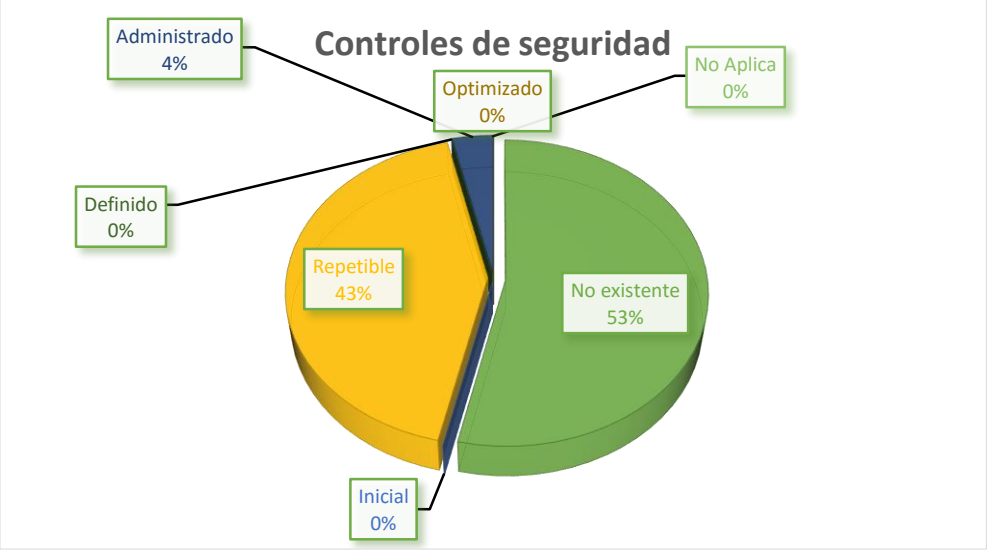
- No existe un documento de políticas de seguridad de la información.
- No se tiene bien definido ni documentado los roles y responsabilidades en materia de seguridad informática
- No existen políticas documentadas sobre el uso adecuado de dispositivos móviles
- No existen cláusulas de reserva de la información durante y después del empleo
- No existen políticas sobre el uso correcto y responsable de los activos asignados
- No existen procedimientos documentados sobre privilegios de acceso a la información
- No existen procedimientos sobre creación y cambio de contraseñas
- Se carece de políticas que exijan la protección de la información mediante controles criptográficos
- No existen zonas restringidas demarcadas
- No existen controles de seguridad física al ingreso de las instalaciones
- No se cuenta con controles para el retiro de equipos de las instalaciones
- La organización carece de un seguro contra incendios y desastres naturales
- No existen políticas sobre la manipulación de los dispositivos tecnológicos de la empresa
- No se realizan copias de seguridad con frecuencia
- No se actualiza el software con regularidad
- No se cuenta con software antivirus en la totalidad de los equipos de cómputo
- No existe ningún procedimiento de monitoreo físico ni lógico

- Falta de capacitación al personal en temas relacionados con el manejo de correo electrónico
- Falta de seguridad en la configuración de las redes y el acceso a ellas

- No se cuenta con dispositivos de protección de transporte de información
- Falta de acuerdos de confidencialidad.
- No se documenta los incidentes ocurridos
- No se tiene conocimiento sobre cómo actuar en caso de un incidente
- Aunque se tiene conocimiento sobre la legislación, su cumplimiento en mínimo
- Se carece de software legal en un 90%
- Procedimientos ineficientes de protección de datos
- Procedimientos ineficientes de protección de información de tipo personal

En la siguiente imagen se muestra el cumplimiento de los dominios de acuerdo a la norma ISO/IEC 27001:2013, es de notar que el mayor porcentaje, en este caso el 53%, equivale a controles inexistentes, el 43% corresponde al estado repetible lo que significa que se tiene conocimiento de algunos controles, pero no se encuentra bien definidos ni documentados, el 4% corresponde a controles administrados, lo que representa un porcentaje muy bajo.

Figura 22. Controles de seguridad existentes



Fuente: El autor.

En la siguiente tabla se muestra el porcentaje de cumplimiento de los controles por cada dominio, mostrando unos resultados preocupantes, pues la

organización tiene actualmente un cumplimiento del 15%, lo que representa grandes debilidades en cuanto a seguridad informática se refiere.

Tabla 3. Cumplimiento de controles por dominio

	Control/Objetivo de Control	Estado Actual
5	Políticas de seguridad de la información	0%
6	Organización de la seguridad de la información	0%
7	Seguridad de los recursos humanos	17%
8	Gestión de activos	52%
9	Control de acceso	23%
10	Criptografía	0%
11	Seguridad física y del entorno	40%
12	Seguridad de las operaciones	26%
13	Seguridad de las comunicaciones	40%
14	Adquisición, desarrollo y mantenimientos de sistemas	9%
15	Relación con los proveedores	0%
16	Gestión de incidentes de seguridad de la información	0%
17	Aspectos de seguridad de la información de la gestión de continuidad de negocio	10%
18	Cumplimiento	0%
	TOTAL	**15%**

Fuente: El autor.

En la siguiente imagen se encuentra el cumplimiento de los dominios pero de forma gráfica.

Figura 23. Cumplimiento de dominios

Fuente: El autor.

5.2 **FASE 2: SISTEMA DE GESTION DOCUMENTAL**

Todo sistema de gestión de seguridad informática SGSI debe contener una gestión documental, en este apartado se desarrollará toda la documentación que debe existir en la implementación de un SGSI como lo muestra la norma ISO/EIC 27001.

La autora ROJAS VALDUCIEL, Halena[6] en el año 2.015 afirma que la documentación además de avalar las estrategias y decisiones tomadas con respecto a la seguridad de la información dentro de la empresa, servirá de guía para el análisis de la implementación del SGSI.

5.2.1 **Políticas de seguridad**

Cuando se habla de seguridad informática existen ciertas reglas que se deben cumplir para dar cumplimiento a las premisas de la seguridad informática como son la disponibilidad, integridad y disponibilidad, esa es la razón por la cual todos los procedimientos para llevar la seguridad deben estar documentados, la persona responsable de la seguridad informática de la empresa Servidoc

[6] ROJAS VALDUCIEL, Halena. Elaboración de un plan de implementación de la ISO/IEC 27001:2013

S.A. se debe comprometer en primera instancia a la revisión y actualización de estas normas en unos períodos como máximo de un año, además debe velar por que estas políticas sean conocidas por todos los empleados de la organización.

Estas políticas afectan también a terceras personas como son clientes, proveedores, entre otros. Hay que recalcar que estas normas son de carácter confidencial, lo que significa que sólo el personal interno de la organización tiene derecho a su uso, además podrá ser usado por terceras personas sólo con autorización del personal de seguridad.

Las personas que hagan uso de los sistemas de información deben cumplir unas funciones y obligaciones asignadas por el encargado de la seguridad informática, dentro de estas están:

Control de acceso:

- Responder por las claves de ingreso a los sistemas, no debe compartir las claves con otras personas, estas son privadas.
- Cambiar regularmente la clave, siguiendo algunos estándares para claves seguras.
- Cada usuario se hace responsable de los procedimientos ejecutados con su clave de acceso.

Confidencialidad de la información

- La confidencialidad de la información de la organización se debe respetar, no se debe compartir esta bajo ninguna circunstancia.
- La información no debe ser retirada de la empresa.
- Hay que guardar reserva en el uso de memoria con firmas digitales, estas deben permanecer en caja fuerte y retiradas cuando se vayan a utilizar.

Propiedad intelectual

- Se debe respetar la política de propiedad intelectual, por lo cual no se deben instalar en los equipos de cómputo de Servidoc S.A. aplicaciones que carezcan de licencias adquiridas de manera formal.
- Se prohíbe la duplicación de material que carezca de licencia original.

Control de acceso físico

- Todo el personal que vaya a ingresar a los espacios donde se encuentran los equipos de cómputo, debe contar con previa autorización.
- El ingreso al cuarto técnico, que es donde se encuentran todos los equipos de comunicaciones, debe contar con autorización únicamente del encargado de la seguridad informática de la empresa.
- Nunca deben existir en los puestos de trabajo medios extraíbles que puedan ser fácilmente tomados sin autorización.

Uso apropiado de los recursos

Los recursos asignados a cada empleado por parte de la empresa para el desarrollo de sus funciones se deben utilizar para tal fin y no para realizar actividades personales. Algunas de las actividades que están prohibidas son:

- Instalar programa informáticos en los equipos sin previa autorización
- Instalar programas antivirus, anti spam entre otros.
- Desinstalar o modificar programas sin previo aviso.
- Conectarse a la red con dispositivos diferentes a los asignados por la empresa para el desarrollo normal de sus funciones.

Software

- Se debe utilizar únicamente software legal.
- Queda prohibido la reproducción de programas como software ofimático, sistemas operativos entre otros.
- Informar sobre las actualizaciones de los programas antivirus.
- Chequeo de medios extraíbles autorizados para su uso por medio de antivirus.
- Queda prohibido descargar programas y música.

Hardware

- No se deben retirar los equipos de las instalaciones de la organización sin previo aviso y autorización.
- Los equipos no deben ser manipulados por cualquier usuario, de ser necesario se debe reportar el daño para que las personas encargadas realicen los correctivos necesarios.
- El único hardware autorizado para su funcionamiento, es el autorizado y asignado por la empresa.
- Queda prohibido conectar medios extraíbles en los equipo tales como memorias, cámaras, celulares.

Conexión a internet

- La conexión a internet es restringida de acuerdo a los parámetros establecidos por la organización.
- Se deben conectar sólo los dispositivos autorizados.
- Cada usuario debe responder por la navegación realizada desde su computador.
- En caso de realizar transacciones personales, el usuario se hará responsable de ellas, aunque no se deberían realizar ya que los equipos de cómputo son solamente para funciones laborales.
- No utilizar el internet para descargar programas y canciones.
- El uso de mensajería instantánea, correos, foros, entre otros debe ser solamente para actividades relacionadas con la empresa.

Correo electrónico

- El uso del correo electrónico debe ser solamente relacionado a actividades laborales.
- No utilizar el correo con fines personales.
- En caso de sospechar de algún correo, informarlo al personal encargado de la seguridad informática.
- Los correos corporativos deben llevar la firma del remitente.
- Verificar que los archivos adjuntos no estén infectados.
- Evitar participar en cadenas de oración, y reenvió de correos, ya que estos son factores decisivos para que un atacante pueda vulnerar la red de la empresa.
- No se debe ingresar al correo de otros usuarios y manipular la información.
- Las cuentas de correo deben estar previstas de claves.
- Cada usuario se hará responsable el uso que le dé a su cuenta de correo.

Custodia de recursos informáticos

- Los usuarios deben responder ante la empresa por los recursos informáticos que le sean asignados.
- Mantener actualizado el inventario de los recursos de hardware que la empresa le ha asignado.
- Seguir con los lineamientos establecidos para el uso correcto de los dispositivos.
- Informar oportunamente en caso de pérdida o daño de los recursos informáticos asignados.

Usuarios y contraseñas

- Para el ingreso a los sistemas de información cada usuario debe contar con un nombre de usuario y contraseña.
- Las claves se deben cambiar cada 30 días, sin permitir que se repitan.
- El número máximo de intentos para el ingreso será de cinco veces, en caso de completar todos los intentos, el sistema bloqueara el ingreso, siendo necesario adquirir una nueva clave.
- Las contraseñas serán asignadas por el personal encargado de la seguridad informática, permitiendo el cambio de contraseña de forma inmediata, evitando así que otras personas, incluso el encargado de seguridad pueda tenerlas, su almacenamiento debe ser cifrado.
- Las contraseñas deben contener máximo ocho caracteres alfanuméricos.

5.2.2 **Procedimiento de auditorías internas**

La correcta implementación de un Sistema de gestión de seguridad informática SGSI, le permite a una organización obtener una certificación internacional, lo que significa ser más competitiva en el mercado, demostrando que cumple con todos los estándares de seguridad lo que dará confianza a clientes, proveedores y empleados.

Para llegar a este punto es necesario realizar auditorías, estas son:

Auditoria documental:

En esta etapa, los auditores tienen la obligación de revisar toda la documentación que posee la organización, es necesario revisar las políticas de seguridad, el alcance que se le dio al SGSI, el nivel de madurez que tiene la organización en cuanto a los controles implementados, realizar un detallado análisis de riesgos, para luego seleccionar los controles que se deben implementar.

Una vez realizado este proceso, los auditores preparan un informe muy detallado donde se establecerán las fortalezas y debilidades con que cuenta el SGSI, en este informe deben describirse las no conformidades encontradas, indicando la gravedad que representan, dentro de las no conformidades, se encuentran tres tipos como son:

- No conformidades mayores: Estas representan un incumplimiento grande de la norma, para ello el auditor basado en su experiencia, determina que la seguridad de la información se verá afectada representativamente. Cuando se encuentran conformidades mayores, lo ideal es que estas sean corregidas para el inicio de la siguiente etapa.

- No conformidades menores: Estas corresponden a incumplimientos pequeños respecto a la norma, igual que las no conformidades mayores, se deben corregir para el inicio de la siguiente etapa.
- Observación u oportunidad de mejora: El auditor con el criterio que posee, determina que son situaciones que no ponen en peligro la seguridad de la información, sugiere que sean analizadas en futuros procesos de auditoría.

Auditoria de certificación:

En esta etapa, el SGSI debe cumplir a cabalidad con todo lo descrito en el plan de implementación del sistema de gestión de seguridad informática, no pueden existir no conformidades, las políticas deben estar desarrolladas en su totalidad, esto significa que todos los procesos funcionan eficazmente.

Las auditoria se deben realizar cada año, con el fin de identificar si el SGSI está cumpliendo con lo establecido en la norma ISO/IEC 27001, lo que se trata es de identificar si los procesos están funcionando bien, si necesitan ser reestructurados, si los controles ya son obsoletos o si ya no son necesarios. Este es un proceso repetitivo que deben realizar todas las organizaciones con el fin de llevar el riesgo de la seguridad de la información a su nivel más bajo.

La persona encargada de la seguridad informática en la organización, será el responsable de socializar el informe de auditoría a la alta gerencia, estos informes deben ser archivados con el fin de estar disponibles ante entidades certificadoras.

5.2.3 **Gestión de indicadores**

La creación de indicadores de gestión está orientada principalmente en la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de mejoramiento continuo permitiendo adoptar decisiones de mejora. Estos indicadores o métricas permiten medir realmente que tan segura se encuentra una organización

Estos deben cumplir una serie de requisitos como son:

- Debe ser considerada de importancia para los objetivos que tiene la organización.
- Debe servir de apoyo para el análisis y tratamiento oportuno de riesgos

- Debe ser imparcial.
- Debe ser capaz de evaluar si un control genera seguridad ante la organización.

Existe una gran cantidad de indicadores que se podrían implementar en una empresa, pero dependiendo de su tamaño y presupuesto, es necesario en algunas ocasiones implementar sólo los que sean más relevantes para la organización como es el caso de la empresa Servidoc S.A. Donde el análisis para la implementación del SGSI mostrara sólo indicadores que tienen que ver con la seguridad en los equipos de cómputo de las áreas de contabilidad, facturación y nómina, pues ese es el alcance del desarrollo de este proyecto.

Tabla 4. Indicadores de Gestión

Indicador	Objetivo	Valor Aceptable	Frecuencia	Responsable	Calculo
Políticas de seguridad documentadas	cuantificar los documentos existentes sobre seguridad informática respecto a los esperados	75%	Semestral	Seguridad informática	Doc. Existentes/Doc. esperados
Protección contra código malicioso	Se busca definir la protección que tiene la organización frente a ataques de software maliciosa	90%	Mensual /	Seguridad informática	Equipos con antivirus y antimalware instalado y actualizado / total equipos
Acuerdos de confidencialidad	Obtener un valor real de niveles de confidencialidad firmados con proveedores, clientes, entre otros	80%	Trimestral	RH	Acuerdos de confidencialidad firmados/ total proveedores
No conformidades solucionadas	Identificar la respuesta que se le ha dado a las no conformidades	100%	Semestral		No Conformidades solucionadas / No conformidades emitidas en el periodo

Tabla 4. (continuación)

Indicador	Objetivo	Valor Aceptable	Frecuencia	Responsable	Calculo
Capacitación en seguridad informática	Identificar la cantidad de empleados que han recibido formación en cuanto a seguridad informática se refiere, además saber los roles que tiene asignados	80%	Trimestral	RH-Seguridad Informática	Empleados con capacitación / total empleados
Equipos sin contraseñas	Identificar equipos de cómputo que no cuentas con niveles de seguridad como usuario y contraseña para su ingreso	100%	Mensual	Seguridad Informática	Equipos sin contraseñas/ total equipos
Equipos sin licencias	Cuantificar equipos que no poseen licencias de software	100%	Mensual	Seguridad Informática	Equipos con licencias/equipos totales

Fuente: el autor

5.2.4 **Revisión por parte de la dirección**

El papel que juega la alta dirección es muy importante, puesto que si el análisis para la implementación del SGSI no cuenta con su apoyo, no se lograran los objetivos esperados, esta debe participar en las decisiones que se tomen respecto a seguridad informática, también es importante el seguimiento que le haga a los procedimientos pues de esta manera se dará cuenta si están funcionando correctamente.

Es responsabilidad de la dirección verificar los controles implementados en el SGSI en lazos de tiempo de al menos un año. Dentro de las revisiones que se deben realizar se encuentran:

- Verificar que todo el personal de la organización tenga conocimiento sobre las normas de seguridad implementadas a los sistemas de información.
- Revisar los resultados de las auditorías realizadas.
- Cambios en la organización que puedan afectar el SGSI.

- Debe realizar sugerencias para lograr el mejoramiento en la efectividad de algún control.
- Concientizarse con la necesidad de recursos.

5.2.5 **Gestión de roles y responsabilidades**

Todo sistema de gestión de seguridad informática debe contar con un comité de seguridad quien se encargará de realizar tareas como crear, mantener, supervisar y mejorar el sistema. Este comité debe estar integrado por diferentes responsables de la organización, además de una persona que pertenezca a la alta dirección con el fin de que cuando se tomen decisiones, estas sean aprobadas por un integrante de la dirección.

Comité de seguridad: Las funciones de este comité corresponden a:

- Incentivar el uso de las buenas prácticas en seguridad informática.
- Asignar funciones y responsabilidades en cuanto a seguridad informática.
- Revisar en períodos establecidos el SGSI y su respectiva aprobación.
- Aprobar las políticas de seguridad informática.
- Validar los riesgos a que se enfrenta la organización y sus respectivos controles.

El comité se seguridad de la empresa Servidoc S.A. está compuesto por:

- Administrador general
- Ingeniero de sistemas
- Revisor fiscal
- Enfermera de calidad
- Auditor médico

Funciones y obligaciones del personal

El comité de seguridad asignara funciones a cada uno de los empleados en materia de seguridad informática, estas serán las únicas que estos deban desarrollar, con el fin de brindar seguridad al sistemas de información.

Algunas de las exigencias que se deben realizar a quienes se les haya asignado responsabilidades son no compartir información de la empresa con terceras personas, uso adecuado de los recursos, cumplir con las cláusulas de confidencialidad de la información.

Personal con acceso privilegiado

El personal encargado de administrar el sistema es la persona encargada de:

- Asignación de perfiles a cada uno de los usuarios.
- Es el responsable del buen funcionamiento de los equipos de cómputo.
- Velar por la seguridad de la red y del software que opera en los equipos de cómputo.
- Actualización de los antivirus y demás software instalados.
- Igual que cualquier otro usuario del sistema de información debe respetar las políticas de seguridad de la empresa.

Personal con perfil de usuario

Sólo podrán ingresar a los programas que estén autorizados para el desarrollo normal de sus funciones. Dentro de sus funciones están:

- Cumplir las responsabilidades asignadas.
- Dar un buen uso a los equipos de cómputo.
- Abstener se instalar programas en los equipos.
- Cumplir al pie de la letra las normas establecidas en las políticas de seguridad.
- Guardar confidencialidad con la información que es de propiedad de la empresa.
- Bloquear los equipos cuando se ausenten de los puestos de trabajo.
- Hacer uso adecuado de las contraseñas asignadas.
- Informar al responsable de seguridad sobre anomalías detectadas

Responsable de seguridad

Es la persona encargada de coordinar todas las actividades relacionadas con seguridad informática de la organización, sus funciones son las siguientes:

- Hacer cumplir las políticas de seguridad de la información.
- Asignar privilegios a los usuarios del sistema.
- Analizar constantemente problemas con sus respectivas soluciones.
- Comprobar las políticas de buen uso de los equipos.
- Verificar que las auditorias se realicen en los tiempos establecidos.
- Comprobar que los controles establecidos cumplan los requerimientos.
- Comprobar la realización de copias de seguridad según lo establecido en las políticas.

- Realizar un asesoramiento de las políticas que se deben implementar en la empresa.

5.3 **FASE 3: ANÁLISIS DE RIESGOS**

La metodología utilizada para el desarrollo de este proyecto el cual consiste en el análisis para la implementación de un Sistema de Gestión de Seguridad Informática según la norma ISO 27001 en la empresa Servidoc S.A. se llevara a cabo haciendo uso de la metodología de análisis de riesgos MAGERIT

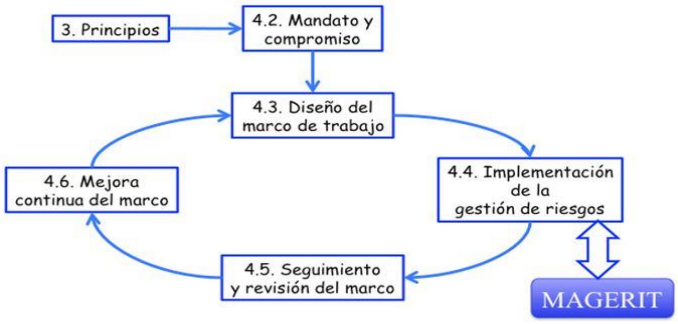
El autor MATALOBOS VEIGA, Juan Manuel (2.009) afirma que “el análisis de riesgos es una herramienta que permite identificar, clasificar y valorar los eventos que pueden amenazar la consecución de los objetivos de la organización y establecer las medidas oportunas para reducir el impacto esperable hasta un nivel tolerable”.

El análisis de riesgos es una de las tareas más importantes en la implementación de un Sistema de Gestión de Seguridad Informática, en este caso, para realizar el estudio de análisis de riesgos en la organización se ha seleccionado la metodología MAGERIT, esta es una metodología que fue elaborada por el Consejo Superior de Administración Electrónica.

Esta metodología está fundamentada principalmente en la minimización de los riesgos en las organizaciones, ya que a medida que crece el uso de las tecnologías de la información, los riegos a que se encuentran sometidas crecen de igual manera.

MAGERIT permite cuantificar los activos que posee la organización y el valor que representa para ella, indicando de esta forma los valores que están en riesgo y la forma de protegerlos, es una metodología que se desarrolla realizando una serie de pasos que se deben seguir al pie de la letra en aras de lograr los resultados esperados.

Figura 24. Análisis de Riesgos.



Fuente.
http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VfhKvvl_Oko

Objetivos

MAGERIT persigue los siguientes objetivos[7]:

- Concienciar a las organizaciones y a los responsables del manejo de la información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Dentro de los informes que se pueden encontrar están:

- Modelo de valor: Se define el valor que representa cada activo para la organización.
- Mapa de riesgos: Se detallan cada una de las amenazas a las cuáles están expuestos los activos de la organización.
- Declaración de aplicabilidad: Se identifican salvaguardas y se define si son relevantes en el SGSI.
- Evaluación de salvaguardas: Establecer un paralelo entre las salvaguardas existentes en relación al riesgo.

[7] PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. Magerit V.3: Metodología de análisis y gestión de riesgos de los sistemas de información. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VfhKvvl_Oko

- Estado de riesgo: Agrupación de los activos por riesgo
- Informe de insuficiencias: Identificar salvaguardas y determinar si son insuficientes o si existen, con el fin de reducir el riesgo
- Cumplimiento de la normatividad: Definir si está bien estructurada de acuerdo a la normatividad.
- Plan de seguridad: Establecimiento de los proyectos de seguridad.

La metodología MAGERIT contempla las siguientes fases:

Toma de datos y procesos de información
En esta fase se hace la definición del alcance del análisis.

Establecimiento de parámetros
Es esta etapa se definen los parámetros que serán utilizados durante todo el análisis, para este caso, los parámetros son:

- Valor de los activos
- Vulnerabilidad
- Impacto
- Efectividad del control

Análisis de activos

En esta fase se identifican de forma detallada todos los activos que la compañía y que son necesarios para el desarrollo normal de sus actividades.

Análisis de amenazas

Esta fase permite clasificar las amenazas que afectan la compañía, se clasifican en:

- Desastres naturales
- Desastres de origen industrial
- Errores y fallos no intencionados
- Ataques intencionados

Establecimiento de vulnerabilidades

Permite identificar las vulnerabilidades que posee la organización que en el momento de materializarse afectan los activos de la empresa.

Valoración de impactos

Se cuantifican el impacto que ejerce una amenaza sobre un activo.

Análisis de riesgo intrínseco
Este análisis muestra el estado en que se encuentra la organización en cuanto a seguridad informática se refiere.

Influencia de salvaguardas

Después de haber identificado los riesgos, es necesario reducir los riesgos, para ello se definen una serie de soluciones

Análisis de riesgos efectivos
Esta etapa informa sobre la manera como se reducirá el riesgo teniendo en cuenta las salvaguardas que se han identificado.

Gestión de riesgos
Esta etapa es la que realmente define el rumbo de la organización, pues aquí es donde se define cuales medidas de seguridad se implementarán según el listado de salvaguardas para reducir el riesgo.

5.3.1 **Declaración de aplicabilidad**

La declaración de aplicabilidad o SOA por sus siglas en inglés (Statement of Applicability), según (Valduciel, 2014). Es un documento que debe contener todo SGSI según la norma ISO/IEC 27001:2013, esta indica los controles que se implementaran en la organización, además se definen cuales controles se excluirán y cuál es la causa de la exclusión.

Al ser parte de la gestión documental, debe ser aprobado por la alta dirección y sometido a revisiones previas con el fin de mantenerlo actualizado de acuerdo al modelo y procesos de la empresa.

Según MENDOZA, Miguel Ángel (2.015) la declaración de aplicabilidad no se limita exclusivamente a los controles del estándar ISO seleccionado, se pueden utilizar otros controles en la medida que se considere necesario.

Tabla 5. Aspectos relevantes para seleccionar un control.

LR	Requerimiento Legal
CO	Obligaciones Contractuales
BR/BP	Requerimientos del negocio / Mejores Prácticas
RRA	Resultado de Análisis de Riesgos

Fuente: El autor.

Se ha diseñado una tabla donde se puede apreciar de una mejor manera la declaración de aplicabilidad, esta incluye cada uno de los controles de la norma ISO/IEC 27001:2013, se detallan los controles que son necesarios implementar en la organización además cada uno de los controles excluidos y la causa de su exclusión. (Véase el Anexo C).

5.3.2 **Toma de datos y procesos de información**

Esta fase va de la mano con el alcance definido para el SGSI, se debe tener en cuenta todos los procesos que desarrolla la organización, es necesario precisar a qué nivel de detalle se pretende llegar, haciendo énfasis en los procesos más críticos y los riesgos que estos generan.

5.3.3 **Establecimiento de parámetros**

En esta etapa se identifican los parámetros que serán de ayuda para realizar un correcto análisis de riesgo, estos son:

Valor de los activos

La siguiente tabla muestra el valor que ha sido asignado a cada activo, es de tener en cuenta que este valor está definido de acuerdo a unos criterios como el que sea conocido por alguien que no debe conocerlo, los perjuicios que causa el hecho que este dañado o que no se pueda utilizar, otro factor importante es su valor de reposición.

Tabla 6. Valor de Activos.

Valor de Activos en Millones de Pesos ($)		
DESCRIPCION	**CONVENCION**	**VALOR**
Muy alto	MA	> 200
Alto	AL	100 - 200
Medio	MD	50 - 100
Bajo	BJ	10 - 50
Muy bajo	MB	1 - 10

Fuente: El Autor

Vulnerabilidad

Cuando se habla de vulnerabilidad se refiere directamente a la posibilidad que tiene una amenaza en materializarse sobre un determinado activo, este cálculo se realiza con períodos de un año (365 días).

Los valores de la vulnerabilidad resultan de dividir el número de semanas entre los días del año, este cálculo genera un valor que será teniendo en cuenta más adelante.

En la tabla siguiente, se resume la explicación anterior.

Tabla 7.Frecuencia Vulnerabilidades.

Frecuencia Vulnerabilidades		
VULNERABILIDAD	**CONVENCION**	**VALOR**
Extremadamente Frecuente	EF	1 - Una vez al día
Muy Frecuente	MF	0,7123 - Quincenal
Frecuente	FR	0,0164 - Bimestral
Poco Frecuente	PF	0,0054 - Semestral
Muy Poco Frecuente	MPF	0,0027 - Anual

Fuente: El Autor

Impacto

Se puede definir como la pérdida del activo cuantificado en porcentajes cuando ocurre un impacto sobre este.

Tabla 8. Impacto.

Impacto		
DESCRIPCION	**CONVENCION**	**Perdida en %**
Crítico	C	80 - 100
Alto	A	60 - 80
Medio	M	30 - 60
Bajo	B	5 -30

Fuente: El autor

Efectividad del control

Aquí se puede comprobar que tan efectivas son las medidas de protección de los riesgos. Se relaciona a continuación una tabla donde se asigna un valor dado en porcentaje de acuerdo a la descripción.

Tabla 9. Valoración Impacto/Vulnerabilidad.

Valoración Impacto/Vulnerabilidad	
DESCRIPCION	**VALOR**
Muy alto	95%
alto	75%
Medio	50%
Bajo	30%
Muy bajo	10%

Fuente: El autor.

Dimensiones de Valoración

En el libro de Magerit – Versión 3.0, libro II, indica que la dimensión es la característica que posee un activo, es decir el aspecto o apariencia que tiene este, los análisis de riesgos de un activo se pueden realizar sobre una faceta en particular, sin tener en cuenta otras.[8]

Algunas de estas características pueden ser la disponibilidad que tiene un activo para ser usado, también se puede hablar de la capacidad de que la información de un activo haya sido alterada sin su debida autorización, otra de las facetas que se contempla es la confidencialidad, refiriéndose a que un activo pueda ser utilizado sólo por personal autorizado, adicionalmente se encuentran la autenticidad, donde es necesarios demostrar que quien dice ser, es realmente, por último es necesario que quede constancia de las acciones realizadas y de eso se ocupa la trazabilidad.

En la siguiente tabla, se describen algunas de estas facetas, asignándole una letra a cada una de ellas.

[8] PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. Magerit V.3: Metodología de análisis y gestión de riesgos de los sistemas de información. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VfhKvvl_Oko

Tabla 10. Dimensiones de Valoración.

Identificación del Impacto	
A	Autenticidad
C	Confidencialidad
I	Integridad
D	Disponibilidad
T	Trazabilidad

Fuente: El autor.

En la siguiente tabla se clasifican los activos teniendo en cuenta la categoría a la cual pertenece.

Tabla 11. Clasificación de activos por tipo.

Tipos de Activos	
I	Instalaciones
H	Hardware
A	Aplicaciones
D	Datos
R	Redes
S	Servicios
P	Personal

5.3.4 **Análisis de Activos**

En esta etapa se identifican todos los activos que posee la organización, como son activos físicos, lógicos (Software), personal, instalaciones, entre otros, estos se valoraran de acuerdo a la tabla de valoración de activos

Tabla 12. Valoración de Activos.

Tipo de Activo	Descripción	Valor Activo	Valor en Millones de $	Criticidad
Personal	Personal Directivo	Muy alto	250	Crítico

Tabla 12. (Continuación)

Tipo de Activo	Descripción	Valor Activo	Valor en Millones de $	Criticidad
	Administradora	Alto	150	Crítico
	Jefes enfermería	Alto	90	Alto
	Personal barra de servicios	Alto	50	Bajo
	Auxiliares enfermería	Medio	50	Bajo
	Auxiliares laboratorio	Medio	50	Bajo
	Médicos Generales	Alto	50	Bajo
	Médicos especialistas	Alto	50	Alto
	Servicios generales	Medio	50	Bajo
	Contadora	Alto	100	Alto
	Asistente contable	Medio	50	Medio
	Revisor fiscal	Alto	100	Medio
	Secretaria gerencia	Medio	50	Bajo
	Secretaria asignación citas	Bajo	10	Bajo
	Ingeniero sistemas	Alto	100	Critico
	Bacteriólogas	Alto	100	Alto
	Mensajero	Alto	3	Muy bajo
	Auditores médicos	Alto	100	Alto
	Electro médico	Alto	100	Medio
	Electricista	Bajo	10	Bajo
	Mantenimiento	Bajo	10	Bajo
Hardware	Portátiles	Bajo	10	Medio
	Equipos de cómputo	Medio	50	Crítico
	Impresoras	Medio	40	Alto
	Servidor Aplicaciones	Muy Alto	200	Critico
Red	Acces point	Medio	50	Crítico
	Swichet	Medio	50	Crítico
	Routers	Medio	50	Crítico
	firewalls	Medio	50	Crítico
Instalación	cableado estructurado	Muy alto	250	Crítico
	Instalaciones eléctricas	Muy alto	250	Crítico
Servicios	Conectividad a internet	Muy alto	250	Crítico
Equipamiento Auxiliar	Planta eléctrica	Medio	60	Bajo
Software o aplicación	Windows server 2010	Medio	50	Crítico
	CgUno	Medio	50	Alto
	Windows	Medio	50	Alto
	Ofimática	Bajo	10	Muy bajo

Tabla 12. (Continuación)

Tipo de Activo	Descripción	Valor Activo	Valor en Millones de $	Criticidad
Activo de información	Contratos de trabajo personal	Bajo	10	Bajo
	Pólizas mantenimiento	Bajo	10	Bajo
	BD usuarios EPS	Medio	50	Crítico
	BD proveedores	Medio	50	Crítico
	contabilidad	Muy alto	200	Crítico
	Mercadeo	Alto	100	Medio

Fuente: El autor.

5.3.5 **Análisis de amenazas**

Las amenazas son consideradas como todas las posibles situaciones que pueden ocasionar problemas de seguridad, las amenazas se clasifican en cuatro grupos como son: Desastres naturales, de origen industrial, errores y fallos no intencionados y ataques intencionados. [9]

A continuación se relaciona una tabla donde se describen cada una de las amenazas, relacionando la dimensión, según (Tabla 10) y los activos afectados, según (Tabla 11)

Tabla 13. Amenazas.

GRUPO	AMENAZA	Dimensión Afectada					Activos Afectados						
		A	C	I	D	T	I	H	A	D	R	S	P
Desastres Naturales	Fuego				X		X	X					
	Daños por agua				X		X	X					
	Contaminación				X		X	X		x			
	Siniestro mayor				X		X	X		x			
	fenómeno climático				X		X	X		x			

[9] PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. Magerit V.3: Metodología de análisis y gestión de riesgos de los sistemas de información. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VfhKvvl_Oko

Tabla 13. (Continuación)

GRUPO	AMENAZA	Dimensión Afectada					Activos Afectados						
		A	C	I	D	T	I	H	A	D	R	S	P
	Fenómeno de origen volcánico				X		X	X		x			
	Fenómeno meteorológico				X		X	X		x			
	Inundación				X		X	X		x			
	Otros desastres Naturales				X		X	X					
Desastres de Origen Industrial	Fuego				X		X	X					
	Daños por agua				X		X	X					
	Contaminación Mecánica				X			X					
	Contaminación electromagnética				X			X					
	Avería de origen físico o lógico				X			X	X				
	Corte del suministro eléctrico				X			X					
	Condiciones inadecuadas de temperatura o humedad				X			X					
	Fallo de servicios de comunicaciones				X						X		
	Interrupción de otros servicios y suministros esenciales				X					X			
	Degradación de los soportes de almacenamiento de la información				X					X			
	Emanaciones electromagnéticas Errores y fallos no intencionados		x				X	X					
Errores y fallos no intencionados	Errores de los usuarios		X	X	X				X	X		x	
	Errores del administrador		X	X	X			X	X	X	X	X	
	Errores de monitorización (log)			X		X				X			
	Errores de configuración			X						X			
	Deficiencias en la organización				X								X
	Difusión de software dañino		X	X	X				X				
	Errores de [re-]encaminamiento		X						X		X	X	
	Errores de secuencia			X					X		X	X	
	Escapes de información		X							X			
	Alteración accidental de la información			X			x		X	X	X	X	
	Destrucción de información				X		x		X	X	X	X	
	Fugas de información		X				x		X	X	x	X	X
	Vulnerabilidades de los programas (software)		X	X	X				X				
	Errores de mantenimiento / actualización de programas (software)			X	X				X				
	Errores de mantenimiento / actualización de equipos (hardware)				X			X					
	Caída del sistema por agotamiento de recursos				X			X	X		X		
	Pérdida de equipos		X		X			X					
	Indisponibilidad del personal				X								X
ataques intencionados	Manipulación de los registros de actividad (log)			X		X				X			

Tabla 13. (Continuación)

GRUPO	AMENAZA	Dimensión Afectada					Activos Afectados						
		A	C	I	D	T	I	H	A	D	R	S	P
	Manipulación de la configuración	X	X	X						X			
	Suplantación de la identidad del usuario	x	X	X	X			X	X	X	X	X	
	Abuso de privilegios de acceso		X	X	X			X	X	X	X	X	
	Uso no previsto		X	X	X			X	X	X	X	X	
	Difusión de software dañino		X	X	X				X				
	[Re-]encaminamiento de mensajes		X						X		X	X	
	Alteración de secuencia			X					X		X	X	
	Acceso no autorizado		X	X			X	X	X	X	X	X	
	Análisis de tráfico		X								X		
	Repudio			X		X				X		X	
	Interceptación de información (escucha)		X								X		
	Modificación deliberada de la información			X				X	X	X	X	X	
	Destrucción de información				X				X	X	X	X	
	Divulgación de información		X						X	X	X	X	
	Manipulación de programas		X	X	X				X				
	Manipulación de los equipos		X		X			X					
	Denegación de servicio				X			X	X	X	X	X	
	Robo		X		X			X		X			
	Ataque destructivo				X		X	X					
	Ocupación enemiga		X		X		X						
	Indisponibilidad del personal				X								X
	Extorsión		X	X	X								X
	Ingeniería social		X	X	X								X

Cuantificación de amenazas

La cuantificación de las amenazas se realiza teniendo en cuenta la frecuencia con que se presenta esta en cada activo, el valor se toma de la tabla frecuencia de vulnerabilidades, donde se da un valor dependiendo de la frecuencia con que ocurre, estos pueden ser diarios, quincenales, bimestrales, semestrales o anuales, luego se le asigna un porcentaje de acuerdo a los valores asignados en la tabla impacto, es decir se asigna un porcentaje si el impacto sobre el activo es muy alto, alto, medio, bajo o muy bajo, estos porcentajes se asignan sobre las características del activo, como son autenticidad, confidencialidad, integridad, disponibilidad y por último trazabilidad. (Véase el anexo D).

5.3.6 **Resultado de vulnerabilidades**

El análisis de las vulnerabilidades se realizó haciendo uso de diferentes técnicas como observación, entrevistas, pruebas de penetración, utilizando

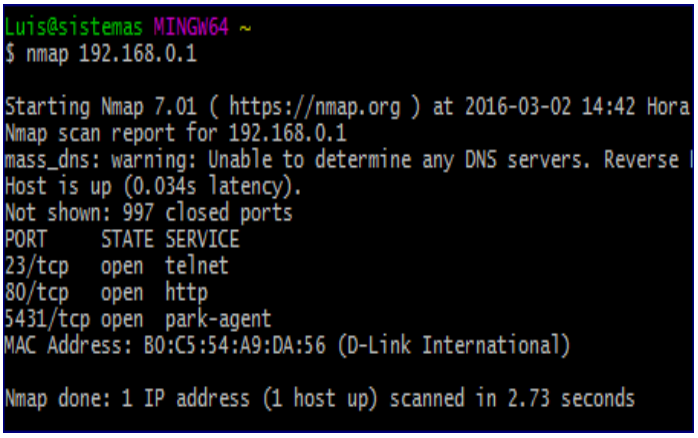
herramientas de software especializadas para el este tipo de análisis, se optó por la utilización de herramientas de distribución libre como Nmap, TheHarvester, DNSenum; Wireshark, Mozilla Firefox.

La primera tarea fue realizar un escaneo de puertos, en este caso se utilizó la herramienta Nmap.

Nmap: es una herramienta de código abierto especializada es escaneo de puertos de una red

Se realiza escaneo de puertos a la red de Servidoc S.A. el resultado obtenido es que los puertos 23, 80 y 5431 se encuentran abiertos, indicando vulnerabilidades de puertos en la red de la organización tal como se muestra en la siguiente imagen.

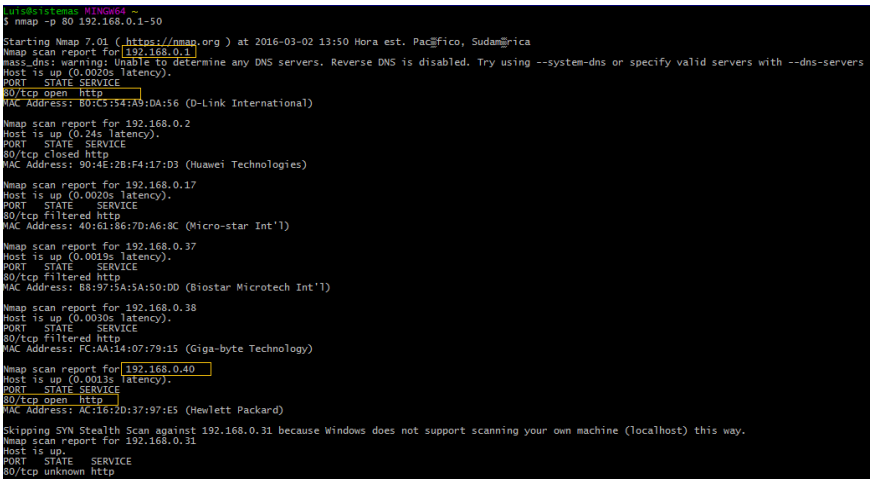
Figura 25. Puertos abiertos



Fuente. El Autor

Ahora se realiza escaneo específicamente al puerto 80, encargado de correr los servicios http, el rango de direcciones corresponde al área de contabilidad. Al ejecutar el programa Nmap se muestran vulnerabilidades, indicando que el puerto 80 se encuentra abierto para la direcciones 192.168.0.1 y 192.168.0.40 como se muestra en la siguiente imagen, adicionalmente indica que hay un dispositivo móvil (Huawei) conectado a la red, permitiendo vulnerabilidades de uso inadecuado de los recursos de la red, esto se puede apreciar en la siguiente imagen

Figura 26. Escaneo de puertos con direcciones IP



Fuente. El autor

También se realizó un análisis de vulnerabilidades a la URL del sitio web de la compañía, en este caso se hizo con la herramienta TheHarvester

TheHarvester: es una herramienta Linux, que busca información de una URL como cuentas de correo electrónico, subdominios que posee, puertos abiertos, entre otros, los datos son obtenidos de fuentes como motores de búsqueda, información de la red LinkedIn, de la base de datos Shodan, servidores PGP.

Se ejecutara TheHarvester a la URL ***servidocips.com***

Figura 27. Escaneo a página web de la organización

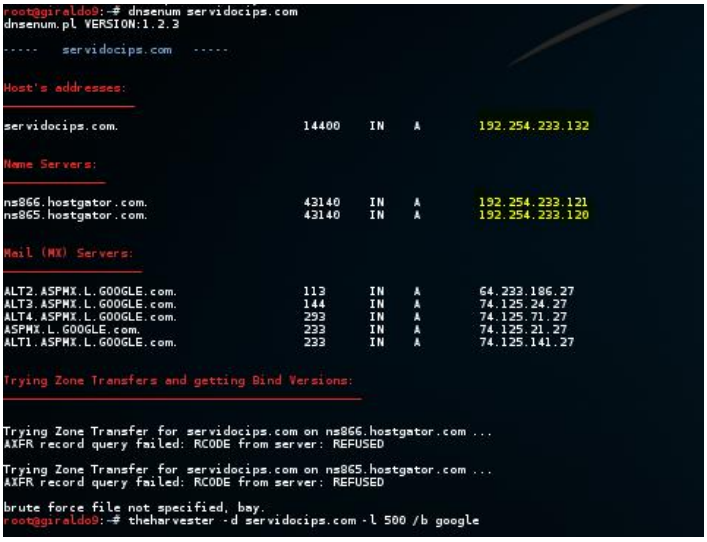
Fuente. El Autor

El resultado obtenido después de ejecutar la herramienta es la cuenta de correo electrónico de Servidoc, y la dirección del host.

Otra herramienta utilizada fue DNSenum.

DNSenum: Permite buscar información DNS, en este caso se obtuvo el nombre del host y los servidores que maneja, adicionalmente sus direcciones IP y el puerto que utiliza.

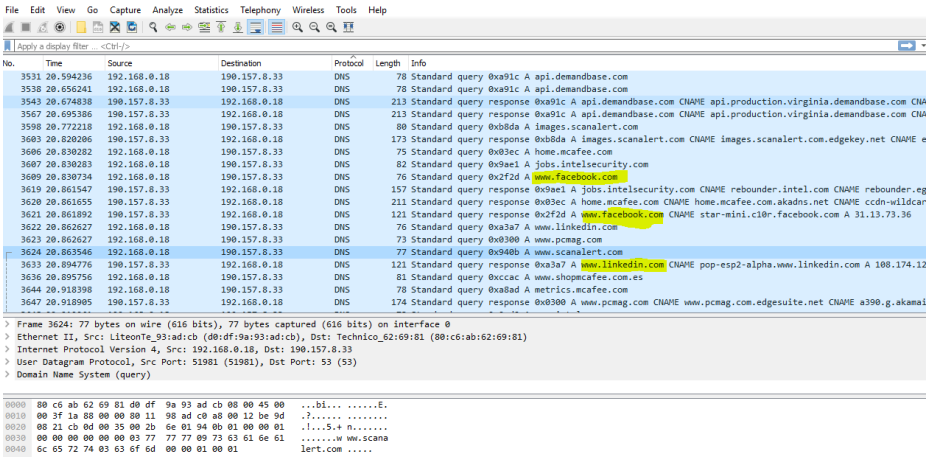
Figura 28. Escaneo DNS a Servidocips.com



Fuente. El Autor

Con **Wireshark**, quien se encarga de analizar de forma exhaustiva el tráfico de la red y permitir filtrado de los diferentes protocoles, se realizó un escaneo a la red, identificando que existe navegación en páginas como Facebook, linkedin, YouTube, reproducciones de páginas web de novelas como RCN y CARACOL NOVELAS.
El uso de redes sociales es una de las grandes vulnerabilidades que poseen las organizaciones, otro factor preocupante es el uso de páginas de streaming video, que además de consumir los recursos del ancho de banda, representan vulnerabilidades.

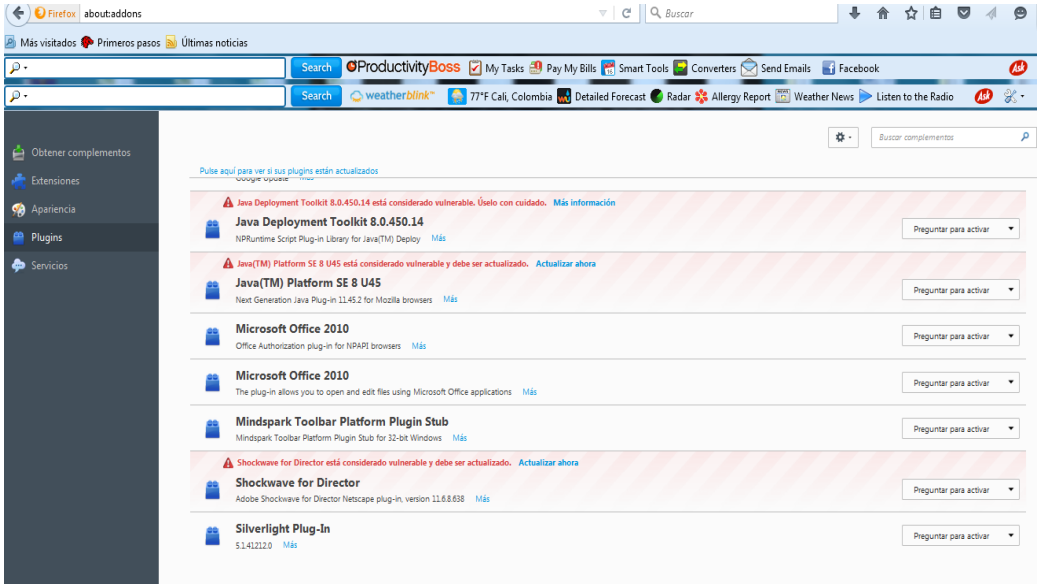
Figura 29. Monitoreo de red



Fuente. El autor

Además del uso de las herramientas Linux descritas anteriormente, se realizó un análisis muy sencillo a una de las estaciones de contabilidad, este consistió en consultar la configuración de los complementos del navegador Mozilla Firefox, arrojando como resultado que hay software desactualizado, convirtiéndose así en un equipo vulnerable ante ataques, tal como lo muestra la siguiente imagen las líneas de color rojo

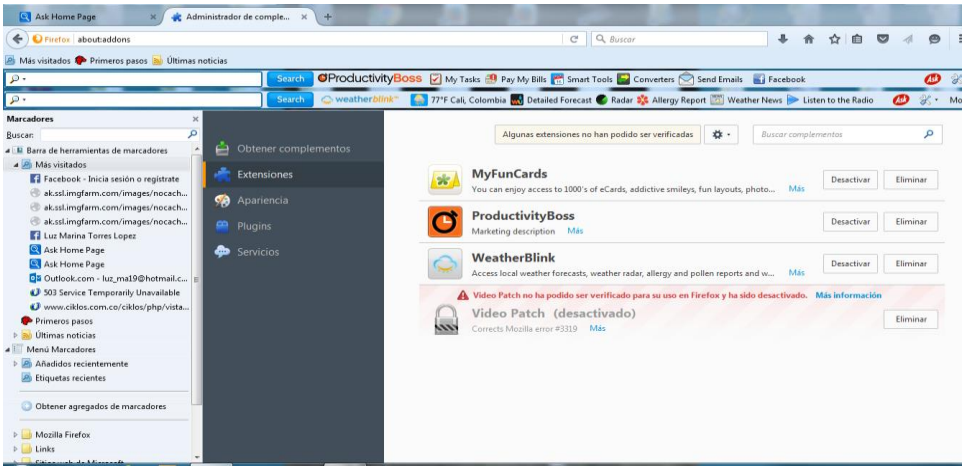
Figura 30. Análisis de software desactualizado



Fuente. El autor

En otro análisis, se identificó que el navegador posee barras de herramientas de publicidad que podrían llegar a ser virus, en este caso se observa MyFunCards.
Con este hallazgo, se puede concluir que los usuarios pueden realizar descargas de software sin ningún control, esto representa grandes vulnerabilidades para Servidoc S.A., demás se puede observar que entre los lugares más visitados se encuentra la página www.facebook.com.

Figura 31. Software instalado no autorizado



Fuente. El autor

Después de aplicar las técnicas descritas anteriormente, se detalla en la siguiente tabla cada una de las vulnerabilidades que posee la organización, se han organizado por grupo de amenazas como son desastres naturales, desastres de origen industrial, errores y fallos no intencionados y ataques intencionados.

Tabla 14. Vulnerabilidades

Origen	Amenazas	Vulnerabilidades
Desastres Naturales	Daños por agua	Falta de controles físicos como detectores de humedad
	Fuego	Falta de controles físicos contra incendio.

Tabla 14. (Continuación)

Origen	Amenazas	Vulnerabilidades
	Avería de origen físico o lógico	Falta de controles físicos y lógicos como mantenimiento preventivo de hardware y software.
Desastres de Origen Industrial	Condiciones inadecuadas de temperatura o humedad	No existen dispositivos de control de humedad
	Contaminación electromagnética	Falta de controles físicos
	Contaminación Mecánica	Falta de mantenimiento preventivo periódico
	Corte del suministro eléctrico	Falta de tablero de transferencia automática
	Degradación de los soportes de almacenamiento de la información	Falta de controles físicos preventivos a los medios de almacenamiento
	Fallo de servicios de comunicaciones	Falta de equipos de comunicación que garanticen la continuidad del servicio
	8nterrupción de otros servicios y suministros esenciales	No existen políticas sobre los suministros que deben permanecer en stock para asegurar la continuidad del servicio
	Otros desastres Naturales	Falta de pólizas con cobertura de desastres naturales
Errores y fallos no intencionados	Alteración accidental de la información	No existen políticas adecuadas de verificación de información y almacenamiento de ella.
	Caída del sistema por agotamiento de recursos	Falta de controles que permitan medir la capacidad de los recursos físicos y lógicos
	Deficiencias en la organización	No hay una definición clara de responsabilidades en materia de seguridad informática, no existe un procedimiento claro sobre a quien se deben reportar los incidentes relacionados con seguridad informática

Tabla 14. (Continuación)

Origen	Amenazas	Vulnerabilidades
	Destrucción de información	Falta de controles de ingreso a las instalaciones y zonas restringidas, no existen controles criptográficos, falta de políticas de copias de seguridad y almacenamiento de la información.
	Errores de configuración	Falta de procedimientos que permitan monitorizar la adecuada configuración de los activos de la organización.
	Errores de los usuarios	Falta de políticas claras sobre el manejo adecuado de los recursos.
	Errores de mantenimiento / actualización de equipos (hardware)	Falta de controles de mantenimiento preventivo y periódico a los dispositivos
	Errores de secuencia	Falta de controles físicos
	Errores del administrador	Falta de capacitación al personal
	Escapes de información	No existen procedimientos sobre el manejo adecuado de información confidencial.
	Indisponibilidad del personal	Falta de capacitación y concientización de los empleados.
	Pérdida de equipos	Falta de controles de acceso a las instalaciones
Ataques intencionados	[Re-]encaminamiento de mensajes	No existen controles sobre el uso de cuentas de correo electrónico ni de acceso a la red, Falta de controles sobre el uso de redes sociales, chat, foros.
	Abuso de privilegios de acceso	Falta de asignación de perfiles de acuerdo al rol que desempeñan para el desarrollo de las actividades, situación que permite que los usuarios tengan acceso total a la información, generando
	Acceso no autorizado	Falta de políticas de acceso a la información e instalaciones de la empresa, configuración inadecuada de equipos de comunicación.

Tabla 14. (Continuación)

Origen	Amenazas	Vulnerabilidades
	Análisis de tráfico	Falta de controles que permitan un monitoreo constante del tráfico que viaja por la red
	Ataque destructivo	Falta de vigilancia de las instalaciones, no se cuenta con pólizas que tengan cobertura por daños a las instalaciones o equipos informáticos
	Denegación de servicio	Falta de controles físicos y lógicos que permitan la continuidad del servicio
	Divulgación de información	Falta de controles que permitan un procedimiento adecuado contra la revelación de información de la empresa
	Extorsión	Falta de políticas que definan un procedimiento a seguir ante vulnerabilidades de este tipo
	Ingeniería social	Falta de capacitación del personal en aspectos relacionados a seguridad informática.
	Manipulación de la configuración	Falta de controles de privilegios de usuarios y configuraciones
	Manipulación de los equipos	Falta de controles sobre el uso adecuado de los recursos y políticas de confidencialidad de la información
	Modificación deliberada de la información	Falta de políticas sobre el uso adecuado e integridad de la información
	Repudio	Falta de controles que permitan monitorear el desarrollo de las actividades
	Robo	Falta de controles de acceso a las instalaciones, no existen políticas del uso seguro de medios de almacenamiento y soportes en papel.
	Suplantación de la identidad del usuario	Falta de privilegios de acceso al sistema y a las redes
	Uso no previsto	Falta de políticas que prohíban el uso de los activos de la organización para fines personales

Fuente: El autor.

5.3.7 **Impacto potencial**

El impacto potencial hace referencia a la cuantificación que se asigna al daño al que puede ser sometido un activo, esto se da cuando una amenaza se materializa.

Para realizar el cálculo, se tomó el valor del activo, se multiplico por el valor asignado a la frecuencia que se estableció anteriormente (valor asignado de acuerdo a días, quincenal, bimestral, semestral, anual) y finalmente se multiplica por el mayor valor de la dimensión afectada.

De acuerdo a los resultados arrojados, la organización considera que el nivel aceptable del riesgo será para valores inferiores a $ 200.000, lo que significa que cualquier activo que se encuentre por encima de este valor, será necesario aplicarle salvaguardas. (véase el Anexo E).

5.3.8 **Riesgo residual**

Después de haber identificado las amenazas que superaban el nivel de riesgo que estableció la empresa, se establecen algunos controles que permitirán mitigar el riesgo identificado, es de aclarar que estos riesgos pueden ser por el impacto que producen sobre el activo o por la ocurrencia, el cálculo se detalla a continuación, donde se incluye una columna llamada descripción de salvaguarda, en esta se encuentra plasmada la solución que puede mitigar el riesgo, la siguiente columna muestra el porcentaje al que se puede disminuir el riesgo, para finalmente tener una nueva cuantificación que resulta del 100% menos él % de reducción del riego por el valor calculado en la columna Frecuencia * Impacto * Valor.

Una vez cuantificado nuevamente el riesgo, se observa que los controles quedan por debajo del valor límite establecido, esta cuantificación indica que los controles que han sido sugeridos son adecuados. (véase el Anexo F).

5.4 **FASE 4: PROPUESTA DE PROYECTOS**

Una vez culminada la etapa anterior donde se identificaron los riesgos, es necesario el planteamiento de proyectos que ayuden a la organización a poder alcanzar el nivel de seguridad deseado cumpliendo con disponibilidad, integridad y confidencialidad de la información.

Objetivo de los proyectos
Los proyectos presentados a la compañía Servidoc S.A. tienen como propósito:

- Llevar los riesgos que han sido identificados en la etapa anterior a un nivel aceptable.
- Concientizar a la empresa en el uso de mejores prácticas de la seguridad de la información.
- Permitirle a la organización estar preparada ante situaciones que afecten la continuidad del negocio.

Alcance

Los proyectos tienen como propósito dar solución a las vulnerabilidades encontradas en el análisis de riesgos, estos proyectos se relacionan directamente con los activos de la empresa los cuales pueden ser tecnología, información, recursos humanos, procesos, entre otros.

Tipos de proyectos

Según PEREIRA, Hose Aurela (2.013) los proyectos se agrupan en tres categorías como son:

- Mitigación de riesgos asociados a desastres de origen natural o industrial.
- Mitigación del riesgo asociado a ataques intencionados.
- Mitigación del riesgo asociado a errores no intencionados.

5.4.1 Mitigación de riesgos asociados a desastres de origen natural o industrial.

Con la implementación de este proyecto se establecerán bases firmes para proteger la organización ante vulnerabilidades de seguridad física y ambiental.

Objetivos: Con la adopción de este proyecto la organización estará en capacidad de:

- Concientizar al personal de la compañía sobre lo importante que es la protección y prevención de incidentes de este tipo.
- Conocer la importancia de tener asegurada la compañía mediante pólizas con cobertura de desastres de origen natural o industrial.

- Realizar mantenimientos periódicos de tipo preventivo y correctivo a dispositivos de control físico y ambiental.
- Contar con un equipo humano que esté capacitado para afrontar eventualidades o desastres de tipo natural o industrial.

Beneficios: Con este proyecto se reforzará la organización en cuanto a seguridad física y ambiental, además se definirán procedimientos que se deben llevar a cabo cuando se presenten amenazas de esta índole, otro de los factores importantes que trae este proyecto es poder establecer mecanismos de medición que aportaran directamente a la mejora continua.

Alcance: El alcance de este proyecto son las instalaciones de Servidoc S.A. y los dispositivos de hardware.

Fases: Para el desarrollo de este proyecto se deben seguir las siguientes fases:

- **Evaluación del estado actual:** Esta fase permite identificar cuáles son los controles que tiene implementados la organización, dará un diagnóstico de su estado actual, además identificará los equipos que hagan falta y deban ser adquiridos ya sea por modalidad de compra, comodato, leasing, además se definirán los procedimientos que se deben desarrollar para su puesta en funcionamiento.

- **Establecer acuerdos con terceros:** Esta fase se realiza una vez se han tomado medidas respecto a la adquisición de los equipos, paso seguido se deben realizar acuerdos con terceros en lo que se refiere a: acuerdos de servicios como periodicidad del mantenimiento de los equipos, consecución de pólizas con cobertura de desastres naturales e industriales, obtención de datos de las personas de contacto, contacto con las autoridades, en este caso autoridades como bomberos y policía.

- **Estructuración de procedimientos:** Se establecerán procedimientos que permitirán llevar a cabo cada una de las tareas que contempla este proyecto, dentro de los procedimientos que se contemplan están: procedimientos de entrenamientos, de configuración de equipos, registro detallado de cada uno de los eventos presentados, establecimiento de métricas, pruebas de equipos.
- **Ejecución de trabajos:** Es aquí donde el personal seleccionado en una de las fases anteriores realiza la instalación y configuración de los equipos.

- **Pruebas:** Para realizar las pruebas es necesario crear escenarios para probar el correcto funcionamiento de los equipos.

- **Entrenamiento:** Se entrenará al personal encargado de la realización del monitoreo de equipos, además se entregará información para concientizar

al personal de la compañía sobre los equipos instalados, es de vital importancia capacitar al personal sobre la realización prácticas que activen los equipos, generando falsas alarmas.

- **Puesta en marcha:** Una vez culminadas todas las fases anteriores, se procede con la formalización de la puesta en marcha de los equipos instalados.

- **Reporte:** Se presentan los resultados del análisis para la implementación del proyecto a la alta gerencia.

El tiempo estimado para implementar este proyecto es de 2 meses.

Los costos estimados para este proyecto contemplando recurso humano y equipos son de $ 26.000.000

5.4.2 **Mitigación de riesgos asociados a ataques intencionados**

Con la implementación de este proyecto se establecerán bases firmes para proteger la organización ante ataques intencionados de seguridad física y lógica de los activos, estos ataques pueden ser realizados por personas ajenas a la organización o por empleados internos.

Objetivos: Con la adopción de este proyecto la organización estará en capacidad de:

- Concientizar al personal de la compañía sobre la importancia que representa la protección y prevención de incidentes de este tipo.
- Conocer la importancia de tener asegurada la compañía mediante pólizas con cobertura de robos ataques destructivos.
- Realizar mantenimientos preventivos y correctivos a dispositivos de control físico.
- Contar con un equipo humano que esté capacitado para afrontar eventualidades y se puedan implementar planes de contingencia.
- Realizar seguimiento y monitoreo a los equipos de cómputo, software e instalaciones.

Beneficios: Con este proyecto se reforzará la organización en cuanto a seguridad física y lógica, además se definirán procedimientos que se deben llevar a cabo cuando se presenten amenazas de esta índole, otro de los factores importantes que trae este proyecto poder establecer mecanismos de medición que aportaran directamente a la mejora continua, estos controles transmitirán confianza tanto a los clientes internos y externos de la organización.

Alcance: El alcance de este proyecto son las instalaciones de Servidoc S.A. y los dispositivos de hardware, software y servicios que presta la compañía.

Fases: Para el desarrollo de este proyecto se deben seguir las siguientes fases:

- **Evaluación del estado actual:** Esta fase permite identificar cuáles son los controles que tiene implementados la organización, dará un diagnóstico de su estado actual, además identificará los elementos físicos o lógicos que hagan falta y deban ser adquiridos, además se definirán los procedimientos que se deben desarrollar para su puesta en funcionamiento.

- **Establecer acuerdos con terceros:** Esta fase se realiza una vez se han tomado medidas respecto a la fase anterior, paso seguido se deben realizar acuerdos con terceros en lo que se refiere a: acuerdos de servicios como periodicidad del mantenimiento de los equipos, consecución de pólizas con cobertura de robo, ocupación enemiga, obtención de datos de las personas de contacto.

- **Estructuración de procedimientos:** Se establecerán procedimientos que permitirán llevar a cabo cada una de las tareas que contempla este proyecto, dentro de los procedimientos que se contemplan están: procedimientos de entrenamiento, de configuración de equipos, registro detallado de cada uno de los eventos presentados, establecimiento de métricas, pruebas de equipos.

- **Ejecución de trabajos:** Es aquí donde el personal seleccionado en una de las fases anteriores realiza la instalación y configuración de los equipos y programas.

- **Pruebas:** Para realizar las pruebas es necesario crear escenarios para probar el correcto funcionamiento de los equipos y programas.

- **Entrenamiento:** Se entrenará al personal encargado de la realización del monitoreo de equipos y software, además se entregará información para concientizar al personal de la compañía sobre los equipos y programas instalados, es de vital importancia capacitar al personal sobre los elementos instalados.

- **Puesta en marcha:** Una vez culminadas todas las fases anteriores, se procede con la formalización de la puesta en marcha de los equipos y programas instalados.

- **Reporte:** Se presentan los resultados del análisis para la implementación del proyecto a la alta gerencia.

El tiempo estimado para la realización de este proyecto es de 2 meses.

Los costos estimados para este proyecto contemplando recurso humano y equipos son de $ 15.000.000

5.4.3 **Mitigación del riego asociado a errores no intencionados**

Con la implementación de este proyecto se establecerán bases firmes para proteger la organización ante errores no intencionados de seguridad física y lógica de los activos, estos ataques pueden ser realizados por personas ajenas a la organización o por empleados internos.

Objetivos: Con la adopción de este proyecto la organización estará en capacidad de:

- Concientizar al personal de la compañía sobre la importancia que representa la protección y prevención de incidentes de este tipo.
- Conocer la importancia de tener asegurada la compañía mediante pólizas con cobertura perdida y daño de equipos.
- Realizar mantenimientos preventivos y correctivos a dispositivos de hardware y software.
- Contar con un equipo humano que esté capacitado para afrontar eventualidades y se puedan implementar planes de contingencia.
- Realizar seguimiento y monitoreo a los equipos de cómputo, software e instalaciones.
- Contar con sistemas de protección de perdida de datos DLP.
- Contar con un sistema de protección antivirus en todos los equipos de cómputo y servidores.
- Contar con políticas de configuración de equipos y perfiles de usuario.

Beneficios: Con este proyecto se reforzará la organización en cuanto a seguridad física y lógica, además se establecerán una serie de procedimientos que se deben llevar a cabo cuando se presenten amenazas de esta índole, otro de los factores importantes que trae este proyecto poder establecer mecanismos de medición que aportaran directamente a la mejora continua, estos controles transmitirán confianza tanto a los clientes internos y externos de la organización.

Alcance: El alcance de este proyecto son las instalaciones de Servidoc S.A. y los dispositivos de hardware, software y servicios que presta la compañía.

Fases: Para el desarrollo de este proyecto se deben seguir las siguientes fases:

- **Evaluación del estado actual:** Esta fase permite identificar cuáles son los controles que tiene implementados la organización, dará un diagnóstico de su estado actual, además identificará los elementos físicos o lógicos que hagan falta y deban ser adquiridos, además se definirán los procedimientos que se deben desarrollar para su puesta en funcionamiento.

- **Establecer acuerdos con terceros:** Esta fase se realiza una vez se han tomado medidas respecto a la fase anterior, paso seguido se deben realizar acuerdos con terceros en lo que se refiere a: acuerdos de servicios como periodicidad del mantenimiento de los equipos, consecución de pólizas con cobertura de robo, ocupación enemiga, obtención de datos de las personas de contacto.

- **Estructuración de procedimientos:** Se establecerán procedimientos que permitirán llevar a cabo cada una de las tareas que contempla este proyecto, dentro de los procedimientos que se contemplan están: procedimientos de entrenamiento, de configuración de equipos, registro detallado de cada uno de los eventos presentados, establecimiento de métricas, pruebas de equipos.

- **Ejecución de trabajos:** Es aquí donde el personal seleccionado en una de las fases anteriores realiza la instalación y configuración de los equipos y programas.

- **Pruebas:** Para la realización de las pruebas es necesario crear escenarios para probar el correcto funcionamiento de los equipos y programas.

- **Entrenamiento:** Se entrenará al personal encargado de la realización del monitoreo de equipos y software, además se entregará información para concientizar al personal de la compañía sobre los equipos y programas instalados, es de vital importancia capacitar al personal sobre los elementos instalados.
- **Puesta en marcha:** Una vez culminadas todas las fases anteriores, se procede con la formalización de la puesta en marcha de los equipos y programas instalados.

- **Reporte:** Se presentan los resultados del análisis para la implementación del proyecto a la alta gerencia.

El tiempo estimado para la realización de este proyecto es de 1 mes.

Los costos estimados para este proyecto contemplando recurso humano y equipos son de $ 16.000.000

5.5 **FASE 5. AUDITORIA DE CUMPLIMIENTO**

5.5.1 **Metodología**

En esta etapa se evalúa cual es el cumplimiento que tiene la organización en cuanto a seguridad informática, para realizar este análisis se tomara cada uno de los controles que contempla la norma ISO/IEC 27001:2013 y se evaluará el cumplimiento de cada uno de ellos por parte de la compañía.

Cabe resaltar que a lo largo del desarrollo de este trabajo, se han establecido algunas acciones de mejora en algunos controles, lo que significa que el estado de madurez que se realizó inicialmente ha cambiado, pero a su vez es necesario realizar la auditoria de cumplimiento para identificar las falencias que se tienen y cuáles son las oportunidades de mejora.

Al finalizar esta etapa, se debe presentar un informe del estado actual con sus respectivas conclusiones

Para la evaluación de cada uno de los controles que contempla la norma ISO/IEC 27001:2013, se debe tener en cuenta la siguiente tabla, donde se podrán encontrar cada una de las convenciones.

Tabla 15. Convenciones nivel de cumplimiento.

Valor	Nombre	Porcentaje	Descripción
0	No existente	0%	No existe evidencia del estándar o practica en la compañía.
1	Inicial	10%	La organización tiene practicas hechas a la medida pero inconsistentes.
2	Repetible	40%	La organización tiene un enfoque coherente pero no documentado.
3	Definido	50%	Se tiene un enfoque coherente y documentado pero no medido.
4	Administrado	80%	Los procesos son medidos frecuente mente y se realizan mejoras.
5	Optimizado	100%	La organización ha refinado su cumplimiento con el nivel de las mejores prácticas
6	No Aplica	N/A	El control no es aplicable a la compañía

Fuente: El autor.

Los cálculos se efectuaran teniendo en cuenta el nivel de cumplimiento en cada control cuantificando cada uno de ellos según la tabla anterior, este

procedimiento se realizara para cada uno de los dominios que estable la norma, estos son:

- Políticas de seguridad de la información.
- Organización de la seguridad de la información.
- Seguridad de los recursos humanos.
- Gestión de activos.
- Control de acceso.
- Criptografía.
- Seguridad física y del entorno.
- Seguridad de las operaciones.
- Seguridad de las comunicaciones.
- Adquisición, desarrollo y mantenimientos de sistemas.
- Relación con los proveedores.
- Gestión de incidentes de seguridad de la información.
- Aspectos de seguridad de la información de la gestión de continuidad de negocio.
- Cumplimiento.

La compañía considera que el porcentaje de cumplimiento que se debe alcanzar es el 80%.

5.5.2 **Evaluación de cumplimiento**

A continuación se evalúa el estado de cumplimiento de cada uno de los controles que contempla la norma ISO/IEC 27001:2013, se evalúa su estado de madurez para ello es necesario regirse al modelo de madurez de la capacidad (CMM), con la aplicación de este modelo se evidenciara el cumplimiento que tiene la compañía respecto a la norma.

En la siguiente tabla se encuentran cada uno de los dominios con sus respectivos controles, además se ha incluido una columna llamada efectividad, donde se mostrara el nombre asignado de acuerdo a la tabla convenciones de nivel de cumplimiento, adicionalmente se encuentra la columna efectividad dada en porcentajes, resultado asignado de acuerdo al nombre de la columna anterior.

Los controles que se encuentran en color amarillo indican que han logrado un gran nivel de madurez, pues durante este análisis se han implementado controles, es el del documento de políticas de la seguridad y la información y el documento de asignación de roles y responsabilidades

Tabla 16. Modelo de madurez y la capacidad (CMM).

	Control/Objetivo de Control		N - C	Descripción	cumple/ no cumple	Porcentaje
5	Políticas de seguridad de la información					**80%**
5.1	Directrices establecidas por la dirección para la seguridad de la información					
5.1.1	Políticas para la seguridad de la información	Seguridad	4	Administrado	Si	80%
5.1.2	Revisión de las políticas para seguridad de la información	Seguridad	4	Administrado	si	80%
6	Organización de la seguridad de la información					**40%**
6.1	Organización interna					
6.1.1	Roles y responsabilidades para la seguridad de información	Seguridad	4	Administrado	si	80%
6.1.2	Separación de deberes	Seguridad	4	Administrado	si	80%
6.1.3	Contacto con las autoridades	Seguridad	0	No existente	no	0%
6.1.4	Contacto con grupos de interés especial	Seguridad	0	No existente	no	0%
6.1.5	Seguridad de la información en la gestión de proyectos	Seguridad	0	No existente	no	0%
6.2	Dispositivos móviles y teletrabajo					
6.2.1	Política para dispositivos móviles	Seguridad	4	Administrado	si	80%
6.2.2	Teletrabajo	Seguridad	6	No Aplica	no	N/A
7	Seguridad de los recursos humanos					**28%**
7.1	Antes de asumir el empleo					
7.1.1	Selección	Rh	3	Definido	si	**50%**
7.1.2	Términos y condiciones del empleo	Rh	2	Repetible	no	**40%**
7.2	Durante la ejecución del empleo					
7.2.1	Responsabilidades de la dirección	Rh	4	Administrado	si	80%
7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Rh	0	No existente	no	**0%**
7.2.3	Proceso disciplinario	Rh	0	No existente	no	**0%**
7.3	Terminación o cambio de empleo					
7.3.1	Terminación o cambio de responsabilidades de empleo	Rh	0	No existente	no	**0%**
8	Gestión de activos					**52%**

Tabla 16. (Continuación)

	Control/Objetivo de Control		N - C	Descripción	cumple/ no cumple	Porcentaje
8.1	Responsabilidad por los activos					
8.1.1	Inventario de activos	Rh	4	Administrado	si	80%
8.1.2	Propiedad de los activos	Rh	4	Administrado	si	80%
8.1.3	Uso aceptable de los activos	Rh	2	Repetible	no	40%
8.1.4	Devolución de activos	Rh	4	Administrado	si	80%
8.2	Clasificación de la información					
8.2.1	Clasificación de la información	Rh	2	Repetible	no	40%
8.2.2	Etiquetado de la información	Sistemas	2	Repetible	no	40%
8.2.3	Manejo de activos	Rh	2	Repetible	no	40%
8.3.1	Gestión de medios removibles	Sistemas	2	Repetible	no	40%
8.3.2	Disposición de los medios	Sistemas	2	Repetible	no	40%
8.3.3	Transferencia de medios físicos	Sistemas	2	Repetible	no	40%
9	Control de acceso					**31%**
9.1	Requisitos del negocio para control de acceso					
9.1.1	Política de control de acceso	Seguridad	4	Administrado	Si	80%
9.1.2	Política sobre el uso de los servicios de red	Seguridad	4	Administrado	Si	80%
9.2	Gestión de acceso de usuarios					
9.2.1	Registro y cancelación del registro de usuarios	Seguridad	2	Repetible	no	40%
9.2.2	Suministro de acceso de usuarios	Seguridad	2	Repetible	no	40%
9.2.3	Gestión de derechos de acceso privilegiado	Seguridad	2	Repetible	no	40%
9.2.4	Gestión de información de autenticación secreta de usuarios	Seguridad	2	Repetible	no	40%
9.2.5	Revisión de los derechos de acceso de usuarios	Seguridad	2	Repetible	no	40%
9.2.6	Retiro o ajuste de los derechos de acceso	Seguridad	2	Repetible	no	40%
9.3	Responsabilidades de los usuarios					
9.3.1	Uso de la información de autenticación secreta	Seguridad	0	No existente	no	0%
9.4	Control de acceso a sistemas y aplicaciones					
9.4.1	Restricción de acceso Información	Seguridad	0	No existente	no	0%
9.4.2	Procedimiento de ingreso seguro	Seguridad	0	No existente	no	0%
9.4.3	Sistema de gestión de contraseñas	Seguridad	0	No existente	no	0%

Tabla 16. (Continuación)

	Control/Objetivo de Control		N - C	Descripción	cumple/ no cumple	Porcentaje
9.4.4	Uso de programas utilitarios privilegiados	Seguridad	0	No existente	no	0%
9.4.5	Control de acceso a códigos fuente de programas	Seguridad	6	No Aplica	no	N/A
10	Criptografía					#¡DIV/0!
10.1	Controles criptográficos					
10.1.1	Política sobre el uso de controles criptográficos	Seguridad	6	No Aplica	no	N/A
10.1.2	Gestión de llaves	Seguridad	6	No Aplica	no	N/A
11	Seguridad física y del entorno					43%
11.1	Áreas seguras					
11.1.1	Perímetro de seguridad física	Seguridad Física	2	Repetible	no	40%
11.1.2	Controles físicos de entrada	Seguridad Física	2	Repetible	no	40%
11.1.3	Seguridad de oficinas, recintos e instalaciones	Seguridad Física	2	Repetible	no	40%
11.1.4	Protección contra amenazas externas y ambientales	Seguridad Física	2	Repetible	no	40%
11.1.5	Trabajo en áreas seguras	Seguridad Física	2	Repetible	no	40%
11.1.6	Áreas de despacho y carga	Seguridad Física	6	No Aplica	no	N/A
11.2	Equipos					
11.2.1	Ubicación y protección de los equipos	Seguridad Física	2	Repetible	no	40%
11.2.2	Servicios de suministro	Seguridad Física	2	Repetible	no	40%
11.2.3	Seguridad del cableado	Sistemas	2	Repetible	no	40%
11.2.4	Mantenimiento de equipos	Sistemas	2	Repetible	no	40%
11.2.5	Retiro de activos	Seguridad Física	2	Repetible	no	40%
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Sistemas	2	Repetible	no	40%
11.2.7	Disposición segura o reutilización de equipos	Seguridad Física	2	Repetible	no	40%
11.2.8	Equipos de usuario desatendidos	Sistemas	2	Repetible	no	40%
11.2.9	Política de escritorio limpio y pantalla limpia	Sistemas	4	Administrado	si	80%
12	Seguridad de las operaciones					28%
12.1	Procedimientos operacionales y responsabilidades					

Tabla 16. (Continuación)

	Control/Objetivo de Control		N - C	Descripción	cumple/ no cumple	Porcentaje
12.1.1	Procedimientos de operación documentados	sistemas	0	No existente	no	0%
12.1.2	Gestión de cambios	sistemas	0	No existente	no	0%
12.1.3	Gestión de capacidad	sistemas	0	No existente	no	0%
12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	sistemas	6	No Aplica	no	N/A
12.2	Protección contra códigos maliciosos					
12.2.1	Controles contra códigos maliciosos	sistemas	2	Repetible	no	40%
12.3	Copias de respaldo					
12.3.1	Respaldo de información	sistemas	2	Repetible	no	40%
12.4	Registro y seguimiento					
12.4.1	Registro de eventos	Sistemas	0	No existente	no	0%
12.4.2	Protección de la información de registro	Sistemas	2	Repetible	no	40%
12.4.3	Registros del administrador y del operador	Sistemas	2	Repetible	no	40%
12.4.4	sincronización de relojes	Sistemas	4	Administrado	si	80%
12.5	Control de software operacional					
12.5.1	Instalación de software en sistemas operativos	Sistemas	2	Repetible	no	40%
12.6	Gestión de la vulnerabilidad técnica					
12.6.1	Gestión de las vulnerabilidades técnicas	Sistemas	2	Repetible	no	40%
12.6.2	Restricciones sobre la instalación de software	Sistemas	2	Repetible	no	40%
12.7	Consideraciones sobre auditorias de sistemas de información					
12.7.1	Información controles de auditoría de sistemas	Sistemas	0	No existente	no	0%
13	Seguridad de las comunicaciones					**40%**
13.1	Gestión de la seguridad de las redes					
13.1.1	Controles de redes	Sistemas	2	Repetible	no	40%
13.1.2	Seguridad de los servicios de red	Sistemas	2	Repetible	no	40%
13.1.3	Separación en las redes	Sistemas	2	Repetible	no	40%
13.2	Transferencia de información					
13.2.1	Políticas y procedimientos de transferencia de información	Sistemas	2	Repetible	no	40%
13.2.2	Acuerdos sobre transferencia de información	Sistemas	2	Repetible	no	40%
13.2.3	Mensajería electrónica	Sistemas	2	Repetible	no	40%
13.2.4	Acuerdos de confidencialidad o de no divulgación	Sistemas	2	Repetible	no	40%

Tabla 16. (Continuación)

	Control/Objetivo de Control		N - C	Descripción	cumple/ no cumple	Porcentaje
14	Adquisición, desarrollo y mantenimientos de sistemas					**17%**
14.1	Requisitos de seguridad de los sistemas de información					
14.1.1	Análisis y especificación de requisitos de seguridad de la información	Sistemas	2	Repetible	no	40%
14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	Sistemas	2	Repetible	no	40%
14.1.3	Protección de transacciones de los servicios de las aplicaciones	Sistemas	2	Repetible	no	40%
14.2	Seguridad en los procesos de desarrollo y soporte					
14.2.1	Política de desarrollo seguro	Seguridad	6	No Aplica	no	N/A
14.2.2	Procedimientos de control de cambios en sistemas	Seguridad	6	No Aplica	no	N/A
14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Seguridad	6	No Aplica	no	N/A
14.2.4	Restricciones en los cambios a los paquetes de software	Seguridad	6	No Aplica	no	N/A
14.2.5	Principios de construcción de sistemas seguros	Seguridad	6	No Aplica	no	N/A
14.2.6	Ambiente de desarrollo seguro	Seguridad	6	No Aplica	no	N/A
14.2.7	Desarrollo contratado externamente	Seguridad	6	No Aplica	no	N/A
14.2.8	Pruebas de seguridad de sistemas	Seguridad	0	No existente	no	0%
14.2.9	Prueba de aceptación de sistemas	Seguridad	0	No existente	no	0%
14.3	Datos de prueba	Seguridad	0	No existente	no	0%
14.3.1	Protección de datos de prueba	Seguridad	0	No existente	no	0%
15	Relación con los proveedores					**11%**
15.1	Seguridad de la información en las relaciones con los proveedores	Seguridad	0	No existente	no	0%
15.1.1	Política de seguridad de la información para las relaciones con proveedores	Seguridad	4	Administrado	si	80%
15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Seguridad	0	No existente	no	0%
15.1.3	Cadena de suministro de tecnología de información y comunicación	Seguridad	0	No existente	no	0%
15.2	Gestión de la prestación de servicios con los proveedores	Seguridad	0	No existente	no	0%
15.2.1	Seguimiento y revisión de los servicios de los proveedores	Seguridad	0	No existente	no	0%

Tabla 16. (Continuación)

	Control/Objetivo de Control		N - C	Descripción	cumple/ no cumple	Porcentaje
15.2.2	Gestión de cambios en los servicios de proveedores	Seguridad	0	No existente	no	0%
16	Gestión de incidentes de seguridad de la información					**11%**
16.1	Gestión de incidentes y mejoras en la seguridad de la información					
16.1.1	Responsabilidad y procedimientos	Seguridad	4	Administrado	si	80%
16.1.2	Reporte de eventos de seguridad de la información	Seguridad	0	No existente	no	0%
16.1.3	Reporte de debilidades de seguridad de la información	Seguridad	0	No existente	no	0%
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Seguridad	0	No existente	no	0%
16.1.5	Respuesta a incidentes de seguridad de la información	Seguridad	0	No existente	no	0%
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Seguridad	0	No existente	no	0%
16.1.7	Recolección de evidencia	Seguridad	0	No existente	no	0%
17	Aspectos de seguridad de la información de la gestión de continuidad de negocio					**10%**
17.1	Continuidad de seguridad de la información					
17.1.1	Planificación de la continuidad de la seguridad de la información	Seguridad	1	Inicial	no	10%
17.1.2	Implementación de la continuidad de la seguridad de la información	Seguridad	1	Inicial	no	10%
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Seguridad	1	Inicial	no	10%
17.2	Redundancias	Seguridad	1	Inicial	no	10%
17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Seguridad	1	Inicial	no	10%
18	Cumplimiento					**10%**
18.1	Cumplimiento de requisitos legales y contractuales	Seguridad	1	Inicial	no	10%
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Seguridad	1	Inicial	no	10%
18.1.2	Derechos de propiedad intelectual	Seguridad	1	Inicial	no	10%
18.1.3	Protección de registros	Seguridad	1	Inicial	no	10%

Tabla 16. (Continuación)

	Control/Objetivo de Control		N - C	Descripción	cumple/ no cumple	Porcentaje
18.1.4	Privacidad y protección de datos personales	Seguridad	1	Inicial	no	10%
18.1.5	Reglamentación de controles criptográficos	Seguridad	6	No Aplica	no	N/A
18.2	Revisiones de seguridad de la información	Seguridad	1	Inicial	no	10%
18.2.1	Revisión independiente de la seguridad de la información	Seguridad	1	Inicial	no	10%
18.2.2	Cumplimiento con las políticas y normas de seguridad	Seguridad	1	Inicial	no	10%
18.2.3	Revisión del cumplimiento técnico	Seguridad	1	Inicial	no	10%

Fuente: El autor.

5.6 **FASE 6. RESULTADOS**

5.6.1 **Análisis y discusión de los resultados**

Después de realizar detalladamente cada uno de los controles y teniendo en cuenta que la compañía definió que el nivel de cumplimiento aceptable es del 80%, se llega a la conclusión que hace falta mucho por realizar, puesto que en estos momentos la organización se encuentra en un 31% del cumplimiento de la norma.

Los controles se encuentran distribuidos así:

Tabla 17. Controles por nivel de cumplimiento.

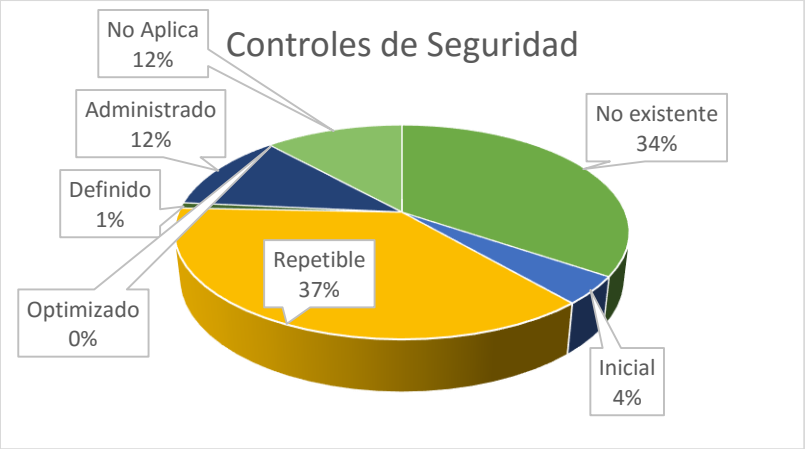
Nivel	Controles
No existente	41
Inicial Repetible	5 44
Definido	1
Administrado	14
Optimizado	0
No Aplica	14

Fuente: El autor.

Como se puede apreciar en tabla anterior, hay 41 controles que no existen, 5 controles donde se ha realizado alguna practica del control, pero con inconsistencias, hay 44 controles sin documentar, hay 1 control que no posee ninguna clase de medición, hay 14 controles a los que se les realiza medición, finalmente hay 14 controles que no se aplican en la compañía.

Aquí se encuentra la distribución de los controles dada en porcentajes.

Figura 4. Estado de madurez de los controles.



Fuente: El autor

Otro análisis realizado fue el nivel de cumplimiento por dominios como se muestra en la siguiente tabla.

Tabla 18. Nivel de cumplimiento por dominios

	Control/Objetivo de Control	Porcentaje
5	Políticas de seguridad de la información	80%
6	Organización de la seguridad de la información	40%
7	Seguridad de los recursos humanos	28%
8	Gestión de activos	52%
9	Control de acceso	31%
10	Criptografía	NA
11	Seguridad física y del entorno	43%
12	Seguridad de las operaciones	28%
13	Seguridad de las comunicaciones	40%
14	Adquisición, desarrollo y mantenimientos de sistemas	17%
15	Relación con los proveedores	11%
16	Gestión de incidentes de seguridad de la información	11%

Tabla 18. (Continuación)

	Control/Objetivo de Control	Porcentaje
17	Aspectos de seguridad de la información de la gestión de continuidad de negocio	10%
18	Cumplimiento	10%
	TOTAL	**31%**

Fuente: El Autor

Interpretación del nivel de cumplimiento por dominios

Políticas de seguridad de la información: es el dominio que se encuentra en un mejor nivel, en este caso el 80%, puesto que durante el desarrollo de este análisis para la implementación de un SGSI se definieron las políticas y quedaron documentadas, en el análisis inicial, se encontraba en un 0%.

Organización de la seguridad de la información: se logró subir de un 0% a un 40%, se implementaron algunas salvaguardas, dentro de la gestión documental se incluyeron los roles y responsabilidades y políticas sobre dispositivos móviles, se sugirieron algunos proyectos que permitirán elevar el porcentaje del dominio al valor esperado.

Seguridad de los recursos humanos: Se mejoró el porcentaje a un 28%, es indispensable que se capacite al personal en temas de seguridad y la implementación de los proyectos sugeridos en ese dominio.

Gestión de activos: Es necesario que se implementen los proyectos sugeridos lo más pronto posible.

Control de acceso: Este dominio se encuentra en un 23%, siendo un valor bajo, aunque se definieron algunas políticas de control de acceso, es necesario la implementación de los proyectos sugeridos.

Criptografía: Este dominio no aplica.

Seguridad física y del entorno: el aumento fue muy bajo, este dominio depende en su totalidad de la implementación de los proyectos sugeridos.

Seguridad de las operaciones: Igual que es dominio anterior, depende de la implementación de los proyectos sugeridos.

Seguridad de las comunicaciones: Es necesario la implementación de los proyectos sugeridos, puesto que es indispensable la adquisición de equipos y software.

Adquisición, desarrollo y mantenimientos de sistemas: La optimización fue poca, pues es necesario implementar los proyectos sugeridos.

Relación con los proveedores: Se definieron políticas, lo que aumento un poco nivel esperado, los procedimientos deben ser aplicados en adelante.

Gestión de incidentes de seguridad de la información: Se definieron políticas y procedimientos que aumentaron un poco el nivel, estas se deben aplicar a futuro para alcanzar un nivel óptimo.

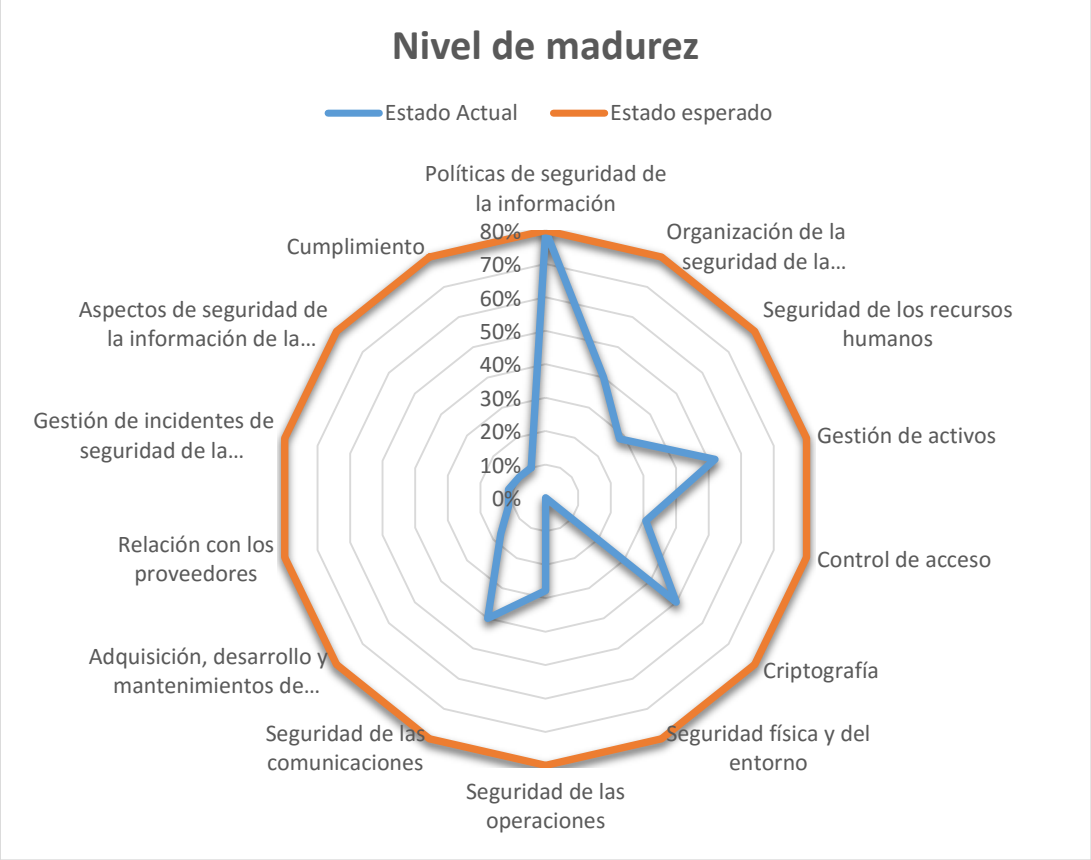
Aspectos de seguridad de la información de la gestión de continuidad de negocio: Se definieron procedimientos, pero es necesario implementar los proyectos sugeridos para alcanzar el nivel óptimo.

Cumplimiento: Se aumentó un poco el porcentaje, pues se definieron políticas, es necesario la implementación de los proyectos para estar en el nivel deseado.

En términos generales, el promedio de cumplimiento de los dominios es del 31%, esto demuestra que la organización representa un gran nivel de vulnerabilidad ante ataques informáticos.

El último informe es un cuadro comparativo del estado de madurez actual contra el estado esperado, para este caso se ha utilizado un gráfico tipo radar el cual permite mostrar el comparativo.

Figura 5. Cumplimiento de dominios en su estado actual y deseado.



Fuente: El Autor

En esta gráfica se puede visualizar el estado actual de la compañía en materia de seguridad informática, como se mencionó anteriormente el promedio es del 31%, en este caso, los controles se identifican en color azul, en color naranja se muestra el nivel esperado, que para el caso de la empresa Servidoc S.A. se definió en un 80%, es de anotar que el dominio que alcanza ese nivel es el de Políticas de Seguridad de la Información, si se tiene en cuenta que están quedaron definidas en el actual análisis para la implementación del SGSI.

6. CONCLUSIONES

- Se logró realizar el análisis que permitirá la implementación del sistema de Gestión de Seguridad de la Información bajo la norma ISO/IEC 27001:2013, planteando soluciones de seguridad.
- La organización posee pocas fortalezas en temas relacionados con seguridad de la información, por otro lado, la cantidad de debilidades es más representativa, lo que significa que la organización se encuentra muy vulnerable ante ataques de seguridad de la información.
- Haciendo uso de la metodología Magerit, se identificaron los riesgos, además se definió el nivel de seguridad que posee cada activo de la organización, permitiendo definir cuáles son los que requieren mayor atención, Se definieron salvaguardas que permitirán en el momento de la implementación del SGSI proteger la seguridad general de la organización.
- El resultado de las vulnerabilidades demuestra que la compañía Servidoc S.A. cuenta con mínimas medidas de seguridad de la información, el análisis para la implementación del SGSI contribuirá a llevar el riesgo a un nivel bajo.
- Se establecieron y documentaron las políticas de la seguridad de la información y la gestión de roles y responsabilidades del personal, además se sugirieron algunos proyectos que deben ser implementados para lograr blindar la organización ante ataques.

7. BIBLIOGRAFÍA

FERNÁNDEZ, Raúl José Gil. Sistematizacion de la gestion de riesgos de la seguridad de la información en la red de la universidad centroccidental “Lisandro Alvarado” [en línea]. Barquisimeto.2011. Disponible en: http://bibcyt.ucla.edu.ve/Edocs_Bciucla/Repositorio/TGEQA76.9.A25C352011.pdf

NIETO, Juan Pablo. Plan de implementación de la ISO/IEC 27001:2005. [en línea]. Barcelona. 2013. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23054/1/Nieto_WP2013_PlanImplementacionISO2007.pdf

MATALOBOS VEIGA, Juan Manuel. Análisis de riesgos de la seguridad de la información. [en línea]. Madrid. 2009. Disponible en: http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

VÁSQUES, Karina del Rocío. Aplicación de la Metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicada a la empresa pesquera e industrial Bravito S.A. . [en línea]. Machala. 2013. Disponible en http://dspace.ups.edu.ec/handle/123456789/5272/statistics.

PEREIRA, Hose Aurela. Plan de implementación de la norma ISO/IEC 27001:2005. [en línea]. Barcelona. 2013. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23704/7/jaurelaTFM0613memoria.pdf

BUENAÑO QUINTA, José Luis; GRANADA LUCES ,Marcelo Alfonso. Planeación y Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 – 27002. [en línea]. Guayaquil. 2009. Disponible en:

CUCHIMBA, John Jairo; PERAFÁN RUIZ, Mildred Caicedo. Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. [en línea]. Cuchimba. 2014. Disponible en: http://repository.unad.edu.co/bitstream/10596/2655/3/76327474.pdf

MEGA, Gustavo Pallas. Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Gustavo Pallas. [en línea]. Montevideo. 2009.

Disponible en: http://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

PEREZ PÉREZ ,Yesica María; OSORIO RIVERO, Yenis Pinedad. Gestión de Riesgos Tecnológicos en la caja de compensación familiar de Fenalco del Tolima "COMFENALCO". . [en línea]. Ocaña. 2014. Disponible en:http://www.uan.edu.co/images/programas-posgrados/Esp_Auditoria_sistemas/documentos/2012_II/GESTION_DE_RIESGOS_TECNOLOGICOS_EN_LA_CAJA_DE_COMPENSACION_FAMILIAR_DE_FENALCO_DEL_TOLIMA_COMFENALCO.pdf

TARAZONA T, Cesar H. Amenazas Informáticas y Seguridad de la Información. (2007). Universidad Externado de Colombia. [en línea]. 2.007. Disponible en: http://revistas.uexternado.edu.co/index.php/derpen/article/view/965/915

AGUILERA LÓPEZ, Purificación. Seguridad Informática Purificación. [en línea]. Navalcarnero. 2.010. Disponible en: https://books.google.com.co/books?id=Mgvm3AYIT64C&pg=PA9&dq=concepto+seguridad+informatica&hl=es&sa=X&ei=jf9bVcWxMYW1sAS9z4CQDg&ved=0CC0Q6AEwAA#v=onepage&q=concepto%20seguridad%20informatica&f=true

ALARCÓN, Vicenç Fernández. Desarrollo de sistemas de información. [en línea]. Barcelona. 2006. Disponible en: https://books.google.com.co/books?id=Sqm7jNZS_L0C&printsec=frontcover&dq=sistema+de+informaci%C3%B3n&hl=es&sa=X&ved=0ahUKEwjzucWSr6fJAhWHJB4KHROrCLUQ6AEIGjAA#v=onepage&q=sistema%20de%20informaci%C3%B3n&f=false

AREITIO BERTOLÍN, Javier. Seguridad de la Información – Redes, informática y sistemas de información. . [en línea]. Madrid. 2008. Disponible en: https://books.google.com.co/books?id=_z2GcBD3deYC&pg=PA201&dq=sistema+gestion+seguridad+informatica&hl=es&sa=X&ei=3gNcVd_wKYOpNvbigUg&ved=0CCQQ6wEwAA#v=onepage&q=sistema%20gestion%20seguridad%20informatica&f=false

GOBIERNO DE ESPAÑA. Familia de Normas ISO 27000. Disponible en: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

MINTIC. El Congreso de Colombia Decreta. [en línea]. Bogotá. 2009. Disponible en: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

DIARIO OFICIAL. Ley 1288 DE 2.009. [en línea]. Bogotá. 2009. Disponible en: http://200.26.152.57/SIDN15%5CArchivos%5CNormatividad%5CLegislaci%C3%B3n%20Nacional%5CLeyes%20de%20Colombia%5CLeyes%202009%20(1270%20-%201371)%5CLey%201288%20de%202009%20%20(Fortalece%20actividades%20de%20inteligencia%20y%20contrainteligencia).pdf

SALCEDO, Robin J. Resumen Ejecutivo memoria TFM plan deimplementacion del SGSI. [en línea]. Barcelona. 2014 Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/41002/4/rsalcedobTFC1214memoria.pdf

ROJAS VALDUCIEL, Halena. Elaboración de un plan de implementación de la ISO/IEC 27001:2013. [en línea]. Barcelona. 2014. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/40297/1/hrojasvTFM1214.pdf

PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. Magerit V.3: Metodología de análisis y gestión de riesgos de los sistemas de información. [en línea]. Madrid. 2012. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VfhKvvl_Oko

MENDOZA, Miguel Angel. ¿Qué es una Declaración de Aplicabilidad (SoA) y para qué sirve?. [en línea]. Buenos Aires. 2015. Disponible en: http://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

UNIVERSIDAD NACIONAL DE COLOMBIA. Técnicas para recolectar información. [en línea]. Bogotá. 2015. Disponible en: datoshttp://www.virtual.unal.edu.co/cursos/sedes/manizales/4060030/lecciones/Capitulo%202/tecnicas.html

Procesamiento y análisis de datos. [en línea]. 2015. Disponible en: http://buendato.ning.com/profiles/blogs/procesamiento-y-analisis-de

Documentación Kali. [en línea]. 2015. Disponible en: https://www.kali.org/

LYON, Gordon. Guía de referencia de Nmap. [en línea]. California. 2015. Disponible en: https://nmap.org/man/es/

REYES PLATA, Alejandro. Ethical Hacking. [en línea]. México. 2010. Disponible en: http://www.seguridad.unam.mx/descarga.dsc?arch=2776

PEREZ, Mario. Tutorial Wireshark. [en línea]. 2013. Disponible en: https://geekytheory.com/tutorial-wirshark-1-instalacion/

Kali Linux Tutoriales. [en línea]. 2016. Disponible en: http://kalilinuxtutorials.com/dnsenum/

OLMEDO, Javier. Obtener Información con The Harvester. [en línea]. 2015. Disponible en: http://hackpuntes.com/obtener-informacion-con-the-harvester/

AMAYA, Camilo. ¿Qué es y por qué hacer un análisis de Riesgos? [en línea]. 2012. Disponible en: http://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/

8. ANEXOS

Anexo A. Encuesta

Número	PREGUNTAS	RESPUESTA	
		SI	NO
1	¿El computador asignado para el desarrollo de sus funciones recibe mantenimiento períodicamente?		
2	¿Existe un Sistema de Gestión de Seguridad Informática en la Empresa?		
3	¿La compañía capacita al personal en temas de seguridad informática?		
4	¿Existe alguna política para el cambio regular de las contraseñas?		
5	¿Antes y despues de la contratación del personal se hace entrega de un manual de funciones y responsabilidades de seguridad de la información?		
6	¿Cuándo ocurre un evento relacionado con seguridad de la información sabe a quien reportarlo?		
7	¿Realiza copias de los datos?		
8	¿Considera necesario que la compañía invierta en la implementación de un Sistema de Gestión de Seguridad de la Información?		
9	¿Posee antivirus el computador asignado?		
10	¿La compañía posee posee software legal en sus totalidad?		
11	¿Existen zonas restringidas de acceso de personal?		
12	¿Se realiza mantenimiento preventivo y correctivo a la UPS?		
13	¿Existen sistemas de seguridad que impidan el acceso a lugares restringidos?		
14	¿Se cuenta con sistemas de alarma como detectores de humo, humedad?		
15	¿Existe vigilancia en la entrada del edificio?		
16	¿Los sitios donde están los equipos de cómputo cuenta con aire acondicionado?		
17	¿Se encuentra asegurados mediante pólizas los equipos de cómputo?		
18	¿Existe algun control para navegar en internet?		
19	¿Existe control sobre el uso del correo electrónico?		

Fuente: El autor.

Anexo B. Análisis Diferencial

	Control/Objetivo de Control	Responsable	N-C	Descripción	cumple/no cumple
5	Políticas de seguridad de la información				
5.1	Directrices establecidas por la dirección para la seguridad de la información				
5.1.1	Políticas para la seguridad de la información	Seguridad	0	No existe	no
5.1.2	Revisión de las políticas para seguridad de la información	Seguridad	0	No existe	no
6	Organización de la seguridad de la información				
6.1	Organización interna				
6.1.1	Roles y responsabilidades para la seguridad de información	Seguridad	0	No existe	no
6.1.2	Separación de deberes	Seguridad	0	No existe	no
6.1.3	Contacto con las autoridades	Seguridad	0	No existe	no
6.1.4	Contacto con grupos de interés especial	Seguridad	0	No existe	no
6.1.5	Seguridad de la información en la gestión de proyectos	Seguridad	0	No existe	no
6.2	Dispositivos móviles y teletrabajo				
6.2.1	Política para dispositivos móviles	Seguridad	0	No existe	no
6.2.2	Teletrabajo	Seguridad	0	No existe	no
7	Seguridad de los recursos humanos				
7.1	Antes de asumir el empleo				
7.1.1	Selección	Rh	3	Definido	si
7.1.2	Términos y condiciones del empleo	Rh	2	Repetible	no
7.2	Durante la ejecución del empleo				
7.2.1	Responsabilidades de la dirección	Rh	1	Inicial	no
7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Rh	0	No Existe	no
7.2.3	Proceso disciplinario	Rh	0	No Existe	no
7.3	Terminación o cambio de empleo				
7.3.1	Terminación o cambio de responsabilidades de empleo	Rh	0	No Existe	no
8	Gestión de activos				
8.1	Responsabilidad por los activos				
8.1.1	Inventario de activos	Rh	4	Administrado	si
8.1.2	Propiedad de los activos	Rh	4	Administrado	si
8.1.3	Uso aceptable de los activos	Rh	2	Repetible	no
8.1.4	Devolución de activos	Rh	4	Administrado	si
8.2	Clasificación de la información				
8.2.1	Clasificación de la información	Rh	2	Repetible	no
8.2.2	Etiquetado de la información	Sistemas	2	Repetible	no
8.2.3	Manejo de activos	Rh	2	Repetible	no
8.3.1	Gestión de medios removibles	Sistemas	2	Repetible	no
8.3.2	Disposición de los medios	Sistemas	2	Repetible	no
8.3.3	Transferencia de medios físicos	Sistemas	2	Repetible	no
9	Control de acceso				

Anexo B. (continuación)

	Control/Objetivo de Control	Responsable	N-C	Descripción	cumple/no cumple
9.1	Requisitos del negocio para control de acceso				
9.1.1	Política de control de acceso	Seguridad	2	Repetible	no
9.1.2	Política sobre el uso de los servicios de red	Seguridad	2	Repetible	no
9.2	Gestión de acceso de usuarios				
9.2.1	Registro y cancelación del registro de usuarios	Seguridad	2	Repetible	no
9.2.2	Suministro de acceso de usuarios	Seguridad	2	Repetible	no
9.2.3	Gestión de derechos de acceso privilegiado	Seguridad	2	Repetible	no
9.2.4	Gestión de información de autenticación secreta de usuarios	Seguridad	2	Repetible	no
9.2.5	Revisión de los derechos de acceso de usuarios	Seguridad	2	Repetible	no
9.2.6	Retiro o ajuste de los derechos de acceso	Seguridad	2	Repetible	no
9.3	Responsabilidades de los usuarios				
9.3.1	Uso de la información de autenticación secreta	Seguridad	0	No existe	no
9.4	Control de acceso a sistemas y aplicaciones				
9.4.1	Restricción de acceso Información	Seguridad	0	No existe	no
9.4.2	Procedimiento de ingreso seguro	Seguridad	0	No existe	no
9.4.3	Sistema de gestión de contraseñas	Seguridad	0	No existe	no
9.4.4	Uso de programas utilitarios privilegiados	Seguridad	0	No existe	no
9.4.5	Control de acceso a códigos fuente de programas	Seguridad	0	No existe	no
10	Criptografía				
10.1	Controles criptográficos				
10.1.1	Política sobre el uso de controles criptográficos	Seguridad	0	No existe	no
10.1.2	Gestión de llaves	Seguridad	0	No existe	no
11	Seguridad física y del entorno				
11.1	Áreas seguras				
11.1.1	Perímetro de seguridad física	Seguridad Física	2	Repetible	no
11.1.2	Controles físicos de entrada	Seguridad Física	2	Repetible	no
11.1.3	Seguridad de oficinas, recintos e instalaciones	Seguridad Física	2	Repetible	no
11.1.4	Protección contra amenazas externas y ambientales	Seguridad Física	2	Repetible	no
11.1.5	Trabajo en áreas seguras	Seguridad Física	2	Repetible	no
11.1.6	Áreas de despacho y carga	Seguridad Física	2	Repetible	no
11.2	Equipos				
11.2.1	Ubicación y protección de los equipos	Seguridad Física	2	Repetible	no
11.2.2	Servicios de suministro	Seguridad Física	2	Repetible	no
11.2.3	Seguridad del cableado	Sistemas	2	Repetible	no
11.2.4	Mantenimiento de equipos	Sistemas	2	Repetible	no
11.2.5	Retiro de activos	Seguridad Física	2	Repetible	no

Anexo B. (continuación)

	Control/Objetivo de Control	Responsable	N-C	Descripción	cumple/no cumple
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Sistemas	2	Repetible	no
11.2.7	Disposición segura o reutilización de equipos	Seguridad Física	2	Repetible	no
11.2.8	Equipos de usuario desatendidos	Sistemas	2	Repetible	no
11.2.9	Política de escritorio limpio y pantalla limpia	Sistemas	2	Repetible	no
12	Seguridad de las operaciones				
12.1	Procedimientos operacionales y responsabilidades				
12.1.1	Procedimientos de operación documentados	sistemas	0	No existe	no
12.1.2	Gestión de cambios	sistemas	0	No existe	no
12.1.3	Gestión de capacidad	sistemas	0	No existe	no
12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	sistemas	0	No existe	no
12.2	Protección contra códigos maliciosos				
12.2.1	Controles contra códigos maliciosos	sistemas	2	Repetible	no
12.3	Copias de respaldo				
12.3.1	Respaldo de información	sistemas	2	Repetible	no
12.4	Registro y seguimiento				
12.4.1	Registro de eventos	Sistemas	0	No existe	no
12.4.2	Protección de la información de registro	Sistemas	2	Repetible	no
12.4.3	Registros del administrador y del operador	Sistemas	2	Repetible	no
12.4.4	sincronización de relojes	Sistemas	4	Administrado	si
12.5	Control de software operacional				
12.5.1	Instalación de software en sistemas operativos	Sistemas	2	Repetible	no
12.6	Gestión de la vulnerabilidad técnica				
12.6.1	Gestión de las vulnerabilidades técnicas	Sistemas	2	Repetible	no
12.6.2	Restricciones sobre la instalación de software	Sistemas	2	Repetible	no
12.7	Consideraciones sobre auditorias de sistemas de información				
12.7.1	Información controles de auditoría de sistemas	Sistemas	0	No existe	no
13	Seguridad de las comunicaciones				
13.1	Gestión de la seguridad de las redes				
13.1.1	Controles de redes	Sistemas	2	Repetible	no
13.1.2	Seguridad de los servicios de red	Sistemas	2	Repetible	no
13.1.3	Separación en las redes	Sistemas	2	Repetible	no
13.2	Transferencia de información				
13.2.1	Políticas y procedimientos de transferencia de información	Sistemas	2	Repetible	no
13.2.2	Acuerdos sobre transferencia de información	Sistemas	2	Repetible	no
13.2.3	Mensajería electrónica	Sistemas	2	Repetible	no

Anexo B. (continuación)

	Control/Objetivo de Control	Responsable	N-C	Descripción	cumple/no cumple
13.2.4	Acuerdos de confidencialidad o de no divulgación	Sistemas	2	Repetible	no
14	Adquisición, desarrollo y mantenimientos de sistemas				
14.1	Requisitos de seguridad de los sistemas de información				
14.1.1	Análisis y especificación de requisitos de seguridad de la información	Sistemas	2	Repetible	no
14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	Sistemas	2	Repetible	no
14.1.3	Protección de transacciones de los servicios de las aplicaciones	Sistemas	2	Repetible	no
14.2	Seguridad en los procesos de desarrollo y soporte				
14.2.1	Política de desarrollo seguro	Seguridad	0	No existe	no
14.2.2	Procedimientos de control de cambios en sistemas	Seguridad	0	No existe	no
14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Seguridad	0	No existe	no
14.2.4	Restricciones en los cambios a los paquetes de software	Seguridad	0	No existe	no
14.2.5	Principios de construcción de sistemas seguros	Seguridad	0	No existe	no
14.2.6	Ambiente de desarrollo seguro	Seguridad	0	No existe	no
14.2.7	Desarrollo contratado externamente	Seguridad	0	No existe	no
14.2.8	Pruebas de seguridad de sistemas	Seguridad	0	No existe	no
14.2.9	Prueba de aceptación de sistemas	Seguridad	0	No existe	no
14.3	Datos de prueba	Seguridad	0	No existe	no
14.3.1	Protección de datos de prueba	Seguridad	0	No existe	no
15	Relación con los proveedores				
15.1	Seguridad de la información en las relaciones con los proveedores	Seguridad	0	No existe	no
15.1.1	Política de seguridad de la información para las relaciones con proveedores	Seguridad	0	No existe	no
15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Seguridad	0	No existe	no
15.1.3	Cadena de suministro de tecnología de información y comunicación	Seguridad	0	No existe	no
15.2	Gestión de la prestación de servicios con los proveedores	Seguridad	0	No existe	no
15.2.1	Seguimiento y revisión de los servicios de los proveedores	Seguridad	0	No existe	no
15.2.2	Gestión de cambios en los servicios de proveedores	Seguridad	0	No existe	no
16	Gestión de incidentes de seguridad de la información				
16.1	Gestión de incidentes y mejoras en la seguridad de la información				
16.1.1	Responsabilidad y procedimientos	Seguridad	0	No existe	no

Anexo B. (continuación)

	Control/Objetivo de Control	Responsable	N-C	Descripción	cumple/no cumple
16.1.2	Reporte de eventos de seguridad de la información	Seguridad	0	No existe	no
16.1.3	Reporte de debilidades de seguridad de la información	Seguridad	0	No existe	no
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Seguridad	0	No existe	no
16.1.5	Respuesta a incidentes de seguridad de la información	Seguridad	0	No existe	no
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Seguridad	0	No existe	no
16.1.7	Recolección de evidencia	Seguridad	0	No existe	no
17	Aspectos de seguridad de la información de la gestión de continuidad de negocio				
17.1	Continuidad de seguridad de la información				
17.1.1	Planificación de la continuidad de la seguridad de la información	Seguridad	1	Inicial	no
17.1.2	Implementación de la continuidad de la seguridad de la información	Seguridad	1	Inicial	no
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Seguridad	1	Inicial	no
17.2	Redundancias	Seguridad	1	Inicial	no
17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Seguridad	1	Inicial	no
18	Cumplimiento				
18.1	Cumplimiento de requisitos legales y contractuales	Seguridad	0	No existe	no
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Seguridad	0	No existe	no
18.1.2	Derechos de propiedad intelectual	Seguridad	0	No existe	no
18.1.3	Protección de registros	Seguridad	0	No existe	no
18.1.4	Privacidad y protección de datos personales	Seguridad	0	No existe	no
18.1.5	Reglamentación de controles criptográficos	Seguridad	0	No existe	no
18.2	Revisiones de seguridad de la información	Seguridad	0	No existe	no
18.2.1	Revisión independiente de la seguridad de la información	Seguridad	0	No existe	no
18.2.2	Cumplimiento con las políticas y normas de seguridad	Seguridad	0	No existe	no
18.2.3	Revisión del cumplimiento técnico	Seguridad	0	No existe	no

Fuente: El autor.

Anexo C. Declaración de aplicabilidad

Leyenda (Razón de controles seleccionados)
LR: Requemamientos Legales, **CO**: Obligaciones Contractuales
BR/BP: Requerimientos del negocio/Mejores Prácticas,
RRA: Resultado de Análisis de Riesgos

	Control/Objetivo de Control	**Descripción**	**Justificación de exclusión**	**Controles seleccionados y razones de selección**				**Aplica?**
				LR	CO	BR/BP	RRA	
5	Políticas de seguridad de la información							
5.1	Directrices establecidas por la dirección para la seguridad de la información							
5.1.1	Políticas para la seguridad de la información	Existen políticas de seguridad de la información pero no han sido documentadas, se debe redactar un documento que políticas para que sea distribuido y conocido por todo el personal incluido en el proceso del SGSI.		x		x		SI
5.1.2	Revisión de las políticas para seguridad de la información	Se debe establecer un procedimiento que permita la revisión periódica de las políticas de la seguridad de la información por lo menos cada año		x		x		SI
6	Organización de la seguridad de la información							
6.1	Organización interna							
6.1.1	Roles y responsabilidades para la seguridad de información	Se deben definir roles y responsabilidades de acuerdo a las políticas de seguridad de la información a todos los que interactúen con el SGSI.		x		x		SI
6.1.2	Separación de deberes	Se deben separar las ares consideradas de gran importancia para que así los deberes y responsabilidades asignadas sean separadas, de esta forma se evita el uso indebido de los activos de la organización		x		x		SI
6.1.3	Contacto con las autoridades	En el documento de políticas de la seguridad de la información se debe contemplar un procedimiento que permita gestionar el contacto permanente con autoridades reguladoras de seguridad de la información.		x		x		SI

Anexo C. (Continuación)

	Control/Objetivo de Control	Descripción	Justificación de exclusión	Controles seleccionados y razones de selección				Aplica?
				LR	CO	BR/BP	RRA	
6.1.4	Contacto con grupos de interés especial	Es importante que la persona encargada de la seguridad informática gestione el contacto permanente con grupos de interés, estos pueden ser foros, chats, wiki, comunidades relacionadas con la seguridad informática, con la intención de estar actualizados en aspectos relacionados a la seguridad.		x		x		SI
6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe tratar en cualquier proyecto-				x		SI
6.2	Dispositivos móviles y teletrabajo							
6.2.1	Política para dispositivos móviles	Se deben aplicar políticas para el uso adecuado de dispositivos móviles, su uso inadecuado representa grandes riesgos.				x	x	SI
6.2.2	Teletrabajo	La Cía. no posee empleos bajo la modalidad de teletrabajo						No
7	Seguridad de los recursos humanos							
7.1	Antes de asumir el empleo							
7.1.1	Selección	Se deben realizar una exhaustiva comprobación de los antecedentes del personal como empleados, contratistas, terceros, con el fin de saber su procedencia, referencias personales, judiciales entre otras.			x	x		NO
7.1.2	Términos y condiciones del empleo	Se debe diseñar un documento que permita a los empleados, contratistas y terceros firmar cláusulas de confidencialidad con la organización, manejo adecuado de recursos tecnológicos.			x	x		SI
7.2	Durante la ejecución del empleo							
7.2.1	Responsabilidades de la dirección	Se debe exigir a los empleados, contratistas y terceros el cumplimiento a cabalidad de las políticas de seguridad de la información implementadas por la Cía.			x	x		SI

Anexo C. (Continuación)

	Control/Objetivo de Control	Descripción	Justificación de exclusión	Controles seleccionados y razones de selección				Aplica?
				LR	CO	BR/BP	RRA	
7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Se debe capacitar a todo el personal en aspectos relacionados con la seguridad de la información.				x		SI
7.2.3	Proceso disciplinario	Se deben establecer políticas sobre sanciones que se aplicarán a quienes incumplan con lo descrito en las políticas de seguridad.				x		SI
7.3	Terminación o cambio de empleo							
7.3.1	Terminación o cambio de responsabilidades de empleo	Se debe informar a los empleados en los casos donde las responsabilidades y deberes que les fueron asignados durante el empleo, los cobijan aún cuando se realice una terminación o cambio de contrato.				x		SI
8	Gestión de activos							
8.1	Responsabilidad por los activos							
8.1.1	Inventario de activos	Se debe contar con un inventario detallado de los activos que posee la Cía.		x		x		NO
8.1.2	Propiedad de los activos	Además de la implementación del control anterior, se debe identificar en custodia de quien se encuentra actualmente el activo		x		x		NO
8.1.3	Uso aceptable de los activos	Debe existir una clausula donde los empleados se comprometan a realizar un uso aceptable de los activos de la organización		x		x		SI
8.1.4	Devolución de activos	Se debe establecer un proceso para la devolución de los activos para cuando los empleados cambien de puesto o cuando se termine su contrato.		x		x		NO
8.2	Clasificación de la información							
8.2.1	Clasificación de la información	Se debe establecer un procedimiento que permita clasificar la información de acuerdo a su valor				x		SI

Anexo C. (Continuación)

	Control/Objetivo de Control	Descripción	Justificación de exclusión	Controles seleccionados y razones de selección				Aplica?
				LR	CO	BR/BP	RRA	
8.2.2	Etiquetado de la información	La información debe estar debidamente rotulada, además esta rotulación se debe clasificar de acuerdo al valor que representa la información para la empresa				x		SI
8.2.3	Manejo de activos	Se debe contar con procedimientos que ayuden en el adecuado manejo que se le debe dar a un activo				x		SI
8.3.1	Gestión de medios removibles	Se deben establecer políticas sobre el correcto manejo que se le deben dar a los medios removibles, puesto que estos son necesarios en el desarrollo de las labores diarias.				x		SI
8.3.2	Disposición de los medios	Protección de la información cuando los medios sean destinados a labores diferentes a las actuales, se podría hablar de un procedimiento de eliminación de información ene estos casos.				x		SI
8.3.3	Transferencia de medios físicos	Definir procedimientos que permitan que la información almacenada en estos no sea divulgada, modificada o eliminada.				x		SI
9	Control de acceso							
9.1	Requisitos del negocio para control de acceso							
9.1.1	Política de control de acceso	Establecer políticas que permitan el acceso a la información de acuerdo a privilegios establecidos según sus funciones				x		SI
9.1.2	Política sobre el uso de los servicios de red	Definir el acceso a la red para el desarrollo de funciones que les fueron asignadas.				x		SI
9.2	Gestión de acceso de usuarios							
9.2.1	Registro y cancelación del registro de usuarios	Todos los usuarios con acceso a sistema de información deben estar debidamente registrados, adicionalmente se debe dar de baja a los que ya no hagan parte de la organización o no hagan uso del sistema.		x		x	x	SI

Anexo C. (Continuación)

	Control/Objetivo de Control	Descripción	Justificación de exclusión	Controles seleccionados y razones de selección				Aplica?
				LR	CO	BR/BP	RRA	
9.2.2	Suministro de acceso de usuarios	Implementar un procedimiento que permita a los usuarios del sistema acceder al sistema o negar el acceso a este cuando se considere necesario.				x	x	SI
9.2.3	Gestión de derechos de acceso privilegiado	Se deben establecer privilegios de acceso a la información de acuerdo al desempeño de sus funciones.				x	x	SI
9.2.4	Gestión de información de autenticación secreta de usuarios	Esta información sólo debe ser accesada por personal con privilegios especiales				x	x	SI
9.2.5	Revisión de los derechos de acceso de usuarios	Monitoreo de privilegios asignados a usuarios con el fin de identificar si los privilegios asignados son adecuados para el desarrollo de sus funciones.				x	x	SI
9.2.6	Retiro o ajuste de los derechos de acceso	Se debe dar de baja o modificar los privilegios de acceso a la información en caso de traslado del usuario o retiro de la organización.			x	x	x	SI
9.3	Responsabilidades de los usuarios							
9.3.1	Uso de la información de autenticación secreta	Se deben crear perfiles para el acceso a información considerada de suma importancia para la empresa			x	x	x	SI
9.4	Control de acceso a sistemas y aplicaciones							
9.4.1	Restricción de acceso Información	Restringir el acceso a la información por parte de personal no autorizado.				x	x	SI
9.4.2	Procedimiento de ingreso seguro	Se deben establecer procedimientos que restrinjan el acceso a la información a personal no autorizado				x	x	SI
9.4.3	Sistema de gestión de contraseñas	Se deben establece políticas de gestión de contraseñas como caducidad, bloqueo después de determinado número de intentos, parámetros para creación de contraseñas seguras.				x	x	SI

Anexo C. (Continuación)

	Control/Objetivo de Control	Descripción	Justificación de exclusión	Controles seleccionados y razones de selección				Aplica?
				LR	CO	BR/BP	RRA	
9.4.4	Uso de programas utilitarios privilegiados	Restringir el uso de programas utilitarios ya que pueden violentar la seguridad de las contraseñas, pues algunos revelan las contraseñas, vulnerando la seguridad.				x	x	SI
9.4.5	Control de acceso a códigos fuente de programas	Políticas de acceso al código fuente, este sólo debe ser accesado por el personal autorizado				x	x	SI
10	Criptografía							
10.1	Controles criptográficos							
10.1.1	Política sobre el uso de controles criptográficos	Se deben establecer controles criptográficos que permitan la confidencialidad, disponibilidad, integridad y no repudio de la información		x		x		SI
10.1.2	Gestión de llaves	Se deben establecer controles criptográficos que permitan la confidencialidad, disponibilidad, integridad y no repudio de la información		x		x		SI
11	Seguridad física y del entorno							
11.1	Áreas seguras							
11.1.1	Perímetro de seguridad física	Se debe establecer un perímetro de tal forma que los sitios donde se encuentren los activos tengan accesos restringido			x	x		NO
11.1.2	Controles físicos de entrada	Se debe restringir el acceso a sitios seguros como centro de cableado, ubicación del servidor, espacios donde se encuentre información confidencial, estos sitios deben permanecer con llave.				x		SI
11.1.3	Seguridad de oficinas, recintos e instalaciones	Restringir el acceso a personal no autorizado, las áreas deben estar demarcadas dando aviso que son sitios restringidos				x		NO

Anexo C. (Continuación)

	Control/Objetivo de Control	Descripción	Justificación de exclusión	Controles seleccionados y razones de selección				Aplica?
				LR	CO	BR/BP	RRA	
11.1.4	Protección contra amenazas externas y ambientales	Se debe contar con detectores de humo y humedad, ubicación de extinguidores en sitios estratégicos, cuartos técnicos con aire acondicionado, adquisición de pólizas contra robo y desastres naturales			x	x		SI
11.1.5	Trabajo en áreas seguras	Se deben preservar los sitios donde se encuentren activos valiosos con el fin de protegerlos contra daños intencionados				x		NO
11.1.6	Áreas de despacho y carga	Se deben designar sitios especiales para carga y despacho, lo recomendable es que estén aislados de los denominados sitios seguros o restringidos	No se cuenta con despacho o recibo de carga que amerite un espacio			x		NO
11.2	Equipos							
11.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados en sitios seguros, de esta forma se protegen contra robo, accesos no autorizados.				x		SI
11.2.2	Servicios de suministro	Se debe contar con un adecuado suministro y respaldo de energía				x		SI
11.2.3	Seguridad del cableado	Se debe proteger el cableado eléctrico y de datos de posibles daños como interceptaciones con el fin de causar daño.				x		SI
11.2.4	Mantenimiento de equipos	Se debe contar con mantenimiento preventivo y correctivo en períodos de tiempo establecidos, con el fin de evitar daños en hardware, actualización de software.				x		NO
11.2.5	Retiro de activos	Se debe definir un procedimiento que autorice el retiro de activos de la empresa tales como equipos de cómputo, software.				x		SI

Anexo C. (Continuación)

	Control/Objetivo de Control	Descripción	Justificación de exclusión	Controles seleccionados y razones de selección				Aplica?
				LR	CO	BR/BP	RRA	
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Aplicar la misma seguridad que se realiza a los equipos dentro de la empresa	No se cuenta con equipos ni activos fuera de la organización					No
11.2.7	Disposición segura o reutilización de equipos	Se debe proteger la información confidencial de equipos en desuso o cuando son dados de baja.				x		SI
11.2.8	Equipos de usuario desatendidos	Establecer políticas para equipos cuando los usuarios no están presentes, evitando así el acceso no autorizado o robo de información.				x		SI
11.2.9	Política de escritorio limpio y pantalla limpia	Definir procedimientos para que los escritorios estén libres de papeles, medios de almacenamiento que puedan permitir filtración de información, además políticas de pantallas limpias.				x		SI
12	Seguridad de las operaciones							
12.1	Procedimientos operacionales y responsabilidades							
12.1.1	Procedimientos de operación documentados	Los procedimientos deben estar documentados y puestos al alcance de todos, también manuales de operaciones específicas				x		SI
12.1.2	Gestión de cambios	Establecer políticas donde los cambios sean realizados por personal autorizado, además deben quedar soportados para llevar un control para evitar contratiempos.				x		SI
12.1.3	Gestión de capacidad	Se debe realizar un monitoreo de los recursos de tal forma que no afecten la operación, algunos pueden ser capacidad de banda ancha, circuitos descalibrados que afecten el fluido eléctrico, equipos de cómputo lentos.				x		SI

Anexo C. (Continuación)

	Control/Objetivo de Control	Descripción	Justificación de exclusión	Controles seleccionados y razones de selección				Aplica?
				LR	CO	BR/BP	RRA	
12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Los ambientes de desarrollo prueba y operación deben estar aislados, con restricciones de acceso con el fin de evitar cambios o modificaciones no autorizadas.				x		SI
12.2	Protección contra códigos maliciosos							
12.2.1	Controles contra códigos maliciosos	Los equipos de cómputo deben contar con software contra código malicioso, el cual se debe actualizar constantemente con el fin actualizar parches que mitiguen las nuevas vulnerabilidades.				x		SI
12.3	Copias de respaldo							
12.3.1	Respaldo de información	Se debe realizar respaldo de la información, además se deben realizar pruebas para comprobar que estos cumplen con las políticas de respaldo-				x		SI
12.4	Registro y seguimiento							
12.4.1	Registro de eventos	Se debe llevar un control de los eventos con el fin de establecer procedimientos que ayuden a repararlos o eliminarlos definitivamente, con el fin de que no se vuelvan a presentar				x		SI
12.4.2	Protección de la información de registro	Se debe proteger la información de registro de personal no autorizado, sólo el administrador o encargado será quien pueda tener acceso a estos, se deben realizar copias de logs.				x		SI
12.4.3	Registros del administrador y del operador	Todas las tareas que desarrollen el administrador y el operador del sistema de información deben estar registradas, además se debe realizar un respaldo de estos registros.				x		SI
12.4.4	sincronización de relojes	Los relojes de los dispositivos que intervienen en el procesamiento de información deben estar sincronizados.						NO
12.5	Control de software operacional							

Anexo C. (Continuación)

	Control/Objetivo de Control	Descripción	Justificación de exclusión	Controles seleccionados y razones de selección				Aplica?
				LR	CO	BR/BP	RRA	
12.5.1	Instalación de software en sistemas operativos	La instalación de software debe estar controlada, de tal forma que sólo las personas autorizadas puedan realizar estas tareas, además deben quedar registradas.				x		SI
12.6	Gestión de la vulnerabilidad técnica							
12.6.1	Gestión de las vulnerabilidades técnicas	Se deben establecer procedimientos que minimicen las vulnerabilidades a que están expuestos los activos tecnológicos.				x		SI
12.6.2	Restricciones sobre la instalación de software	La instalación de software debe estar controlada, de tal forma que sólo las personas autorizadas puedan realizar estas tareas, además deben quedar registradas.				x		SI
12.7	Consideraciones sobre auditorias de sistemas de información							
12.7.1	Información controles de auditoría de sistemas	Se deben establecer procedimientos que permitan el buen uso de las herramientas de auditoría a los sistemas, pero siempre procurando minimizar la interrupción del servicio a causa de estas.						SI
13	Seguridad de las comunicaciones							
13.1	Gestión de la seguridad de las redes							
13.1.1	Controles de redes	Se deben instalar dispositivos o software que permita controlar el acceso a la red como Firewall, Ids, autenticación para su ingreso		x		x	x	SI
13.1.2	Seguridad de los servicios de red	Establecer controles de acceso, acuerdos de servicio en su utilización, monitoreo constante para detectar intrusos				x		SI
13.1.3	Separación en las redes	Es necesario loa separación de las redes como la intranet de la red con acceso a internet, para lo cual se debe implementar un DMZ				x	x	SI
13.2	Transferencia de información							
13.2.1	Políticas y procedimientos de transferencia de información	Se deben establecer todas las políticas que sean necesarias para proteger la información en el momento de ser transferida (intercambio de información),		x		x	x	SI

Anexo C. (Continuación)

	Control/Objetivo de Control	Descripción	Justificación de exclusión	Controles seleccionados y razones de selección				Aplica?
				LR	CO	BR/BP	RRA	
		permitiendo integridad y confidencialidad.						
13.2.2	Acuerdos sobre transferencia de información	Se deben establecer controles que permitan respetar acuerdos de intercambio o transferencia de información		x		x	x	SI
13.2.3	Mensajería electrónica	Deben existir controles sobre el uso adecuado de la mensajería electrónica, para ello se deben instalar programas que detecten antivirus y spam, además se debe existir capacitación sobre situaciones donde existan correos sospechosos, también políticas del uso adecuado de los recursos, en este caso uso del correo electrónico sólo para el desarrollo de las funciones asignadas.				x	x	SI
13.2.4	Acuerdos de confidencialidad o de no divulgación	Se deben cumplir las políticas de confidencialidad de la información, las cuáles fueron aceptadas en el momento de la firma del contrato.		x	x	x		SI
14	Adquisición, desarrollo y mantenimientos de sistemas							
14.1	Requisitos de seguridad de los sistemas de información							
14.1.1	Análisis y especificación de requisitos de seguridad de la información	Las especificaciones de requisitos se deben tener en cuenta cuando se vaya a realizar un cambio o implementar un nuevo sistema de información				x		SI
14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	Se debe implementar seguridad en los servicios que viajan por redes públicas tales como autenticación, manejo de cookies, sesiones, pki, con el fin de garantizar la confiabilidad de la información		x		x	x	SI
14.1.3	Protección de transacciones de los servicios de las aplicaciones	Se debe implementar seguridad en los servicios que viajan por redes públicas tales como autenticación, manejo de cookies, sesiones, pki, con el fin de garantizar la confiabilidad de la información		x		x	x	SI
14.2	Seguridad en los procesos de desarrollo y soporte							

Anexo C. (Continuación)

	Control/Objetivo de Control	Descripción	Justificación de exclusión	Controles seleccionados y razones de selección				Aplica?
				LR	CO	BR/BP	RRA	
14.2.1	Política de desarrollo seguro	Es importante establecer políticas de código seguro en el desarrollo de software, es aquí donde se deben implementar procedimientos de seguridad como paso de variables por cabecera, sesiones, entre otros, los cuáles deben blindar el sistema de información para evitar vulnerabilidades	Se excluye este control, ya que la Cía. No cuenta con desarrollo de software	x		x		NO
14.2.2	Procedimientos de control de cambios en sistemas	Todos los cambios que se realicen a los programas se deben documentar y quedar registrados, para lo cual se deben establecer procedimientos	Se excluye este control, ya que la Cía. No cuenta con desarrollo de software	x		x		NO
14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Se deben realizar pruebas a las aplicaciones que han sido modificadas, con el fin de evitar alteraciones en la prestación del servicio o mal funcionamiento a causa del desarrollo.	Se excluye este control, ya que la Cía. No cuenta con desarrollo de software	x		x		NO
14.2.4	Restricciones en los cambios a los paquetes de software	Los cambios o modificaciones que se le realizan a las aplicaciones deben estar restringidos con el fin de evitar fallas no deseadas.	Se excluye este control, ya que la Cía. No cuenta con desarrollo de software	x		x		NO
14.2.5	Principios de construcción de sistemas seguros	Establecer procedimientos y políticas que permitan la construcción de aplicaciones seguras	Se excluye este control, ya que la Cía. No cuenta con desarrollo de software	x		x		NO

Anexo C. (Continuación)

	Control/Objetivo de Control	Descripción	Justificación de exclusión	Controles seleccionados y razones de selección				Aplica?
				LR	CO	BR/BP	RRA	
14.2.6	Ambiente de desarrollo seguro	Los ambientes de desarrollo deben estar aislados y contar con todas las medidas de seguridad en cuanto a control de acceso a la información y a las instalaciones	Se excluye este control, ya que la Cía. No cuenta con desarrollo de software	x		x		NO
14.2.7	Desarrollo contratado externamente	Cuando se adquieran sistemas externos, realizar seguimiento, es necesario validarlos antes de ponerlos en funcionamiento		x		x		SI
14.2.8	Pruebas de seguridad de sistemas	Someter los sistemas a pruebas con el fin de identificar vulnerabilidades, se podría contemplar pruebas de hacking ético.		x		x		SI
14.2.9	Prueba de aceptación de sistemas	Someter los sistemas a pruebas con el fin de identificar vulnerabilidades, se podría contemplar pruebas de hacking ético.		x		x		SI
14.3	Datos de prueba							
14.3.1	Protección de datos de prueba	Hay que tener cuidado con los datos que se van a ingresar para realizarle pruebas a la aplicación, esto con el fin de evitar alguna fuga de información importante.		x		x		SI
15	Relación con los proveedores							
15.1	Seguridad de la información en las relaciones con los proveedores							
15.1.1	Política de seguridad de la información para las relaciones con proveedores	Igual que con los usuarios de la organización, con los proveedores se deben establecer acuerdos de confidencialidad, control de acceso a l información, seguridad física, intercambio de información entre otros para no ver afectada la seguridad de la información.				x		SI
15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Definir acuerdos de confidencialidad				x		SI

Anexo C. (Continuación)

	Control/Objetivo de Control	Descripción	Justificación de exclusión	Controles seleccionados y razones de selección				Aplica?
				LR	CO	BR/BP	RRA	
15.1.3	Cadena de suministro de tecnología de información y comunicación	Se deben establecer acuerdos que permitan mitigar los riesgos de la seguridad de la información derivados de la cadena se suministro.				x		SI
15.2	Gestión de la prestación de servicios con los proveedores							
15.2.1	Seguimiento y revisión de los servicios de los proveedores							
15.2.2	Gestión de cambios en los servicios de proveedores	Se debe contar con otras alternativas de proveedores que permitan la continuidad del servicio en caso de cambio de proveedor				x		SI
16	Gestión de incidentes de seguridad de la información							
16.1	Gestión de incidentes y mejoras en la seguridad de la información							
16.1.1	Responsabilidad y procedimientos	Definir procedimientos que permitan una reacción rápida ante problemas generados por causa d ella seguridad de la información.				x		SI
16.1.2	Reporte de eventos de seguridad de la información	Se debe informar sobre eventos generados a causa de seguridad de la información con el fin de documentar la solución, es necesario llevar un registro de estos.				x		SI
16.1.3	Reporte de debilidades de seguridad de la información	Informar oportunamente sobre eventos generados, con el fin de identificar recurrencias y debilidades en seguridad de la información.				x		SI
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Cada vez que se presente un evento se seguridad de la información es importante evaluar si será considerado como un incidente o no.				x		SI
16.1.5	Respuesta a incidentes de seguridad de la información	Se debe establecer un proceso que permita establecer los pasos a seguir para atender el incidente.				x		SI

Anexo C. (Continuación)

	Control/Objetivo de Control	Descripción	Justificación de exclusión	Controles seleccionados y razones de selección				Aplica?
				LR	CO	BR/BP	RRA	
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	La experiencia que se ha adquirido en resolver los incidentes, es pieza fundamental para reducir el impacto que pueda causar este incidente a la seguridad de la información				x		SI
16.1.7	Recolección de evidencia	Definir un procedimiento para documentar los incidentes de tal forma que exista una evidencia.				x		SI
17	Aspectos de seguridad de la información de la gestión de continuidad de negocio							
17.1	Continuidad de seguridad de la información							
17.1.1	Planificación de la continuidad de la seguridad de la información	Definir políticas que permita la gestión de la continuidad del negocio, aunque la organización presente una crisis				x		SI
17.1.2	Implementación de la continuidad de la seguridad de la información	Implementar procedimientos que permitan la continuidad del negocio ante situaciones imprevistas que podrían causar retrasos en la operación.				x		SI
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Realizar revisiones a los procedimientos implementados para la gestión de la continuidad del servicio para determinar si son efectivos o no.				x		SI
17.2	Redundancias							
17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Es necesario establecer redundancias en las instalaciones donde se procesa la información con el fin de que no se vea afectada la disponibilidad de la información.				x		SI
18	Cumplimiento							
18.1	Cumplimiento de requisitos legales y contractuales							

Anexo C. (Continuación)

	Control/Objetivo de Control	Descripción	Justificación de exclusión	Controles seleccionados y razones de selección				Aplica?
				LR	CO	BR/BP	RRA	
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Definir el marco legal con el cual se debe regir la seguridad de la información.		x		x		SI
18.1.2	Derechos de propiedad intelectual	Cumplir a cabalidad las políticas de derechos de propiedad intelectual, software patentado.		x		x		SI
18.1.3	Protección de registros	Procedimiento que permita la custodia de los registros ante situaciones de robo, modificación, divulgación.		x		x		SI
18.1.4	Privacidad y protección de datos personales	Cumplir con las políticas de la protección de datos personales		x		x		SI
18.1.5	Reglamentación de controles criptográficos	Cumplir con las normas relacionadas con controles criptográficos		x		x		SI
18.2	Revisiones de seguridad de la información							
18.2.1	Revisión independiente de la seguridad de la información	Se debe revisar periódicamente el SGSI, estas revisiones deben ser adicionales a las establecidas en las políticas de seguridad de la información.				x		SI
18.2.2	Cumplimiento con las políticas y normas de seguridad	La dirección debe revisar los cumplimientos de las políticas de seguridad de la información establecidas de acuerdo a su área de responsabilidad.				x		SI
18.2.3	Revisión del cumplimiento técnico	Se deben revisar que todo el personal conoce y cumple con las políticas de seguridad de la información				x		SI

Fuente: El autor.

Anexo D. Cuantificación de Activos y dimensiones.

Activo	Amenaza	Frecuencia	Impacto- Dimensión Afectada				
			A	C	I	D	T
Personal Directivo	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Administradora	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Jefes enfermería	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Personal barra de servicios	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Auxiliares enfermería	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Auxiliares laboratorio	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Médicos Generales	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Médicos especialistas	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Servicios generales	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	

Anexo D. (Continuación)

Activo	Amenaza	Frecuencia	Impacto- Dimensión Afectada				
			A	C	I	D	T
	Ingeniería social	0,0054		80%	60%	60%	
Contadora	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Asistente contable	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Revisor fiscal	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Secretaria gerencia	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Secretaria asignación citas	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Ingeniero sistemas	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Bacteriólogas	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Mensajero	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Auditores médicos	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Electro médico	Deficiencias en la organización	0,0054				50%	

Anexo D. (Continuación)

Activo	Amenaza	Frecuencia	Impacto- Dimensión Afectada				
			A	C	I	D	T
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Electricista	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Mantenimiento	Deficiencias en la organización	0,0054				50%	
	Fugas de información	0,0054		80%			
	Indisponibilidad del personal	0,0054				80%	
	Extorsión	0,0027		70%	70%	70%	
	Ingeniería social	0,0054		80%	60%	60%	
Portátiles	Fuego	0,0027				90%	
	Daños por agua	0,0027				80%	
	Otros desastres Naturales	0,0027				80%	
	Fuego	0,0027				90%	
	Daños por agua	0,0027				80%	
	Contaminacion Mecanica	0,0027				80%	
	Contaminación electromagnética	0,0027				50%	
	Avería de origen físico o lógico	0,0027				60%	
	Corte del suministro eléctrico	0,0027				60%	
	Condiciones inadecuadas de temperatura o humedad	0,0027				60%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de mantenimiento / actualización de equipos (hardware)	0,0164				60%	
	Modificación deliberada de la información	0,0027			70%		
	Abuso de privilegios de acceso	0,0054		80%	60%	70%	
	Robo	0,0027		90%		90%	
	Ataque destructivo	0,0027				80%	
	Uso no previsto	0,0164		70%	70%	70%	
	Emanaciones electromagnéticas	0,0027				50%	
	Caída del sistema por agotamiento de recursos	0,0164				80%	
	Pérdida de equipos	0,0027		80%		80%	
	Acceso no autorizado	0,0027		70%	60%		
	Manipulación de los equipos	0,0054		60%		60%	
	Denegación de servicio	0,0027				70%	
Equipos de cómputo	Fuego	0,0027				90%	
	Daños por agua	0,0027				80%	
	Otros desastres Naturales	0,0027				80%	
	Fuego	0,0027				90%	
	Daños por agua	0,0027				80%	
	Contaminacion Mecanica	0,0027				80%	

Anexo D. (Continuación)

Activo	Amenaza	Frecuencia	Impacto- Dimensión Afectada				
			A	C	I	D	T
	Contaminación electromagnética	0,0027				50%	
	Avería de origen físico o lógico	0,0027				60%	
	Corte del suministro eléctrico	0,0027				60%	
	Condiciones inadecuadas de temperatura o humedad	0,0027				60%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de mantenimiento / actualización de equipos (hardware)	0,0164				60%	
	Modificación deliberada de la información	0,0027			70%		
	Abuso de privilegios de acceso	0,0054		80%	60%	70%	
	Robo	0,0027		90%		90%	
	Ataque destructivo	0,0027				80%	
	Uso no previsto	0,0164		70%	70%	70%	
	Emanaciones electromagnéticas	0,0027				50%	
	Caída del sistema por agotamiento de recursos	0,0164				80%	
	Pérdida de equipos	0,0027		80%		80%	
	Acceso no autorizado	0,0027		70%	60%		
	Manipulación de los equipos	0,0054		60%		60%	
	Denegación de servicio	0,0027				70%	
Impresoras	Fuego	0,0027				90%	
	Daños por agua	0,0027				80%	
	Otros desastres Naturales	0,0027				80%	
	Fuego	0,0027				90%	
	Daños por agua	0,0027				80%	
	Contaminacion Mecanica	0,0027				80%	
	Contaminación electromagnética	0,0027				50%	
	Avería de origen físico o lógico	0,0027				60%	
	Corte del suministro eléctrico	0,0027				60%	
	Condiciones inadecuadas de temperatura o humedad	0,0027				60%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de mantenimiento / actualización de equipos (hardware)	0,0164				60%	
	Modificación deliberada de la información	0,0027			70%		
	Abuso de privilegios de acceso	0,0054		80%	60%	70%	
	Robo	0,0027		90%		90%	
	Ataque destructivo	0,0027				80%	
	Uso no previsto	0,0164		70%	70%	70%	
	Emanaciones electromagnéticas	0,0027				50%	
	Caída del sistema por agotamiento de recursos	0,0164				80%	
	Pérdida de equipos	0,0027		80%		80%	
	Acceso no autorizado	0,0027		70%	60%		
	Manipulación de los equipos	0,0054		60%		60%	
	Denegación de servicio	0,0027				70%	

Anexo D. (Continuación)

Activo	Amenaza	Frecuencia	Impacto- Dimensión Afectada				
			A	C	I	D	T
Servidor Aplicaciones	Fuego	0,0027				90%	
	Daños por agua	0,0027				80%	
	Otros desastres Naturales	0,0027				80%	
	Fuego	0,0027				90%	
	Daños por agua	0,0027				80%	
	Contaminacion Mecanica	0,0027				80%	
	Contaminación electromagnética	0,0027				50%	
	Avería de origen físico o lógico	0,0027				60%	
	Corte del suministro eléctrico	0,0027				60%	
	Condiciones inadecuadas de temperatura o humedad	0,0027				60%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de mantenimiento / actualización de equipos (hardware)	0,0164				60%	
	Modificación deliberada de la información	0,0027			70%		
	Abuso de privilegios de acceso	0,0054		80%	60%	70%	
	Robo	0,0027		90%		90%	
	Ataque destructivo	0,0027				80%	
	Uso no previsto	0,0027		60%	60%	60%	
	Emanaciones electromagnéticas	0,0027				50%	
	Caída del sistema por agotamiento de recursos	0,0164				80%	
	Pérdida de equipos	0,0027		80%		80%	
	Acceso no autorizado	0,0027		70%	60%		
	Manipulación de los equipos	0,0054		60%		60%	
	Denegación de servicio	0,0027				70%	
Acces point	Fallo de servicios de comunicaciones	0,0027				70%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de [re-]encaminamiento	0,0027		60%			
	Errores de secuencia	0,0055			60%		
	Alteración accidental de la información	0,0055			70%		
	Destrucción de información	0,0027				80%	
	Caída del sistema por agotamiento de recursos	0,0055				80%	
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		
	Abuso de privilegios de acceso	0,0055		80%	60%	70%	
	Uso no previsto	0,0027		60%	60%	60%	
	[Re-]encaminamiento de mensajes	0,0027		70%			
	Alteración de secuencia	0,0027			60%		
	Acceso no autorizado	0,0027		70%	60%		
	Análisis de tráfico	0,0055		60%			
	Interceptación de información (escucha)	0,0027		60%			
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	

Anexo D. (Continuación)

Activo	Amenaza	Frecuencia	Impacto- Dimensión Afectada				
			A	C	I	D	T
	Divulgación de información	0,0027		70%			
	Denegación de servicio	0,0027				70%	
Swichet	Fallo de servicios de comunicaciones	0,0027				70%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de [re-]encaminamiento	0,0027		60%			
	Errores de secuencia	0,0055			60%		
	Alteración accidental de la información	0,0055			70%		
	Destrucción de información	0,0027				80%	
	Caída del sistema por agotamiento de recursos	0,0055				80%	
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		
	Abuso de privilegios de acceso	0,0055		80%	60%	70%	
	Uso no previsto	0,0027		60%	60%	60%	
	[Re-]encaminamiento de mensajes	0,0027		70%			
	Alteración de secuencia	0,0027			60%		
	Acceso no autorizado	0,0027		70%	60%		
	Análisis de tráfico	0,0055		60%			
	Interceptación de información (escucha)	0,0027		60%			
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	
	Divulgación de información	0,0027		70%			
	Denegación de servicio	0,0027				70%	
Routers	Fallo de servicios de comunicaciones	0,0027				70%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de [re-]encaminamiento	0,0027		60%			
	Errores de secuencia	0,0055			60%		
	Alteración accidental de la información	0,0055			70%		
	Destrucción de información	0,0027				80%	
	Caída del sistema por agotamiento de recursos	0,0055				80%	
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		
	Abuso de privilegios de acceso	0,0055		80%	60%	70%	
	Uso no previsto	0,0027		60%	60%	60%	
	[Re-]encaminamiento de mensajes	0,0027		70%			
	Alteración de secuencia	0,0027			60%		
	Acceso no autorizado	0,0027		70%	60%		
	Análisis de tráfico	0,0055		60%			
	Interceptación de información (escucha)	0,0027		60%			
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	
	Divulgación de información	0,0027		70%			
	Denegación de servicio	0,0027				70%	

Anexo D. (Continuación)

Activo	Amenaza	Frecuencia	Impacto- Dimensión Afectada				
			A	C	I	D	T
firewalls	Fallo de servicios de comunicaciones	0,0027				70%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de [re-]encaminamiento	0,0027		60%			
	Errores de secuencia	0,0055			60%		
	Alteración accidental de la información	0,0055			70%		
	Destrucción de información	0,0027				80%	
	Caída del sistema por agotamiento de recursos	0,0055				80%	
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		
	Abuso de privilegios de acceso	0,0055		80%	60%	70%	
	Uso no previsto	0,0027		60%	60%	60%	
	[Re-]encaminamiento de mensajes	0,0027		70%			
	Alteración de secuencia	0,0027			60%		
	Acceso no autorizado	0,0027		70%	60%		
	Análisis de tráfico	0,0055		60%			
	Interceptación de información (escucha)	0,0027		60%			
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	
	Divulgación de información	0,0027		70%			
	Denegación de servicio	0,0027				70%	
cableado estructurado	Errores de los usuarios	0,0164		70%	60%	70%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de [re-]encaminamiento	0,0027		60%			
	Errores de secuencia	0,0055			60%		
	Alteración accidental de la información	0,0055			70%		
	Destrucción de información	0,0027				80%	
	Fugas de información	0,0055		80%			
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		
	Abuso de privilegios de acceso	0,0055		80%	60%	70%	
	Uso no previsto	0,0027		60%	60%	60%	
	[Re-]encaminamiento de mensajes	0,0027		70%			
	Alteración de secuencia	0,0027			60%		
	Acceso no autorizado	0,0027		70%	60%		
	Repudio	0,0027			60%		70%
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	
	Divulgación de información	0,0027		70%			
	Denegación de servicio	0,0027				70%	
Instalaciones eléctricas	Errores de los usuarios	0,0164		70%	60%	70%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de [re-]encaminamiento	0,0027		60%			
	Errores de secuencia	0,0055			60%		

Anexo D. (Continuación)

Activo	Amenaza	Frecuencia	Impacto- Dimensión Afectada				
			A	C	I	D	T
	Alteración accidental de la información	0,0055			70%		
	Destrucción de información	0,0027				80%	
	Fugas de información	0,0055		80%			
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		
	Abuso de privilegios de acceso	0,0055		80%	60%	70%	
	Uso no previsto	0,0027		60%	60%	60%	
	[Re-]encaminamiento de mensajes	0,0027		70%			
	Alteración de secuencia	0,0027			60%		
	Acceso no autorizado	0,0027		70%	60%		
	Repudio	0,0027			60%		70%
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	
	Divulgación de información	0,0027		70%			
	Denegación de servicio	0,0027				70%	
Conectividad a internet	Errores de los usuarios	0,0164		70%	60%	70%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de [re-]encaminamiento	0,0027		60%			
	Errores de secuencia	0,0055			60%		
	Alteración accidental de la información	0,0055			70%		
	Destrucción de información	0,0027				80%	
	Fugas de información	0,0055		80%			
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		
	Abuso de privilegios de acceso	0,0055		80%	60%	70%	
	Uso no previsto	0,0027		60%	60%	60%	
	[Re-]encaminamiento de mensajes	0,0027		70%			
	Alteración de secuencia	0,0027			60%		
	Acceso no autorizado	0,0027		70%	60%		
	Repudio	0,0027			60%		70%
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	
	Divulgación de información	0,0027		70%			
	Denegación de servicio	0,0027				70%	
Planta eléctrica	Fuego	0,0027				90%	
	Daños por agua	0,0027				90%	
	Otros desastres Naturales	0,0027				80%	
	Fuego	0,0027				90%	
	Daños por agua	0,0027				80%	
	Emanaciones electromagnéticas	0,0027				50%	
	Acceso no autorizado	0,0027		70%	60%		
	Ataque destructivo	0,0027				80%	
	Ocupación enemiga	0,0027		80%		80%	
Windows server 2010	Fallo de servicios de comunicaciones	0,0164				70%	
	Errores del administrador	0,0027		60%	60%	60%	

Anexo D. (Continuación)

Activo	Amenaza	Frecuencia	Impacto- Dimensión Afectada				
			A	C	I	D	T
	Errores de [re-]encaminamiento	0,0027		60%			
	Errores de secuencia	0,0054			60%		
	Alteración accidental de la información	0,0054			80%		
	Destrucción de información	0,0027				80%	
	Caída del sistema por agotamiento de recursos	0,0164				80%	
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		
	Abuso de privilegios de acceso	0,0054		80%	60%	70%	
	Uso no previsto	0,0027		70%	70%	70%	
	[Re-]encaminamiento de mensajes	0,0027		70%			
	Alteración de secuencia	0,0027			60%		
	Acceso no autorizado	0,0027		70%	60%		
	Análisis de tráfico	0,0054		60%			
	Interceptación de información (escucha)	0,0027		60%			
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	
	Divulgación de información	0,0027		70%			
	Denegación de servicio	0,0027				80%	
CgUno	Fallo de servicios de comunicaciones	0,0164				70%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de [re-]encaminamiento	0,0027		60%			
	Errores de secuencia	0,0054			60%		
	Alteración accidental de la información	0,0054			80%		
	Destrucción de información	0,0027				80%	
	Caída del sistema por agotamiento de recursos	0,0164				80%	
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		
	Abuso de privilegios de acceso	0,0054		80%	60%	70%	
	Uso no previsto	0,0027		70%	70%	70%	
	[Re-]encaminamiento de mensajes	0,0027		70%			
	Alteración de secuencia	0,0027			60%		
	Acceso no autorizado	0,0027		70%	60%		
	Análisis de tráfico	0,0054		60%			
	Interceptación de información (escucha)	0,0027		60%			
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	
	Divulgación de información	0,0027		70%			
	Denegación de servicio	0,0027				80%	
Windows	Fallo de servicios de comunicaciones	0,0164				70%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de [re-]encaminamiento	0,0027		60%			
	Errores de secuencia	0,0054			60%		

Anexo D. (Continuación)

Activo	Amenaza	Frecuencia	Impacto- Dimensión Afectada				
			A	C	I	D	T
	Alteración accidental de la información	0,0054			80%		
	Destrucción de información	0,0027				80%	
	Caída del sistema por agotamiento de recursos	0,0164				80%	
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		
	Abuso de privilegios de acceso	0,0054		80%	60%	70%	
	Uso no previsto	0,0027		70%	70%	70%	
	[Re-]encaminamiento de mensajes	0,0027		70%			
	Alteración de secuencia	0,0027			60%		
	Acceso no autorizado	0,0027		70%	60%		
	Análisis de tráfico	0,0054		60%			
	Interceptación de información (escucha)	0,0027		60%			
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	
	Divulgación de información	0,0027		70%			
	Denegación de servicio	0,0027				80%	
Ofimática	Fallo de servicios de comunicaciones	0,0164				70%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de [re-]encaminamiento	0,0027		60%			
	Errores de secuencia	0,0054			60%		
	Alteración accidental de la información	0,0054			80%		
	Destrucción de información	0,0027				80%	
	Caída del sistema por agotamiento de recursos	0,0164				80%	
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		
	Abuso de privilegios de acceso	0,0054		80%	60%	70%	
	Uso no previsto	0,0027		70%	70%	70%	
	[Re-]encaminamiento de mensajes	0,0027		70%			
	Alteración de secuencia	0,0027			60%		
	Acceso no autorizado	0,0027		70%	60%		
	Análisis de tráfico	0,0054		60%			
	Interceptación de información (escucha)	0,0027		60%			
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	
	Divulgación de información	0,0027		70%			
	Denegación de servicio	0,0027				80%	
Contratos de trabajo personal	Interrupción de otros servicios y suministros esenciales	0,0027				60%	
	Degradación de los soportes de almacenamiento de la información	0,0027				60%	
	Errores de los usuarios	0,0164		70%	70%	70%	
	Errores del administrador	0,0027		60%	60%	60%	

Anexo D. (Continuación)

Activo	Amenaza	Frecuencia	Impacto- Dimensión Afectada				
			A	C	I	D	T
	Errores de monitorización (log)	0,0027			50%		60%
	Errores de configuración	0,0164			70%		
	Escapes de información	0,0054		80%			
	Alteración accidental de la información	0,0054			70%		
	Destrucción de información	0,0027				80%	
	Fugas de información	0,0054		80%			
	Manipulación de los registros de actividad (log)	0,0028			70%		70%
	Manipulación de la configuración	0,0054	60%	60%	60%		
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		
	Abuso de privilegios de acceso	0,0054		80%	60%	70%	
	Uso no previsto	0,0027		60%	60%	60%	
	Acceso no autorizado	0,0027		70%	60%		
	Repudio	0,0164			60%		70%
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	
	Divulgación de información	0,0027		70%			
	Robo	0,0054		80%		80%	
Pólizas mantenimiento	Interrupción de otros servicios y suministros esenciales	0,0027				60%	
	Degradación de los soportes de almacenamiento de la información	0,0027				60%	
	Errores de los usuarios	0,0164		70%	70%	70%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de monitorización (log)	0,0027			50%		60%
	Errores de configuración	0,0164			70%		
	Escapes de información	0,0054		80%			
	Alteración accidental de la información	0,0054			70%		
	Destrucción de información	0,0027				80%	
	Fugas de información	0,0054		80%			
	Manipulación de los registros de actividad (log)	0,0028			70%		70%
	Manipulación de la configuración	0,0054	60%	60%	60%		
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		
	Abuso de privilegios de acceso	0,0054		80%	60%	70%	
	Uso no previsto	0,0027		60%	60%	60%	
	Acceso no autorizado	0,0027		70%	60%		
	Repudio	0,0164			60%		70%
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	
	Divulgación de información	0,0027		70%			
	Robo	0,0054		80%		80%	

Anexo D. (Continuación)

Activo	Amenaza	Frecuencia	Impacto- Dimensión Afectada				
			A	C	I	D	T
BD usuarios EPS	Interrupción de otros servicios y suministros esenciales	0,0027				60%	
	Degradación de los soportes de almacenamiento de la información	0,0027				60%	
	Errores de los usuarios	0,0164		70%	70%	70%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de monitorización (log)	0,0027			50%		60%
	Errores de configuración	0,0164			70%		
	Escapes de información	0,0054		80%			
	Alteración accidental de la información	0,0054			70%		
	Destrucción de información	0,0027				80%	
	Fugas de información	0,0054		80%			
	Manipulación de los registros de actividad (log)	0,0028			70%		70%
	Manipulación de la configuración	0,0054	60%	60%	60%		
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		
	Abuso de privilegios de acceso	0,0054		80%	60%	70%	
	Uso no previsto	0,0027		60%	60%	60%	
	Acceso no autorizado	0,0027		70%	60%		
	Repudio	0,0164			60%		70%
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	
	Divulgación de información	0,0027		70%			
	Robo	0,0054		80%		80%	
BD proveedores	Interrupción de otros servicios y suministros esenciales	0,0027				60%	
	Degradación de los soportes de almacenamiento de la información	0,0027				60%	
	Errores de los usuarios	0,0164		70%	70%	70%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de monitorización (log)	0,0027			50%		60%
	Errores de configuración	0,0164			70%		
	Escapes de información	0,0054		80%			
	Alteración accidental de la información	0,0054			70%		
	Destrucción de información	0,0027				80%	
	Fugas de información	0,0054		80%			
	Manipulación de los registros de actividad (log)	0,0028			70%		70%
	Manipulación de la configuración	0,0054	60%	60%	60%		
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		
	Abuso de privilegios de acceso	0,0054		80%	60%	70%	
	Uso no previsto	0,0027		60%	60%	60%	
	Acceso no autorizado	0,0027		70%	60%		
	Repudio	0,0164			60%		70%

Anexo D. (Continuación)

Activo	Amenaza	Frecuencia	Impacto- Dimensión Afectada				
			A	C	I	D	T
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	
	Divulgación de información	0,0027		70%			
	Robo	0,0054		80%		80%	
contabilidad	Interrupción de otros servicios y suministros esenciales	0,0027				60%	
	Degradación de los soportes de almacenamiento de la información	0,0027				60%	
	Errores de los usuarios	0,0164		70%	70%	70%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de monitorización (log)	0,0027			50%		60%
	Errores de configuración	0,0164			70%		
	Escapes de información	0,0054		80%			
	Alteración accidental de la información	0,0054			70%		
	Destrucción de información	0,0027				80%	
	Fugas de información	0,0054		80%			
	Manipulación de los registros de actividad (log)	0,0028			70%		70%
	Manipulación de la configuración	0,0054	60%	60%	60%		
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		
	Abuso de privilegios de acceso	0,0054		80%	60%	70%	
	Uso no previsto	0,0027		60%	60%	60%	
	Acceso no autorizado	0,0027		70%	60%		
	Repudio	0,0164			60%		70%
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	
	Divulgación de información	0,0027		70%			
	Robo	0,0054		80%		80%	
Mercadeo	Interrupción de otros servicios y suministros esenciales	0,0027				60%	
	Degradación de los soportes de almacenamiento de la información	0,0027				60%	
	Errores de los usuarios	0,0164		70%	70%	70%	
	Errores del administrador	0,0027		60%	60%	60%	
	Errores de monitorización (log)	0,0027			50%		60%
	Errores de configuración	0,0164			70%		
	Escapes de información	0,0054		80%			
	Alteración accidental de la información	0,0054			70%		
	Destrucción de información	0,0027				80%	
	Fugas de información	0,0054		80%			
	Manipulación de los registros de actividad (log)	0,0028			70%		70%
	Manipulación de la configuración	0,0054	60%	60%	60%		
	Suplantación de la identidad del usuario	0,0027	80%	80%	60%		

Anexo D. (Continuación)

Activo	Amenaza	Frecuencia	Impacto- Dimensión Afectada				
			A	C	I	D	T
	Abuso de privilegios de acceso	0,0054		80%	60%	70%	
	Uso no previsto	0,0027		60%	60%	60%	
	Acceso no autorizado	0,0027		70%	60%		
	Repudio	0,0164			60%		70%
	Modificación deliberada de la información	0,0027			70%		
	Destrucción de información	0,0027				80%	
	Divulgación de información	0,0027		70%			
	Robo	0,0054		80%		80%	

Fuente: El autor.

Anexo E. Impacto Potencial

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
Personal Directivo	$ 250	Deficiencias en la organización	0,0054				50%		$ 675.000	SI
		Fugas de información	0,0054		80%				$ 1.080.000	SI
		Indisponibilidad del personal	0,0054				80%		$ 1.080.000	SI
		Extorsión	0,0027		70%	70%	70%		$ 472.500	SI
		Ingeniería social	0,0054		80%	60%	60%		$ 1.080.000	SI
Administradora	$ 150	Deficiencias en la organización	0,0054				50%		$ 405.000	SI
		Fugas de información	0,0054		80%				$ 648.000	SI
		Indisponibilidad del personal	0,0054				80%		$ 648.000	SI
		Extorsión	0,0027		70%	70%	70%		$ 283.500	SI
		Ingeniería social	0,0054		80%	60%	60%		$ 648.000	SI
Jefes enfermería	$ 90	Deficiencias en la organización	0,0054				50%		$ 243.000	SI
		Fugas de información	0,0054		80%				$ 388.800	SI
		Indisponibilidad del personal	0,0054				80%		$ 388.800	SI
		Extorsión	0,0027		70%	70%	70%		$ 170.100	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 388.800	SI
Personal barra de servicios	$ 50	Deficiencias en la organización	0,0054				50%		$ 135.000	NO
		Fugas de información	0,0054		80%				$ 216.000	SI
		Indisponibilidad del personal	0,0054				80%		$ 216.000	SI
		Extorsión	0,0027		70%	70%	70%		$ 94.500	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 216.000	SI
Auxiliares enfermería	$ 50	Deficiencias en la organización	0,0054				50%		$ 135.000	NO
		Fugas de información	0,0054		80%				$ 216.000	SI
		Indisponibilidad del personal	0,0054				80%		$ 216.000	SI
		Extorsión	0,0027		70%	70%	70%		$ 94.500	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 216.000	SI
Auxiliares laboratorio	$ 50	Deficiencias en la organización	0,0054				50%		$ 135.000	NO
		Fugas de información	0,0054		80%				$ 216.000	SI
		Indisponibilidad del personal	0,0054				80%		$ 216.000	SI
		Extorsión	0,0027		70%	70%	70%		$ 94.500	NO

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
M. Generales	$ 50	Deficiencias en la organización	0,0054				50%		$ 135.000	NO
		Fugas de información	0,0054		80%				$ 216.000	SI
		Indisponibilidad del personal	0,0054				80%		$ 216.000	SI
		Extorsión	0,0027		70%	70%	70%		$ 94.500	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 216.000	SI
especialistas Médicos	$ 50	Deficiencias en la organización	0,0054				50%		$ 135.000	NO
		Fugas de información	0,0054		80%				$ 216.000	SI
		Indisponibilidad del personal	0,0054				80%		$ 216.000	SI
		Extorsión	0,0027		70%	70%	70%		$ 94.500	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 216.000	SI
generales Servicios	$ 50	Deficiencias en la organización	0,0054				50%		$ 135.000	NO
		Fugas de información	0,0054		80%				$ 216.000	SI
		Indisponibilidad del personal	0,0054				80%		$ 216.000	SI
		Extorsión	0,0027		70%	70%	70%		$ 94.500	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 216.000	SI
Contadora	$ 100	Deficiencias en la organización	0,0054				50%		$ 270.000	SI
		Fugas de información	0,0054		80%				$ 432.000	SI
		Indisponibilidad del personal	0,0054				80%		$ 432.000	SI
		Extorsión	0,0027		70%	70%	70%		$ 189.000	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 432.000	SI
Asistente contable	$ 50	Deficiencias en la organización	0,0054				50%		$ 135.000	NO
		Fugas de información	0,0054		80%				$ 216.000	SI
		Indisponibilidad del personal	0,0054				80%		$ 216.000	SI
		Extorsión	0,0027		70%	70%	70%		$ 94.500	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 216.000	SI
Revisor fiscal	$ 100	Deficiencias en la organización	0,0054				50%		$ 270.000	SI
		Fugas de información	0,0054		80%				$ 432.000	SI
		Indisponibilidad del personal	0,0054				80%		$ 432.000	SI
		Extorsión	0,0027		70%	70%	70%		$ 189.000	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 432.000	SI
gerencia Secretaria	$ 50	Deficiencias en la organización	0,0054				50%		$ 135.000	NO
		Fugas de información	0,0054		80%				$ 216.000	SI
		Indisponibilidad del personal	0,0054				80%		$ 216.000	SI

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
		Extorsión	0,0027		70%	70%	70%		$ 94.500	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 216.000	SI
asignación citas Secretaria	$ 10	Deficiencias en la organización	0,0054				50%		$ 27.000	NO
		Fugas de información	0,0054		80%				$ 43.200	NO
		Indisponibilidad del personal	0,0054				80%		$ 43.200	NO
		Extorsión	0,0027		70%	70%	70%		$ 18.900	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 43.200	NO
sistemas Ingeniero	$ 100	Deficiencias en la organización	0,0054				50%		$ 270.000	SI
		Fugas de información	0,0054		80%				$ 432.000	SI
		Indisponibilidad del personal	0,0054				80%		$ 432.000	SI
		Extorsión	0,0027		70%	70%	70%		$ 189.000	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 432.000	SI
Bacteriólogas	$ 100	Deficiencias en la organización	0,0054				50%		$ 270.000	SI
		Fugas de información	0,0054		80%				$ 432.000	SI
		Indisponibilidad del personal	0,0054				80%		$ 432.000	SI
		Extorsión	0,0027		70%	70%	70%		$ 189.000	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 432.000	SI
Mensajero	$ 3	Deficiencias en la organización	0,0054				50%		$ 8.100	NO
		Fugas de información	0,0054		80%				$ 12.960	NO
		Indisponibilidad del personal	0,0054				80%		$ 12.960	NO
		Extorsión	0,0027		70%	70%	70%		$ 5.670	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 12.960	NO
Auditores médicos	$ 100	Deficiencias en la organización	0,0054				50%		$ 270.000	SI
		Fugas de información	0,0054		80%				$ 432.000	SI
		Indisponibilidad del personal	0,0054				80%		$ 432.000	SI
		Extorsión	0,0027		70%	70%	70%		$ 189.000	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 432.000	SI
Electro médico	$ 100	Deficiencias en la organización	0,0054				50%		$ 270.000	SI
		Fugas de información	0,0054		80%				$ 432.000	SI
		Indisponibilidad del personal	0,0054				80%		$ 432.000	SI
		Extorsión	0,0027		70%	70%	70%		$ 189.000	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 432.000	SI

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
Electricista	$ 10	Deficiencias en la organización	0,0054				50%		$ 27.000	NO
		Fugas de información	0,0054		80%				$ 43.200	NO
		Indisponibilidad del personal	0,0054				80%		$ 43.200	NO
		Extorsión	0,0027		70%	70%	70%		$ 18.900	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 43.200	NO
Mantenimiento	$ 10	Deficiencias en la organización	0,0054				50%		$ 27.000	NO
		Fugas de información	0,0054		80%				$ 43.200	NO
		Indisponibilidad del personal	0,0054				80%		$ 43.200	NO
		Extorsión	0,0027		70%	70%	70%		$ 18.900	NO
		Ingeniería social	0,0054		80%	60%	60%		$ 43.200	NO
Portátiles	$ 50	Fuego	0,0027				90%		$ 121.500	NO
		Daños por agua	0,0027				80%		$ 108.000	NO
		Otros desastres Naturales	0,0027				80%		$ 108.000	NO
		Fuego	0,0027				90%		$ 121.500	NO
		Daños por agua	0,0027				80%		$ 108.000	NO
		Contaminación Mecánica	0,0027				80%		$ 108.000	NO
		Contaminación electromagnética	0,0027				50%		$ 67.500	NO
		Avería de origen físico o lógico	0,0027				60%		$ 81.000	NO
		Corte del suministro eléctrico	0,0027				60%		$ 81.000	NO
		Condiciones inadecuadas de temperatura o humedad	0,0027				60%		$ 81.000	NO
		Errores del administrador	0,0027		60%	60%	60%		$ 81.000	NO
		Errores de mantenimiento / actualización de equipos (hardware)	0,0164				60%		$ 492.000	SI
		Modificación deliberada de la información	0,0027			70%			$ 94.500	NO
		Abuso de privilegios de acceso	0,0054		80%	60%	70%		$ 216.000	SI
		Robo	0,0027		90%		90%		$ 121.500	NO
		Ataque destructivo	0,0027				80%		$ 108.000	NO
		Uso no previsto	0,0164		70%	70%	70%		$ 574.000	SI

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
		Emanaciones electromagnéticas Errores y fallos no intencionados	0,0027				50%		$ 67.500	NO
		Caída del sistema por agotamiento de recursos	0,0164				80%		$ 656.000	SI
		Pérdida de equipos	0,0027		80%		80%		$ 108.000	NO
		Acceso no autorizado	0,0027		70%	60%			$ 94.500	NO
		Manipulación de los equipos	0,0054		60%		60%		$ 162.000	NO
		Denegación de servicio	0,0027				70%		$ 94.500	NO
Equipos de cómputo	$ 90	Fuego	0,0027				90%		$ 218.700	SI
		Daños por agua	0,0027				80%		$ 194.400	NO
		Otros desastres Naturales	0,0027				80%		$ 194.400	NO
		Fuego	0,0027				90%		$ 218.700	SI
		Daños por agua	0,0027				80%		$ 194.400	NO
		Contaminación Mecánica	0,0027				80%		$ 194.400	NO
		Contaminación electromagnética	0,0027				50%		$ 121.500	NO
		Avería de origen físico o lógico	0,0027				60%		$ 145.800	NO
		Corte del suministro eléctrico	0,0027				60%		$ 145.800	NO
		Condiciones inadecuadas de temperatura o humedad	0,0027				60%		$ 145.800	NO
		Errores del administrador	0,0027		60%	60%	60%		$ 145.800	NO
		Errores de mantenimiento / actualización de equipos (hardware)	0,0164				60%		$ 885.600	SI
		Modificación deliberada de la información	0,0027			70%			$ 170.100	NO
		Abuso de privilegios de acceso	0,0054		80%	60%	70%		$ 388.800	SI
		Robo	0,0027		90%		90%		$ 218.700	SI
		Ataque destructivo	0,0027				80%		$ 194.400	NO
		Uso no previsto	0,0164		70%	70%	70%		$ 1.033.200	SI
		Emanaciones electromagnéticas	0,0027				50%		$ 121.500	NO

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
		Errores y fallos no intencionados								
		Caída del sistema por agotamiento de recursos	0,0164				80%		$ 1.180.800	SI
		Pérdida de equipos	0,0027		80%		80%		$ 194.400	NO
		Acceso no autorizado	0,0027		70%	60%			$ 170.100	NO
		Manipulación de los equipos	0,0054		60%		60%		$ 291.600	SI
		Denegación de servicio	0,0027				70%		$ 170.100	NO
Impresoras	$ 40	Fuego	0,0027				90%		$ 97.200	NO
		Daños por agua	0,0027				80%		$ 86.400	NO
		Otros desastres Naturales	0,0027				80%		$ 86.400	NO
		Fuego	0,0027				90%		$ 97.200	NO
		Daños por agua	0,0027				80%		$ 86.400	NO
		Contaminación Mecánica	0,0027				80%		$ 86.400	NO
		Contaminación electromagnética	0,0027				50%		$ 54.000	NO
		Avería de origen físico o lógico	0,0027				60%		$ 64.800	NO
		Corte del suministro eléctrico	0,0027				60%		$ 64.800	NO
		Condiciones inadecuadas de temperatura o humedad	0,0027				60%		$ 64.800	NO
		Errores del administrador	0,0027		60%	60%	60%		$ 64.800	NO
		Errores de mantenimiento / actualización de equipos (hardware)	0,0164				60%		$ 393.600	SI
		Modificación deliberada de la información	0,0027			70%			$ 75.600	NO
		Abuso de privilegios de acceso	0,0054		80%	60%	70%		$ 172.800	NO
		Robo	0,0027		90%		90%		$ 97.200	NO
		Ataque destructivo	0,0027				80%		$ 86.400	NO
		Uso no previsto	0,0164		70%	70%	70%		$ 459.200	SI
		Emanaciones electromagnéticas Errores y fallos no intencionados	0,0027				50%		$ 54.000	NO

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
		Caída del sistema por agotamiento de recursos	0,0164				80%		$ 524.800	SI
		Pérdida de equipos	0,0027		80%		80%		$ 86.400	NO
		Acceso no autorizado	0,0027		70%	60%			$ 75.600	NO
		Manipulación de los equipos	0,0054		60%		60%		$ 129.600	NO
		Denegación de servicio	0,0027				70%		$ 75.600	NO
Servidor Aplicaciones	$ 200	Fuego	0,0027				90%		$ 486.000	SI
		Daños por agua	0,0027				80%		$ 432.000	SI
		Otros desastres Naturales	0,0027				80%		$ 432.000	SI
		Fuego	0,0027				90%		$ 486.000	SI
		Daños por agua	0,0027				80%		$ 432.000	SI
		Contaminación Mecánica	0,0027				80%		$ 432.000	SI
		Contaminación electromagnética	0,0027				50%		$ 270.000	SI
		Avería de origen físico o lógico	0,0027				60%		$ 324.000	SI
		Corte del suministro eléctrico	0,0027				60%		$ 324.000	SI
		Condiciones inadecuadas de temperatura o humedad	0,0027				60%		$ 324.000	SI
		Errores del administrador	0,0027		60%	60%	60%		$ 324.000	SI
		Errores de mantenimiento / actualización de equipos (hardware)	0,0164				60%		$ 1.968.000	SI
		Modificación deliberada de la información	0,0027			70%			$ 378.000	SI
		Abuso de privilegios de acceso	0,0054		80%	60%	70%		$ 864.000	SI
		Robo	0,0027		90%		90%		$ 486.000	SI
		Ataque destructivo	0,0027				80%		$ 432.000	SI
		Uso no previsto	0,0027		60%	60%	60%		$ 324.000	SI
		Emanaciones electromagnéticas Errores y fallos no intencionados	0,0027				50%		$ 270.000	No

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
		Caída del sistema por agotamiento de recursos	0,0164				80%		$ 2.624.000	SI
		Pérdida de equipos	0,0027		80%		80%		$ 432.000	SI
		Acceso no autorizado	0,0027		70%	60%			$ 378.000	SI
		Manipulación de los equipos	0,0054		60%		60%		$ 648.000	SI
		Denegación de servicio	0,0027				70%		$ 378.000	SI
Acceso point	$ 80	Fallo de servicios de comunicaciones	0,0027				70%		$ 153.384	NO
		Errores del administrador	0,0027		60%	60%	60%		$ 131.472	NO
		Errores de [re-]encaminamiento	0,0027		60%				$ 131.472	NO
		Errores de secuencia	0,0055			60%			$ 262.992	SI
		Alteración accidental de la información	0,0055			70%			$ 306.824	SI
		Destrucción de información	0,0027				80%		$ 175.296	NO
		Caída del sistema por agotamiento de recursos	0,0055				80%		$ 350.656	SI
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 175.296	NO
		Abuso de privilegios de acceso	0,0055		80%	60%	70%		$ 350.656	SI
		Uso no previsto	0,0027		60%	60%	60%		$ 129.600	NO
		[Re-]encaminamiento de mensajes	0,0027		70%				$ 153.384	NO
		Alteración de secuencia	0,0027			60%			$ 131.472	NO
		Acceso no autorizado	0,0027		70%	60%			$ 153.384	NO
		Análisis de tráfico	0,0055		60%				$ 262.992	SI
		Interceptación de información (escucha)	0,0027		60%				$ 131.472	NO
		Modificación deliberada de la información	0,0027			70%			$ 153.384	NO
		Destrucción de información	0,0027				80%		$ 175.296	NO
		Divulgación de información	0,0027		70%				$ 153.384	NO
		Denegación de servicio	0,0027				70%		$ 153.384	NO

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
Swichet	$ 80	Fallo de servicios de comunicaciones	0,0027				70%		$ 153.384	NO
		Errores del administrador	0,0027		60%	60%	60%		$ 131.472	NO
		Errores de [re-]encaminamiento	0,0027		60%				$ 131.472	NO
		Errores de secuencia	0,0055			60%			$ 262.992	SI
		Alteración accidental de la información	0,0055			70%			$ 306.824	SI
		Destrucción de información	0,0027				80%		$ 175.296	NO
		Caída del sistema por agotamiento de recursos	0,0055				80%		$ 350.656	SI
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 175.296	NO
		Abuso de privilegios de acceso	0,0055		80%	60%	70%		$ 350.656	SI
		Uso no previsto	0,0027		60%	60%	60%		$ 129.600	NO
		[Re-]encaminamiento de mensajes	0,0027		70%				$ 153.384	NO
		Alteración de secuencia	0,0027			60%			$ 131.472	NO
		Acceso no autorizado	0,0027		70%	60%			$ 153.384	NO
		Análisis de tráfico	0,0055		60%				$ 262.992	SI
		Interceptación de información (escucha)	0,0027		60%				$ 131.472	NO
		Modificación deliberada de la información	0,0027			70%			$ 153.384	NO
		Destrucción de información	0,0027				80%		$ 175.296	NO
		Divulgación de información	0,0027		70%				$ 153.384	NO
		Denegación de servicio	0,0027				70%		$ 153.384	NO
Routers	$ 80	Fallo de servicios de comunicaciones	0,0027				70%		$ 153.384	NO
		Errores del administrador	0,0027		60%	60%	60%		$ 131.472	NO
		Errores de [re-]encaminamiento	0,0027		60%				$ 131.472	NO
		Errores de secuencia	0,0055			60%			$ 262.992	SI
		Alteración accidental de la información	0,0055			70%			$ 306.824	SI
		Destrucción de información	0,0027				80%		$ 175.296	NO

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
		Caída del sistema por agotamiento de recursos	0,0055				80%		$ 350.656	SI
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 175.296	NO
		Abuso de privilegios de acceso	0,0055		80%	60%	70%		$ 350.656	SI
		Uso no previsto	0,0027		60%	60%	60%		$ 129.600	NO
		[Re-]encaminamiento de mensajes	0,0027		70%				$ 153.384	NO
		Alteración de secuencia	0,0027			60%			$ 131.472	NO
		Acceso no autorizado	0,0027		70%	60%			$ 153.384	NO
		Análisis de tráfico	0,0055		60%				$ 262.992	SI
		Interceptación de información (escucha)	0,0027		60%				$ 131.472	NO
		Modificación deliberada de la información	0,0027			70%			$ 153.384	NO
		Destrucción de información	0,0027				80%		$ 175.296	NO
		Divulgación de información	0,0027		70%				$ 153.384	NO
		Denegación de servicio	0,0027				70%		$ 153.384	NO
firewalls	$ 80	Fallo de servicios de comunicaciones	0,0027				70%		$ 153.384	NO
		Errores del administrador	0,0027		60%	60%	60%		$ 131.472	NO
		Errores de [re-]encaminamiento	0,0027		60%				$ 131.472	NO
		Errores de secuencia	0,0055			60%			$ 262.992	SI
		Alteración accidental de la información	0,0055			70%			$ 306.824	SI
		Destrucción de información	0,0027				80%		$ 175.296	NO
		Caída del sistema por agotamiento de recursos	0,0055				80%		$ 350.656	SI
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 175.296	NO
		Abuso de privilegios de acceso	0,0055		80%	60%	70%		$ 350.656	SI
		Uso no previsto	0,0027		60%	60%	60%		$ 129.600	NO
		[Re-]encaminamiento de mensajes	0,0027		70%				$ 153.384	NO

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
		Alteración de secuencia	0,0027			60%			$ 131.472	NO
		Acceso no autorizado	0,0027		70%	60%			$ 153.384	NO
		Análisis de tráfico	0,0055		60%				$ 262.992	SI
		Interceptación de información (escucha)	0,0027		60%				$ 131.472	NO
		Modificación deliberada de la información	0,0027			70%			$ 153.384	NO
		Destrucción de información	0,0027				80%		$ 175.296	NO
		Divulgación de información	0,0027		70%				$ 153.384	NO
		Denegación de servicio	0,0027				70%		$ 153.384	NO
cableado estructurado	$ 250	Errores de los usuarios	0,0164		70%	60%	70%		$ 2.876.650	SI
		Errores del administrador	0,0027		60%	60%	60%		$ 410.850	SI
		Errores de [re-]encaminamiento	0,0027		60%				$ 410.850	NO
		Errores de secuencia	0,0055			60%			$ 821.850	SI
		Alteración accidental de la información	0,0055			70%			$ 958.825	SI
		Destrucción de información	0,0027				80%		$ 547.800	SI
		Fugas de información	0,0055		80%				$ 1.095.800	SI
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 547.800	SI
		Abuso de privilegios de acceso	0,0055		80%	60%	70%		$ 1.095.800	SI
		Uso no previsto	0,0027		60%	60%	60%		$ 405.000	SI
		[Re-]encaminamiento de mensajes	0,0027		70%				$ 479.325	SI
		Alteración de secuencia	0,0027			60%			$ 410.850	NO
		Acceso no autorizado	0,0027		70%	60%			$ 479.325	SI
		Repudio	0,0027			60%		70%	$ 479.325	SI
		Modificación deliberada de la información	0,0027			70%			$ 479.325	SI
		Destrucción de información	0,0027				80%		$ 547.800	SI
		Divulgación de información	0,0027		70%				$ 479.325	SI
		Denegación de servicio	0,0027				70%		$ 479.325	SI

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
Instalaciones eléctricas	$ 200	Errores de los usuarios	0,0164		70%	60%	70%		$ 2.301.320	SI
		Errores del administrador	0,0027		60%	60%	60%		$ 328.680	SI
		Errores de [re-]encaminamiento	0,0027		60%				$ 328.680	NO
		Errores de secuencia	0,0055			60%			$ 657.480	SI
		Alteración accidental de la información	0,0055			70%			$ 767.060	SI
		Destrucción de información	0,0027				80%		$ 438.240	SI
		Fugas de información	0,0055		80%				$ 876.640	SI
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 438.240	SI
		Abuso de privilegios de acceso	0,0055		80%	60%	70%		$ 876.640	SI
		Uso no previsto	0,0027		60%	60%	60%		$ 324.000	SI
		[Re-]encaminamiento de mensajes	0,0027		70%				$ 383.460	SI
		Alteración de secuencia	0,0027			60%			$ 328.680	NO
		Acceso no autorizado	0,0027		70%	60%			$ 383.460	SI
		Repudio	0,0027			60%		70%	$ 383.460	SI
		Modificación deliberada de la información	0,0027			70%			$ 383.460	SI
		Destrucción de información	0,0027				80%		$ 438.240	SI
		Divulgación de información	0,0027		70%				$ 383.460	SI
		Denegación de servicio	0,0027				70%		$ 383.460	SI
Conectividad a internet	$ 90	Errores de los usuarios	0,0164		70%	60%	70%		$ 1.035.594	SI
		Errores del administrador	0,0027		60%	60%	60%		$ 147.906	NO
		Errores de [re-]encaminamiento	0,0027		60%				$ 147.906	NO
		Errores de secuencia	0,0055			60%			$ 295.866	SI
		Alteración accidental de la información	0,0055			70%			$ 345.177	SI
		Destrucción de información	0,0027				80%		$ 197.208	NO
		Fugas de información	0,0055		80%				$ 394.488	SI
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 197.208	NO
		Abuso de privilegios de acceso	0,0055		80%	60%	70%		$ 394.488	SI
		Uso no previsto	0,0027		60%	60%	60%		$ 145.800	NO

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
		[Re-]encaminamiento de mensajes	0,0027		70%				$ 172.557	NO
		Alteración de secuencia	0,0027			60%			$ 147.906	NO
		Acceso no autorizado	0,0027		70%	60%			$ 172.557	NO
		Repudio	0,0027			60%		70%	$ 172.557	NO
		Modificación deliberada de la información	0,0027			70%			$ 172.557	NO
		Destrucción de información	0,0027				80%		$ 197.208	NO
		Divulgación de información	0,0027		70%				$ 172.557	NO
		Denegación de servicio	0,0027				70%		$ 172.557	NO
Planta eléctrica	$ 90	Fuego	0,0027				90%		$ 218.700	SI
		Daños por agua	0,0027				90%		$ 218.700	SI
		Otros desastres Naturales	0,0027				80%		$ 194.400	NO
		Fuego	0,0027				90%		$ 218.700	SI
		Daños por agua	0,0027				80%		$ 194.400	NO
		Emanaciones electromagnéticas Errores y fallos no intencionados	0,0027				50%		$ 121.500	NO
		Acceso no autorizado	0,0027		70%	60%			$ 170.100	NO
		Ataque destructivo	0,0027				80%		$ 194.400	NO
		Ocupación enemiga	0,0027		80%		80%		$ 194.400	NO
Windows server 2010	$ 50	Fallo de servicios de comunicaciones	0,0164				70%		$ 574.000	SI
		Errores del administrador	0,0027		60%	60%	60%		$ 81.000	NO
		Errores de [re-]encaminamiento	0,0027		60%				$ 81.000	NO
		Errores de secuencia	0,0054			60%			$ 162.000	NO
		Alteración accidental de la información	0,0054			80%			$ 216.000	SI
		Destrucción de información	0,0027				80%		$ 108.000	NO
		Caída del sistema por agotamiento de recursos	0,0164				80%		$ 656.000	SI
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 108.000	NO
		Abuso de privilegios de acceso	0,0054		80%	60%	70%		$ 216.000	SI
		Uso no previsto	0,0027		70%	70%	70%		$ 94.500	NO

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
		[Re-]encaminamiento de mensajes	0,0027		70%				$ 94.500	NO
		Alteración de secuencia	0,0027			60%			$ 81.000	NO
		Acceso no autorizado	0,0027		70%	60%			$ 94.500	NO
		Análisis de tráfico	0,0054		60%				$ 162.000	NO
		Interceptación de información (escucha)	0,0027		60%				$ 81.000	NO
		Modificación deliberada de la información	0,0027			70%			$ 94.500	NO
		Destrucción de información	0,0027				80%		$ 108.000	NO
		Divulgación de información	0,0027		70%				$ 94.500	NO
		Denegación de servicio	0,0027				80%		$ 108.000	NO
CgUno	$ 50	Fallo de servicios de comunicaciones	0,0164				70%		$ 574.000	SI
		Errores del administrador	0,0027		60%	60%	60%		$ 81.000	NO
		Errores de [re-]encaminamiento	0,0027		60%				$ 81.000	NO
		Errores de secuencia	0,0054			60%			$ 162.000	NO
		Alteración accidental de la información	0,0054			80%			$ 216.000	SI
		Destrucción de información	0,0027				80%		$ 108.000	NO
		Caída del sistema por agotamiento de recursos	0,0164				80%		$ 656.000	SI
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 108.000	NO
		Abuso de privilegios de acceso	0,0054		80%	60%	70%		$ 216.000	SI
		Uso no previsto	0,0027		70%	70%	70%		$ 94.500	NO
		[Re-]encaminamiento de mensajes	0,0027		70%				$ 94.500	NO
		Alteración de secuencia	0,0027			60%			$ 81.000	NO
		Acceso no autorizado	0,0027		70%	60%			$ 94.500	NO
		Análisis de tráfico	0,0054		60%				$ 162.000	NO
		Interceptación de información (escucha)	0,0027		60%				$ 81.000	NO
		Modificación deliberada de la información	0,0027			70%			$ 94.500	NO

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
		Destrucción de información	0,0027				80%		$ 108.000	NO
		Divulgación de información	0,0027		70%				$ 94.500	NO
		Denegación de servicio	0,0027				80%		$ 108.000	NO
Windows	$ 50	Fallo de servicios de comunicaciones	0,0164				70%		$ 574.000	SI
		Errores del administrador	0,0027		60%	60%	60%		$ 81.000	NO
		Errores de [re-]encaminamiento	0,0027		60%				$ 81.000	NO
		Errores de secuencia	0,0054			60%			$ 162.000	NO
		Alteración accidental de la información	0,0054			80%			$ 216.000	SI
		Destrucción de información	0,0027				80%		$ 108.000	NO
		Caída del sistema por agotamiento de recursos	0,0164				80%		$ 656.000	SI
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 108.000	NO
		Abuso de privilegios de acceso	0,0054		80%	60%	70%		$ 216.000	SI
		Uso no previsto	0,0027		70%	70%	70%		$ 94.500	NO
		[Re-]encaminamiento de mensajes	0,0027		70%				$ 94.500	NO
		Alteración de secuencia	0,0027			60%			$ 81.000	NO
		Acceso no autorizado	0,0027		70%	60%			$ 94.500	NO
		Análisis de tráfico	0,0054		60%				$ 162.000	NO
		Interceptación de información (escucha)	0,0027		60%				$ 81.000	NO
		Modificación deliberada de la información	0,0027			70%			$ 94.500	NO
		Destrucción de información	0,0027				80%		$ 108.000	NO
		Divulgación de información	0,0027		70%				$ 94.500	NO
		Denegación de servicio	0,0027				80%		$ 108.000	NO
Ofimática	$ 10	Fallo de servicios de comunicaciones	0,0164				70%		$ 114.800	NO
		Errores del administrador	0,0027		60%	60%	60%		$ 16.200	NO

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
		Errores de [re-]encaminamiento	0,0027		60%				$ 16.200	NO
		Errores de secuencia	0,0054			60%			$ 32.400	NO
		Alteración accidental de la información	0,0054			80%			$ 43.200	NO
		Destrucción de información	0,0027				80%		$ 21.600	NO
		Caída del sistema por agotamiento de recursos	0,0164				80%		$ 131.200	NO
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 21.600	NO
		Abuso de privilegios de acceso	0,0054		80%	60%	70%		$ 43.200	NO
		Uso no previsto	0,0027		70%	70%	70%		$ 18.900	NO
		[Re-]encaminamiento de mensajes	0,0027		70%				$ 18.900	NO
		Alteración de secuencia	0,0027			60%			$ 16.200	NO
		Acceso no autorizado	0,0027		70%	60%			$ 18.900	NO
		Análisis de tráfico	0,0054		60%				$ 32.400	NO
		Interceptación de información (escucha)	0,0027		60%				$ 16.200	NO
		Modificación deliberada de la información	0,0027			70%			$ 18.900	NO
		Destrucción de información	0,0027				80%		$ 21.600	NO
		Divulgación de información	0,0027		70%				$ 18.900	NO
		Denegación de servicio	0,0027				80%		$ 21.600	NO
Contratos de trabajo personal	$ 10	Interrupción de otros servicios y suministros esenciales	0,0027				60%		$ 16.200	NO
		Degradación de los soportes de almacenamiento de la información	0,0027				60%		$ 16.200	NO
		Errores de los usuarios	0,0164		70%	70%	70%		$ 114.800	NO
		Errores del administrador	0,0027		60%	60%	60%		$ 16.200	NO
		Errores de monitorización (log)	0,0027			50%		60%	$ 16.200	NO
		Errores de configuración	0,0164			70%			$ 114.800	NO

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
		Escapes de información	0,0054		80%				$ 43.200	NO
		Alteración accidental de la información	0,0054			70%			$ 37.800	NO
		Destrucción de información	0,0027				80%		$ 21.600	NO
		Fugas de información	0,0054		80%				$ 43.200	NO
		Manipulación de los registros de actividad (log)	0,0028			70%		70%	$ 19.530	NO
		Manipulación de la configuración	0,0054	60%	60%	60%			$ 32.400	NO
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 21.600	NO
		Abuso de privilegios de acceso	0,0054		80%	60%	70%		$ 43.200	NO
		Uso no previsto	0,0027		60%	60%	60%		$ 16.200	NO
		Acceso no autorizado	0,0027		70%	60%			$ 18.900	NO
		Repudio	0,0164			60%		70%	$ 114.800	NO
		Modificación deliberada de la información	0,0027			70%			$ 18.900	NO
		Destrucción de información	0,0027				80%		$ 21.600	NO
		Divulgación de información	0,0027		70%				$ 18.900	NO
		Robo	0,0054		80%		80%		$ 43.200	NO
Pólizas mantenimiento	$ 10	Interrupción de otros servicios y suministros esenciales	0,0027				60%		$ 16.200	NO
		Degradación de los soportes de almacenamiento de la información	0,0027				60%		$ 16.200	NO
		Errores de los usuarios	0,0164		70%	70%	70%		$ 114.800	NO
		Errores del administrador	0,0027		60%	60%	60%		$ 16.200	NO
		Errores de monitorización (log)	0,0027			50%		60%	$ 16.200	NO
		Errores de configuración	0,0164			70%			$ 114.800	NO
		Escapes de información	0,0054		80%				$ 43.200	NO
		Alteración accidental de la información	0,0054			70%			$ 37.800	NO
		Destrucción de información	0,0027				80%		$ 21.600	NO

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
		Fugas de información	0,0054		80%				$ 43.200	NO
		Manipulación de los registros de actividad (log)	0,0028			70%		70%	$ 19.530	NO
		Manipulación de la configuración	0,0054	60%	60%	60%			$ 32.400	NO
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 21.600	NO
		Abuso de privilegios de acceso	0,0054		80%	60%	70%		$ 43.200	NO
		Uso no previsto	0,0027		60%	60%	60%		$ 16.200	NO
		Acceso no autorizado	0,0027		70%	60%			$ 18.900	NO
		Repudio	0,0164			60%		70%	$ 114.800	NO
		Modificación deliberada de la información	0,0027			70%			$ 18.900	NO
		Destrucción de información	0,0027				80%		$ 21.600	NO
		Divulgación de información	0,0027		70%				$ 18.900	NO
		Robo	0,0054		80%		80%		$ 43.200	NO
BD usuarios EPS	$ 90	Interrupción de otros servicios y suministros esenciales	0,0027				60%		$ 145.800	NO
		Degradación de los soportes de almacenamiento de la información	0,0027				60%		$ 145.800	NO
		Errores de los usuarios	0,0164		70%	70%	70%		$ 1.033.200	SI
		Errores del administrador	0,0027		60%	60%	60%		$ 145.800	NO
		Errores de monitorización (log)	0,0027			50%		60%	$ 145.800	NO
		Errores de configuración	0,0164			70%			$ 1.033.200	SI
		Escapes de información	0,0054		80%				$ 388.800	SI
		Alteración accidental de la información	0,0054			70%			$ 340.200	SI
		Destrucción de información	0,0027				80%		$ 194.400	NO
		Fugas de información	0,0054		80%				$ 388.800	SI
		Manipulación de los registros de actividad (log)	0,0028			70%		70%	$ 175.770	NO

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
		Manipulación de la configuración	0,0054	60%	60%	60%			$ 291.600	SI
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 194.400	NO
		Abuso de privilegios de acceso	0,0054		80%	60%	70%		$ 388.800	SI
		Uso no previsto	0,0027		60%	60%	60%		$ 145.800	NO
		Acceso no autorizado	0,0027		70%	60%			$ 170.100	NO
		Repudio	0,0164			60%		70%	$ 1.033.200	SI
		Modificación deliberada de la información	0,0027			70%			$ 170.100	NO
		Destrucción de información	0,0027				80%		$ 194.400	NO
		Divulgación de información	0,0027		70%				$ 170.100	NO
		Robo	0,0054		80%		80%		$ 388.800	SI
BD proveedores	$ 90	Interrupción de otros servicios y suministros esenciales	0,0027				60%		$ 145.800	NO
		Degradación de los soportes de almacenamiento de la información	0,0027				60%		$ 145.800	NO
		Errores de los usuarios	0,0164		70%	70%	70%		$ 1.033.200	SI
		Errores del administrador	0,0027		60%	60%	60%		$ 145.800	NO
		Errores de monitorización (log)	0,0027			50%		60%	$ 145.800	NO
		Errores de configuración	0,0164			70%			$ 1.033.200	SI
		Escapes de información	0,0054		80%				$ 388.800	SI
		Alteración accidental de la información	0,0054			70%			$ 340.200	SI
		Destrucción de información	0,0027				80%		$ 194.400	NO
		Fugas de información	0,0054		80%				$ 388.800	SI
		Manipulación de los registros de actividad (log)	0,0028			70%		70%	$ 175.770	NO
		Manipulación de la configuración	0,0054	60%	60%	60%			$ 291.600	SI
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 194.400	NO
		Abuso de privilegios de acceso	0,0054		80%	60%	70%		$ 388.800	SI

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
		Uso no previsto	0,0027		60%	60%	60%		$ 145.800	NO
		Acceso no autorizado	0,0027		70%	60%			$ 170.100	NO
		Repudio	0,0164			60%		70%	$ 1.033.200	SI
		Modificación deliberada de la información	0,0027			70%			$ 170.100	NO
		Destrucción de información	0,0027				80%		$ 194.400	NO
		Divulgación de información	0,0027		70%				$ 170.100	NO
		Robo	0,0054		80%		80%		$ 388.800	SI
contabilidad	$ 200	Interrupción de otros servicios y suministros esenciales	0,0027				60%		$ 324.000	SI
		Degradación de los soportes de almacenamiento de la información	0,0027				60%		$ 324.000	SI
		Errores de los usuarios	0,0164		70%	70%	70%		$ 2.296.000	SI
		Errores del administrador	0,0027		60%	60%	60%		$ 324.000	SI
		Errores de monitorización (log)	0,0027			50%		60%	$ 324.000	No
		Errores de configuración	0,0164			70%			$ 2.296.000	SI
		Escapes de información	0,0054		80%				$ 864.000	SI
		Alteración accidental de la información	0,0054			70%			$ 756.000	SI
		Destrucción de información	0,0027				80%		$ 432.000	SI
		Fugas de información	0,0054		80%				$ 864.000	SI
		Manipulación de los registros de actividad (log)	0,0028			70%		70%	$ 390.600	No
		Manipulación de la configuración	0,0054	60%	60%	60%			$ 648.000	SI
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 432.000	SI
		Abuso de privilegios de acceso	0,0054		80%	60%	70%		$ 864.000	SI
		Uso no previsto	0,0027		60%	60%	60%		$ 324.000	SI
		Acceso no autorizado	0,0027		70%	60%			$ 378.000	SI
		Repudio	0,0164			60%		70%	$ 2.296.000	SI
		Modificación deliberada de la información	0,0027			70%			$ 378.000	SI

Anexo E. (Continuación)

Activo	Valor en Millones de $	Amenaza	Frecuencia	Impacto- Dimensión Afectada					Frecuencia * Impacto * Valor	Salvaguardar
				A	C	I	D	T		
		Destrucción de información	0,0027				80%		$ 432.000	SI
		Divulgación de información	0,0027		70%				$ 378.000	SI
		Robo	0,0054		80%		80%		$ 864.000	SI
Mercadeo	$ 100	Interrupción de otros servicios y suministros esenciales	0,0027				60%		$ 162.000	NO
		Degradación de los soportes de almacenamiento de la información	0,0027				60%		$ 162.000	NO
		Errores de los usuarios	0,0164		70%	70%	70%		$ 1.148.000	SI
		Errores del administrador	0,0027		60%	60%	60%		$ 162.000	NO
		Errores de monitorización (log)	0,0027			50%		60%	$ 162.000	NO
		Errores de configuración	0,0164			70%			$ 1.148.000	SI
		Escapes de información	0,0054		80%				$ 432.000	SI
		Alteración accidental de la información	0,0054			70%			$ 378.000	SI
		Destrucción de información	0,0027				80%		$ 216.000	SI
		Fugas de información	0,0054		80%				$ 432.000	SI
		Manipulación de los registros de actividad (log)	0,0028			70%		70%	$ 195.300	NO
		Manipulación de la configuración	0,0054	60%	60%	60%			$ 324.000	SI
		Suplantación de la identidad del usuario	0,0027	80%	80%	60%			$ 216.000	SI
		Abuso de privilegios de acceso	0,0054		80%	60%	70%		$ 432.000	SI
		Uso no previsto	0,0027		60%	60%	60%		$ 162.000	NO
		Acceso no autorizado	0,0027		70%	60%			$ 189.000	NO
		Repudio	0,0164			60%		70%	$ 1.148.000	SI
		Modificación deliberada de la información	0,0027			70%			$ 189.000	NO
		Destrucción de información	0,0027				80%		$ 216.000	SI
		Divulgación de información	0,0027		70%				$ 189.000	NO
		Robo	0,0054		80%		80%		$ 432.000	SI

Fuente: El autor.

Anexo F. Riesgo Residual

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
Personal Directivo	$ 250	Deficiencias en la organización	Definir responsabilidades sobre ciertas acciones o eventos, establecer jerarquías para reportar incidentes o acciones a tomar a quien corresponda	60%	$ 270.000
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 432.000
		Deficiencias en la organización	Definir responsabilidades sobre ciertas acciones o eventos, establecer jerarquías para reportar incidentes o acciones a tomar a quien corresponda	60%	$ 270.000
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 432.000
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 540.000
		Extorsión	Aplicar políticas de seguridad en cuanto a acercamiento a las autoridades	50%	$ 236.250

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
Administradora	$ 150	Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 432.000
		Deficiencias en la organización	Definir responsabilidades sobre ciertas acciones o eventos, establecer jerarquías para reportar incidentes o acciones a tomar a quien corresponda	60%	$ 162.000
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 259.200
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 324.000
		Extorsión	Aplicar políticas de seguridad en cuanto a acercamiento a las autoridades	50%	$ 141.750
		Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 259.200
Jefes enfermería	$ 90	Deficiencias en la organización	Definir responsabilidades sobre ciertas acciones o eventos, establecer jerarquías para reportar incidentes o acciones a tomar a quien corresponda	60%	$ 97.200
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 155.520
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 194.400
		Extorsión	NO APLICA	0%	$ 170.100

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 155.520
Personal barra de servicios	$ 50	Deficiencias en la organización	NO APLICA	0%	$ 135.000
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 86.400
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 108.000
		Extorsión	NO APLICA	0%	$ 94.500
		Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 86.400
Auxiliares enfermería	$ 50	Deficiencias en la organización	NO APLICA	0%	$ 135.000
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 86.400
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 108.000
		Extorsión	NO APLICA	0%	$ 94.500
		Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 86.400

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
Auxiliares laboratorio	$ 50	Deficiencias en la organización	NO APLICA	0%	$ 135.000
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 86.400
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 108.000
		Extorsión	NO APLICA	0%	$ 94.500
		Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 86.400
Médicos Generales	$ 50	Deficiencias en la organización	NO APLICA	0%	$ 135.000
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 86.400
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 108.000
		Extorsión	NO APLICA	0%	$ 94.500
		Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 86.400
Médicos especialistas	$ 50	Deficiencias en la organización	NO APLICA	0%	$ 135.000

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 86.400
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 108.000
		Extorsión	NO APLICA	0%	$ 94.500
		Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 86.400
Servicios generales	$ 50	Deficiencias en la organización	NO APLICA	0%	$ 135.000
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 86.400
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 108.000
		Extorsión	NO APLICA	0%	$ 94.500
		Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 86.400
Contadora	$ 100	Deficiencias en la organización	Definir responsabilidades sobre ciertas acciones o eventos, establecer jerarquías para reportar incidentes o acciones a tomar a quien corresponda	60%	$ 108.000

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 172.800
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 216.000
		Extorsión	NO APLICA	0%	$ 189.000
		Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 172.800
Asistente contable	$ 50	Deficiencias en la organización	NO APLICA	0%	$ 135.000
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 86.400
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 108.000
		Extorsión	NO APLICA	0%	$ 94.500
		Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 86.400
Revisor fiscal	$ 100	Deficiencias en la organización	Definir responsabilidades sobre ciertas acciones o eventos, establecer jerarquías para reportar incidentes o acciones a tomar a quien corresponda	60%	$ 108.000

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 172.800
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 216.000
		Extorsión	NO APLICA	0%	$ 189.000
		Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 172.800
Secretaria gerencia	$ 50	Deficiencias en la organización	NO APLICA	0%	$ 135.000
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 86.400
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 108.000
		Extorsión	NO APLICA	0%	$ 94.500
		Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 86.400
asignación citas Secretaria	$ 10	Deficiencias en la organización	NO APLICA	0%	$ 27.000
		Fugas de información	NO APLICA	0%	$ 43.200

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Indisponibilidad del personal	NO APLICA	0%	$ 43.200
		Extorsión	NO APLICA	0%	$ 18.900
		Ingeniería social	NO APLICA	0%	$ 43.200
Ingeniero sistemas	$ 100	Deficiencias en la organización	Definir responsabilidades sobre ciertas acciones o eventos, establecer jerarquías para reportar incidentes o acciones a tomar a quien corresponda	60%	$ 108.000
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 172.800
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 216.000
		Extorsión	NO APLICA	0%	$ 189.000
		Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 172.800
Bacteriólogas	$ 100	Deficiencias en la organización	Definir responsabilidades sobre ciertas acciones o eventos, establecer jerarquías para reportar incidentes o acciones a tomar a quien corresponda	60%	$ 108.000
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 172.800
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 216.000
		Extorsión	NO APLICA	0%	$ 189.000

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 172.800
Mensajero	$ 3	Deficiencias en la organización	NO APLICA	0%	$ 8.100
		Fugas de información	NO APLICA	0%	$ 12.960
		Indisponibilidad del personal	NO APLICA	0%	$ 12.960
		Extorsión	NO APLICA	0%	$ 5.670
		Ingeniería social	NO APLICA	0%	$ 12.960
Auditores médicos	$ 100	Deficiencias en la organización	Definir responsabilidades sobre ciertas acciones o eventos, establecer jerarquías para reportar incidentes o acciones a tomar a quien corresponda	60%	$ 108.000
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 172.800
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 216.000
		Extorsión	NO APLICA	0%	$ 189.000
		Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 172.800
médico Electro	$ 100	Deficiencias en la organización	Definir responsabilidades sobre ciertas acciones o eventos, establecer jerarquías para reportar incidentes o acciones a tomar a quien corresponda	60%	$ 108.000

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 172.800
		Indisponibilidad del personal	Capacitación de personal para asumir otras responsabilidades cuando alguien no se encuentre en su puesto de trabajo por diferentes razones	50%	$ 216.000
		Extorsión	NO APLICA	0%	$ 189.000
		Ingeniería social	Capacitación sobre buenas prácticas de seguridad informática, lectura de correos sospechosos, no dejar secciones de trabajo abiertas, digitación de claves en presencia de otras personas	60%	$ 172.800
Electricista	$ 10	Deficiencias en la organización	NO APLICA	0%	$ 27.000
		Fugas de información	NO APLICA	0%	$ 43.200
		Indisponibilidad del personal	NO APLICA	0%	$ 43.200
		Extorsión	NO APLICA	0%	$ 18.900
		Ingeniería social	NO APLICA	0%	$ 43.200
Mantenimiento	$ 10	Deficiencias en la organización	NO APLICA	0%	$ 27.000
		Fugas de información	NO APLICA	0%	$ 43.200
		Indisponibilidad del personal	NO APLICA	0%	$ 43.200
		Extorsión	NO APLICA	0%	$ 18.900
		Ingeniería social	NO APLICA	0%	$ 43.200
Portátiles	$ 50	Fuego	NO APLICA	0%	$ 121.500
		Daños por agua	NO APLICA	0%	$ 108.000

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Otros desastres Naturales	NO APLICA	0%	$ 108.000
		Fuego	NO APLICA	0%	$ 121.500
		Daños por agua	NO APLICA	0%	$ 108.000
		Contaminación Mecánica	NO APLICA	0%	$ 108.000
		Contaminación electromagnética	NO APLICA	0%	$ 67.500
		Avería de origen físico o lógico	NO APLICA	0%	$ 81.000
		Corte del suministro eléctrico	NO APLICA	0%	$ 81.000
		Condiciones inadecuadas de temperatura o humedad	NO APLICA	0%	$ 81.000
		Errores del administrador	NO APLICA	0%	$ 81.000
		Errores de mantenimiento / actualización de equipos (hardware)	Mantenimiento preventivo y correctivo de equipos de cómputo	40%	$ 295.200
		Modificación deliberada de la información	NO APLICA	0%	$ 94.500
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 86.400
		Robo	NO APLICA	0%	$ 121.500

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Ataque destructivo	NO APLICA	0%	$ 108.000
		Uso no previsto	Políticas de uso adecuado de los recursos asignados para actividades laborales	60%	$ 229.600
		Emanaciones electromagnéticas Errores y fallos no intencionados	NO APLICA	0%	$ 67.500
		Caída del sistema por agotamiento de recursos	Revisar configuración de equipos de cómputo, servidor, capacidad de la banda ancha.	70%	$ 196.800
		Pérdida de equipos	NO APLICA	0%	$ 108.000
		Acceso no autorizado	NO APLICA	0%	$ 94.500
		Manipulación de los equipos	NO APLICA	0%	$ 162.000
		Denegación de servicio	NO APLICA	0%	$ 94.500
Equipos de cómputo	$ 90	Fuego	Instalación de detectores de humo, extinguidores, adquisición de pólizas	50%	$ 109.350
		Daños por agua	NO APLICA	0%	$ 194.400
		Otros desastres Naturales	NO APLICA	0%	$ 194.400
		Fuego	Instalación de detectores de humo, extinguidores, adquisición de pólizas	50%	$ 109.350
		Daños por agua	NO APLICA	0%	$ 194.400
		Contaminación Mecánica	NO APLICA	0%	$ 194.400
		Contaminación electromagnética	NO APLICA	0%	$ 121.500

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Avería de origen físico o lógico	NO APLICA	0%	$ 145.800
		Corte del suministro eléctrico	NO APLICA	0%	$ 145.800
		Condiciones inadecuadas de temperatura o humedad	NO APLICA	0%	$ 145.800
		Errores del administrador	NO APLICA	0%	$ 145.800
		Errores de mantenimiento / actualización de equipos (hardware)	Mantenimiento preventivo y correctivo de equipos de cómputo	40%	$ 531.360
		Modificación deliberada de la información	NO APLICA	0%	$ 170.100
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 155.520
		Robo	Políticas de escritorio limpio, implantación de seguridad en las instalaciones, monitorización de la red, asignación de perfiles de acuerdo a sus funciones	60%	$ 87.480
		Ataque destructivo	NO APLICA	0%	$ 194.400
		Uso no previsto	Políticas de uso adecuado de los recursos asignados para actividades laborales	60%	$ 413.280
		Emanaciones electromagnéticas Errores y fallos no	NO APLICA	0%	$ 121.500

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		intencionados			
		Caída del sistema por agotamiento de recursos	Revisar configuración de equipos de cómputo, servidor, capacidad de la banda ancha.	70%	$ 354.240
		Pérdida de equipos	NO APLICA	0%	$ 194.400
		Acceso no autorizado	NO APLICA	0%	$ 170.100
		Manipulación de los equipos	Sistema de monitoreo de integridad de detección de intrusos (HIDS)	50%	$ 145.800
		Denegación de servicio	NO APLICA	0%	$ 170.100
Impresoras	$ 40	Fuego	NO APLICA	0%	$ 97.200
		Daños por agua	NO APLICA	0%	$ 86.400
		Otros desastres Naturales	NO APLICA	0%	$ 86.400
		Fuego	NO APLICA	0%	$ 97.200
		Daños por agua	NO APLICA	0%	$ 86.400
		Contaminación Mecánica	NO APLICA	0%	$ 86.400
		Contaminación electromagnética	NO APLICA	0%	$ 54.000
		Avería de origen físico o lógico	NO APLICA	0%	$ 64.800
		Corte del suministro eléctrico	NO APLICA	0%	$ 64.800
		Condiciones inadecuadas de temperatura o humedad	NO APLICA	0%	$ 64.800

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Errores del administrador	NO APLICA	0%	$ 64.800
		Errores de mantenimiento / actualización de equipos (hardware)	Mantenimiento preventivo y correctivo de equipos de cómputo	40%	$ 236.160
		Modificación deliberada de la información	NO APLICA	0%	$ 75.600
		Abuso de privilegios de acceso	NO APLICA	0%	$ 172.800
		Robo	NO APLICA	0%	$ 97.200
		Ataque destructivo	NO APLICA	0%	$ 86.400
		Uso no previsto	Políticas de uso adecuado de los recursos asignados para actividades laborales	60%	$ 183.680
		Emanaciones electromagnéticas Errores y fallos no intencionados	NO APLICA	0%	$ 54.000
		Caída del sistema por agotamiento de recursos	Revisar configuración de equipos de cómputo, servidor, capacidad de la banda ancha.	70%	$ 157.440
		Pérdida de equipos	NO APLICA	0%	$ 86.400
		Acceso no autorizado	NO APLICA	0%	$ 75.600
		Manipulación de los equipos	NO APLICA	0%	$ 129.600
		Denegación de servicio	NO APLICA	0%	$ 75.600

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
Servidor Aplicaciones	$ 200	Fuego	Instalación de detectores de humo, extinguidores, adquisición de pólizas	50%	$ 243.000
		Daños por agua	Instalación de detectores de humedad	50%	$ 216.000
		Otros desastres Naturales	Adquisición Pólizas	60%	$ 172.800
		Fuego	Instalación de detectores de humo, extinguidores, adquisición de pólizas	50%	$ 243.000
		Daños por agua	Instalación de detectores de humedad	50%	$ 216.000
		Contaminación Mecánica	Mantenimiento general al cuarto técnico donde se encuentra el servidor, además mantenimiento preventivo por parte del personal técnico.	50%	$ 216.000
		Contaminación electromagnética	Ubicación de servidor lejos de sala de RX, esa sala debe tener paredes cubiertas de plomo para evitar fuga de radiación	40%	$ 162.000
		Avería de origen físico o lógico	Realizar mantenimiento preventivo periódicamente	40%	$ 194.400
		Corte del suministro eléctrico	Instalación de planta eléctrica inteligente, que tome el control apenas hayan fallos de energía, esta debe ser online, para el sea transparente para los equipos.	50%	$ 162.000
		Condiciones inadecuadas de temperatura o humedad	Mantenimiento aire acondicionado, detectores de humedad.	40%	$ 194.400
		Errores del administrador	Revisión de configuraciones y actualizaciones	50%	$ 162.000
		Errores de mantenimiento / actualización de equipos (hardware)	Mantenimiento preventivo y correctivo de equipos de cómputo	40%	$1.180.800
		Modificación deliberada de la	Aplicar políticas de integridad de la información	60%	$ 151.200

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		información			
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 345.600
		Robo	Políticas de escritorio limpio, implantación de seguridad en las instalaciones, monitorización de la red, asignación de perfiles de acuerdo a sus funciones	60%	$ 194.400
		Ataque destructivo	Adquisición de pólizas	50%	$ 216.000
		Uso no previsto	Políticas de uso adecuado de los recursos asignados para actividades laborales	60%	$ 129.600
		Emanaciones electromagnéticas Errores y fallos no intencionados	NO APLICA	0%	$ 270.000
		Caída del sistema por agotamiento de recursos	Revisar configuración de equipos de cómputo, servidor, capacidad de la banda ancha.	70%	$ 787.200
		Pérdida de equipos	Control de acceso físico y pólizas de seguro	50%	$ 216.000
		Acceso no autorizado	Tomar medias sobre el ingreso a las instalaciones de la empresa, configuración adecuada de firewall, IDS, implementación de políticas de escritorio limpio, uso de contraseñas para acceso al sistema	60%	$ 151.200
		Manipulación de los equipos	Sistema de monitoreo de integridad de detección de intrusos (HIDS)	50%	$ 324.000
		Denegación de servicio	instalación de IDS, ups en buenas condiciones, asignación de buen espacio de banda ancha, protección antivirus.	60%	$ 151.200

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
Acceso point	$ 80	Fallo de servicios de comunicaciones	NO APLICA	0%	$ 153.384
		Errores del administrador	NO APLICA	0%	$ 131.472
		Errores de [re-]encaminamiento	NO APLICA	0%	$ 131.472
		Errores de secuencia	Instalación y configuración correcta de IDS	40%	$ 157.795
		Alteración accidental de la información	Prohibición de medios de almacenamiento externo, deshabilitar puertos USB de los equipos de cómputo, en caso de ser autorizados medios extraíbles, tomar las medidas preventivas de no dejarlos expuestos, guardarlos en sitios seguros	60%	$ 122.730
		Destrucción de información	NO APLICA	0%	$ 175.296
		Caída del sistema por agotamiento de recursos	Revisar configuración de equipos de cómputo, servidor, capacidad de la banda ancha.	70%	$ 105.197
		Suplantación de la identidad del usuario	NO APLICA	0%	$ 175.296
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 140.262
		Uso no previsto	NO APLICA	0%	$ 129.600
		[Re-]encaminamiento de mensajes	NO APLICA	0%	$ 153.384
		Alteración de secuencia	NO APLICA	0%	$ 131.472

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Acceso no autorizado	NO APLICA	0%	$ 153.384
		Análisis de tráfico	Monitorear el tráfico de la red	50%	$ 131.496
		Interceptación de información (escucha)	NO APLICA	0%	$ 131.472
		Modificación deliberada de la información	NO APLICA	0%	$ 153.384
		Destrucción de información	NO APLICA	0%	$ 175.296
		Divulgación de información	NO APLICA	0%	$ 153.384
		Denegación de servicio	NO APLICA	0%	$ 153.384
Swichet	$ 80	Fallo de servicios de comunicaciones	NO APLICA	0%	$ 153.384
		Errores del administrador	NO APLICA	0%	$ 131.472
		Errores de [re-]encaminamiento	NO APLICA	0%	$ 131.472
		Errores de secuencia	Instalación y configuración correcta de IDS	40%	$ 157.795
		Alteración accidental de la información	Prohibición de medios de almacenamiento externo, deshabilitar puertos USB de los equipos de cómputo, en caso de ser autorizados medios extraíbles, tomar las medidas preventivas de no dejarlos expuestos, guardarlos en sitios seguros	60%	$ 122.730
		Destrucción de	NO APLICA	0%	$ 175.296

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		información			
		Caída del sistema por agotamiento de recursos	Revisar configuración de equipos de cómputo, servidor, capacidad de la banda ancha.	70%	$ 105.197
		Suplantación de la identidad del usuario	NO APLICA	0%	$ 175.296
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 140.262
		Uso no previsto	NO APLICA	0%	$ 129.600
		[Re-]encaminamiento de mensajes	NO APLICA	0%	$ 153.384
		Alteración de secuencia	NO APLICA	0%	$ 131.472
		Acceso no autorizado	NO APLICA	0%	$ 153.384
		Análisis de tráfico	Monitorear el tráfico de la red	50%	$ 131.496
		Interceptación de información (escucha)	NO APLICA	0%	$ 131.472
		Modificación deliberada de la información	NO APLICA	0%	$ 153.384
		Destrucción de información	NO APLICA	0%	$ 175.296
		Divulgación de información	NO APLICA	0%	$ 153.384

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Denegación de servicio	NO APLICA	0%	$ 153.384
Routers	$ 80	Fallo de servicios de comunicaciones	NO APLICA	0%	$ 153.384
		Errores del administrador	NO APLICA	0%	$ 131.472
		Errores de [re-]encaminamiento	NO APLICA	0%	$ 131.472
		Errores de secuencia	Instalación y configuración correcta de IDS	40%	$ 157.795
		Alteración accidental de la información	Prohibición de medios de almacenamiento externo, deshabilitar puertos USB de los equipos de cómputo, en caso de ser autorizados medios extraíbles, tomar las medidas preventivas de no dejarlos expuestos, guardarlos en sitios seguros	60%	$ 122.730
		Destrucción de información	NO APLICA	0%	$ 175.296
		Caída del sistema por agotamiento de recursos	Revisar configuración de equipos de cómputo, servidor, capacidad de la banda ancha.	70%	$ 105.197
		Suplantación de la identidad del usuario	NO APLICA	0%	$ 175.296
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 140.262
		Uso no previsto	NO APLICA	0%	$ 129.600
		[Re-]encaminamiento de mensajes	NO APLICA	0%	$ 153.384

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Alteración de secuencia	NO APLICA	0%	$ 131.472
		Acceso no autorizado	NO APLICA	0%	$ 153.384
		Análisis de tráfico	Monitorear el tráfico de la red	50%	$ 131.496
		Interceptación de información (escucha)	NO APLICA	0%	$ 131.472
		Modificación deliberada de la información	NO APLICA	0%	$ 153.384
		Destrucción de información	NO APLICA	0%	$ 175.296
		Divulgación de información	NO APLICA	0%	$ 153.384
		Denegación de servicio	NO APLICA	0%	$ 153.384
firewalls	$ 80	Fallo de servicios de comunicaciones	NO APLICA	0%	$ 153.384
		Errores del administrador	NO APLICA	0%	$ 131.472
		Errores de [re-]encaminamiento	NO APLICA	0%	$ 131.472
		Errores de secuencia	Instalación y configuración correcta de IDS	40%	$ 157.795
		Alteración accidental de la información	Prohibición de medios de almacenamiento externo, deshabilitar puertos USB de los equipos de cómputo, en caso de ser autorizados medios extraíbles, tomar las medidas	60%	$ 122.730

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
			preventivas de no dejarlos expuestos, guardarlos en sitios seguros		
		Destrucción de información	NO APLICA	0%	$ 175.296
		Caída del sistema por agotamiento de recursos	Revisar configuración de equipos de cómputo, servidor, capacidad de la banda ancha.	70%	$ 105.197
		Suplantación de la identidad del usuario	NO APLICA	0%	$ 175.296
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 140.262
		Uso no previsto	NO APLICA	0%	$ 129.600
		[Re-]encaminamiento de mensajes	NO APLICA	0%	$ 153.384
		Alteración de secuencia	NO APLICA	0%	$ 131.472
		Acceso no autorizado	NO APLICA	0%	$ 153.384
		Análisis de tráfico	Monitorear el tráfico de la red	50%	$ 131.496
		Interceptación de información (escucha)	NO APLICA	0%	$ 131.472
		Modificación deliberada de la información	NO APLICA	0%	$ 153.384
		Destrucción de	NO APLICA	0%	$ 175.296

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		información			
		Divulgación de información	NO APLICA	0%	$ 153.384
		Denegación de servicio	NO APLICA	0%	$ 153.384
cableado estructurado	$ 250	Errores de los usuarios	Instalación de programas sólo por personal capacitado y autorizado.	50%	$1.438.325
		Errores del administrador	Revisión de configuraciones y actualizaciones	50%	$ 205.425
		Errores de [re-]encaminamiento	NO APLICA	0%	$ 410.850
		Errores de secuencia	Instalación y configuración correcta de IDS	40%	$ 493.110
		Alteración accidental de la información	Prohibición de medios de almacenamiento externo, deshabilitar puertos USB de los equipos de cómputo, en caso de ser autorizados medios extraíbles, tomar las medidas preventivas de no dejarlos expuestos, guardarlos en sitios seguros	60%	$ 383.530
		Destrucción de información	Guardas en sitios seguros unidades externas de almacenamiento donde se grabe información confidencial, procedimiento adecuado de las copias de seguridad, prohibir acceso de personal no autorizado a sitios restringidos.	40%	$ 328.680
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 438.320
		Suplantación de la identidad del usuario	Monitoreo del tráfico, autenticación de usuarios	60%	$ 219.120

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 438.320
		Uso no previsto	Políticas de uso adecuado de los recursos asignados para actividades laborales	60%	$ 162.000
		[Re-]encaminamiento de mensajes	Control sobre el uso de cuentas de correos electrónicos, acceso a la red, negación de redes sociales, chat, foros, entre otros	50%	$ 239.663
		Alteración de secuencia	NO APLICA	0%	$ 410.850
		Acceso no autorizado	Tomar medias sobre el ingreso a las instalaciones de la empresa, configuración adecuada de firewall, IDS, implementación de políticas de escritorio limpio, uso de contraseñas para acceso al sistema	60%	$ 191.730
		Repudio	Aplicación de políticas de seguridad en cuanto a integridad de la información	40%	$ 287.595
		Modificación deliberada de la información	Aplicar políticas de integridad de la información	60%	$ 191.730
		Destrucción de información	Guardas en sitios seguros unidades externas de almacenamiento donde se grabe información confidencial, procedimiento adecuado de las copias de seguridad, prohibir acceso de personal no autorizado a sitios restringidos.	40%	$ 328.680
		Divulgación de información	aplicar políticas de confidencialidad de la información	40%	$ 287.595
		Denegación de servicio	instalación de IDS, ups en buenas condiciones, asignación de buen espacio de banda ancha, protección antivirus,	60%	$ 191.730
Instalaciones eléctricas	$ 200	Errores de los usuarios	Instalación de programas sólo por personal capacitado y autorizado.	50%	$1.150.660
		Errores del administrador	Revisión de configuraciones y actualizaciones	50%	$ 164.340

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Errores de [re-]encaminamiento	NO APLICA	0%	$ 328.680
		Errores de secuencia	Instalación y configuración correcta de IDS	40%	$ 394.488
		Alteración accidental de la información	Prohibición de medios de almacenamiento externo, deshabilitar puertos USB de los equipos de cómputo, en caso de ser autorizados medios extraíbles, tomar las medidas preventivas de no dejarlos expuestos, guardarlos en sitios seguros	60%	$ 306.824
		Destrucción de información	Guardas en sitios seguros unidades externas de almacenamiento donde se grabe información confidencial, procedimiento adecuado de las copias de seguridad, prohibir acceso de personal no autorizado a sitios restringidos.	40%	$ 262.944
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 350.656
		Suplantación de la identidad del usuario	Monitoreo del tráfico, autenticación de usuarios	60%	$ 175.296
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 350.656
		Uso no previsto	Políticas de uso adecuado de los recursos asignados para actividades laborales	60%	$ 129.600
		[Re-]encaminamiento de mensajes	Control sobre el uso de cuentas de correos electrónicos, acceso a la red, negación de redes sociales, chat, foros, entre otros	50%	$ 191.730
		Alteración de secuencia	NO APLICA	0%	$ 328.680

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Acceso no autorizado	Tomar medias sobre el ingreso a las instalaciones de la empresa, configuración adecuada de firewall, IDS, implementación de políticas de escritorio limpio, uso de contraseñas para acceso al sistema	60%	$ 153.384
		Repudio	Aplicación de políticas de seguridad en cuanto a integridad de la información	40%	$ 230.076
		Modificación deliberada de la información	Aplicar políticas de integridad de la información	60%	$ 153.384
		Destrucción de información	Guardas en sitios seguros unidades externas de almacenamiento donde se grabe información confidencial, procedimiento adecuado de las copias de seguridad, prohibir acceso de personal no autorizado a sitios restringidos.	40%	$ 262.944
		Divulgación de información	aplicar políticas de confidencialidad de la información	40%	$ 230.076
		Denegación de servicio	instalación de IDS, ups en buenas condiciones, asignación de buen espacio de banda ancha, protección antivirus,	60%	$ 153.384
Conectividad a internet	$ 90	Errores de los usuarios	Instalación de programas sólo por personal capacitado y autorizado.	50%	$ 517.797
		Errores del administrador	NO APLICA	0%	$ 147.906
		Errores de [re-]encaminamiento	NO APLICA	0%	$ 147.906
		Errores de secuencia	Instalación y configuración correcta de IDS	40%	$ 177.520
		Alteración accidental de la información	Prohibición de medios de almacenamiento externo, deshabilitar puertos USB de los equipos de cómputo, en caso de ser autorizados medios extraíbles, tomar las medidas preventivas de no dejarlos expuestos, guardarlos en sitios seguros	60%	$ 138.071

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Destrucción de información	NO APLICA	0%	$ 197.208
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 157.795
		Suplantación de la identidad del usuario	NO APLICA	0%	$ 197.208
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 157.795
		Uso no previsto	NO APLICA	0%	$ 145.800
		[Re-]encaminamiento de mensajes	NO APLICA	0%	$ 172.557
		Alteración de secuencia	NO APLICA	0%	$ 147.906
		Acceso no autorizado	NO APLICA	0%	$ 172.557
		Repudio	NO APLICA	0%	$ 172.557
		Modificación deliberada de la información	NO APLICA	0%	$ 172.557
		Destrucción de información	NO APLICA	0%	$ 197.208
		Divulgación de información	NO APLICA	0%	$ 172.557
		Denegación de servicio	NO APLICA	0%	$ 172.557
Planta eléctr	$ 90	Fuego	Instalación de detectores de humo, extinguidores, adquisición de pólizas	50%	$ 109.350

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Daños por agua	Instalación de detectores de humedad	50%	$ 109.350
		Otros desastres Naturales	NO APLICA	0%	$ 194.400
		Fuego	Instalación de detectores de humo, extinguidores, adquisición de pólizas	50%	$ 109.350
		Daños por agua	NO APLICA	0%	$ 194.400
		Emanaciones electromagnéticas Errores y fallos no intencionados	NO APLICA	0%	$ 121.500
		Acceso no autorizado	NO APLICA	0%	$ 170.100
		Ataque destructivo	NO APLICA	0%	$ 194.400
		Ocupación enemiga	NO APLICA	0%	$ 194.400
Windows server 2010	$ 50	Fallo de servicios de comunicaciones	Instalación de equipos de comunicaciones de apoyo, en caso de que los equipos primarios se vean afectados	60%	$ 229.600
		Errores del administrador	NO APLICA	0%	$ 81.000
		Errores de [re-]encaminamiento	NO APLICA	0%	$ 81.000
		Errores de secuencia	NO APLICA	0%	$ 162.000
		Alteración accidental de la información	Prohibición de medios de almacenamiento externo, deshabilitar puertos USB de los equipos de cómputo, en caso de ser autorizados medios extraíbles, tomar las medidas preventivas de no dejarlos expuestos, guardarlos en sitios seguros	60%	$ 86.400
		Destrucción de información	NO APLICA	0%	$ 108.000

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Caída del sistema por agotamiento de recursos	Revisar configuración de equipos de cómputo, servidor, capacidad de la banda ancha.	70%	$ 196.800
		Suplantación de la identidad del usuario	NO APLICA	0%	$ 108.000
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 86.400
		Uso no previsto	NO APLICA	0%	$ 94.500
		[Re-]encaminamiento de mensajes	NO APLICA	0%	$ 94.500
		Alteración de secuencia	NO APLICA	0%	$ 81.000
		Acceso no autorizado	NO APLICA	0%	$ 94.500
		Análisis de tráfico	NO APLICA	0%	$ 162.000
		Interceptación de información (escucha)	NO APLICA	0%	$ 81.000
		Modificación deliberada de la información	NO APLICA	0%	$ 94.500
		Destrucción de información	NO APLICA	0%	$ 108.000
		Divulgación de información	NO APLICA	0%	$ 94.500
		Denegación de servicio	NO APLICA	0%	$ 108.000

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
CgUno	$ 50	Fallo de servicios de comunicaciones	Instalación de equipos de comunicaciones de apoyo, en caso de que los equipos primarios se vean afectados	60%	$ 229.600
		Errores del administrador	NO APLICA	0%	$ 81.000
		Errores de [re-]encaminamiento	NO APLICA	0%	$ 81.000
		Errores de secuencia	NO APLICA	0%	$ 162.000
		Alteración accidental de la información	Prohibición de medios de almacenamiento externo, deshabilitar puertos USB de los equipos de cómputo, en caso de ser autorizados medios extraíbles, tomar las medidas preventivas de no dejarlos expuestos, guardarlos en sitios seguros	60%	$ 86.400
		Destrucción de información	NO APLICA	0%	$ 108.000
		Caída del sistema por agotamiento de recursos	Revisar configuración de equipos de cómputo, servidor, capacidad de la banda ancha.	70%	$ 196.800
		Suplantación de la identidad del usuario	NO APLICA	0%	$ 108.000
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 86.400
		Uso no previsto	NO APLICA	0%	$ 94.500
		[Re-]encaminamiento de mensajes	NO APLICA	0%	$ 94.500
		Alteración de secuencia	NO APLICA	0%	$ 81.000
		Acceso no autorizado	NO APLICA	0%	$ 94.500

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Análisis de tráfico	NO APLICA	0%	$ 162.000
		Interceptación de información (escucha)	NO APLICA	0%	$ 81.000
		Modificación deliberada de la información	NO APLICA	0%	$ 94.500
		Destrucción de información	NO APLICA	0%	$ 108.000
		Divulgación de información	NO APLICA	0%	$ 94.500
		Denegación de servicio	NO APLICA	0%	$ 108.000
Windows	$ 50	Fallo de servicios de comunicaciones	Instalación de equipos de comunicaciones de apoyo, en caso de que los equipos primarios se vean afectados	60%	$ 229.600
		Errores del administrador	NO APLICA	0%	$ 81.000
		Errores de [re-]encaminamiento	NO APLICA	0%	$ 81.000
		Errores de secuencia	NO APLICA	0%	$ 162.000
		Alteración accidental de la información	Prohibición de medios de almacenamiento externo, deshabilitar puertos USB de los equipos de cómputo, en caso de ser autorizados medios extraíbles, tomar las medidas preventivas de no dejarlos expuestos, guardarlos en sitios seguros	60%	$ 86.400
		Destrucción de información	NO APLICA	0%	$ 108.000

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Caída del sistema por agotamiento de recursos	Revisar configuración de equipos de cómputo, servidor, capacidad de la banda ancha.	70%	$ 196.800
		Suplantación de la identidad del usuario	NO APLICA	0%	$ 108.000
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 86.400
		Uso no previsto	NO APLICA	0%	$ 94.500
		[Re-]encaminamiento de mensajes	NO APLICA	0%	$ 94.500
		Alteración de secuencia	NO APLICA	0%	$ 81.000
		Acceso no autorizado	NO APLICA	0%	$ 94.500
		Análisis de tráfico	NO APLICA	0%	$ 162.000
		Interceptación de información (escucha)	NO APLICA	0%	$ 81.000
		Modificación deliberada de la información	NO APLICA	0%	$ 94.500
		Destrucción de información	NO APLICA	0%	$ 108.000
		Divulgación de información	NO APLICA	0%	$ 94.500
		Denegación de servicio	NO APLICA	0%	$ 108.000

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
Ofimática	$ 10	Fallo de servicios de comunicaciones	NO APLICA	0%	$ 114.800
		Errores del administrador	NO APLICA	0%	$ 16.200
		Errores de [re-]encaminamiento	NO APLICA	0%	$ 16.200
		Errores de secuencia	NO APLICA	0%	$ 32.400
		Alteración accidental de la información	NO APLICA	0%	$ 43.200
		Destrucción de información	NO APLICA	0%	$ 21.600
		Caída del sistema por agotamiento de recursos	NO APLICA	0%	$ 131.200
		Suplantación de la identidad del usuario	NO APLICA	0%	$ 21.600
		Abuso de privilegios de acceso	NO APLICA	0%	$ 43.200
		Uso no previsto	NO APLICA	0%	$ 18.900
		[Re-]encaminamiento de mensajes	NO APLICA	0%	$ 18.900
		Alteración de secuencia	NO APLICA	0%	$ 16.200
		Acceso no autorizado	NO APLICA	0%	$ 18.900
		Análisis de tráfico	NO APLICA	0%	$ 32.400

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Interceptación de información (escucha)	NO APLICA	0%	$ 16.200
		Modificación deliberada de la información	NO APLICA	0%	$ 18.900
		Destrucción de información	NO APLICA	0%	$ 21.600
		Divulgación de información	NO APLICA	0%	$ 18.900
		Denegación de servicio	NO APLICA	0%	$ 21.600
Contratos de trabajo personal	$ 10	Interrupción de otros servicios y suministros esenciales	NO APLICA	0%	$ 16.200
		Degradación de los soportes de almacenamiento de la información	NO APLICA	0%	$ 16.200
		Errores de los usuarios	NO APLICA	0%	$ 114.800
		Errores del administrador	NO APLICA	0%	$ 16.200
		Errores de monitorización (log)	NO APLICA	0%	$ 16.200
		Errores de configuración	NO APLICA	0%	$ 114.800

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Escapes de información	NO APLICA	0%	$ 43.200
		Alteración accidental de la información	NO APLICA	0%	$ 37.800
		Destrucción de información	NO APLICA	0%	$ 21.600
		Fugas de información	NO APLICA	0%	$ 43.200
		Manipulación de los registros de actividad (log)	NO APLICA	0%	$ 19.530
		Manipulación de la configuración	NO APLICA	0%	$ 32.400
		Suplantación de la identidad del usuario	NO APLICA	0%	$ 21.600
		Abuso de privilegios de acceso	NO APLICA	0%	$ 43.200
		Uso no previsto	NO APLICA	0%	$ 16.200
		Acceso no autorizado	NO APLICA	0%	$ 18.900
		Repudio	NO APLICA	0%	$ 114.800
		Modificación deliberada de la información	NO APLICA	0%	$ 18.900
		Destrucción de información	NO APLICA	0%	$ 21.600

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Divulgación de información	NO APLICA	0%	$ 18.900
		Robo	NO APLICA	0%	$ 43.200
Pólizas mantenimiento	$ 10	Interrupción de otros servicios y suministros esenciales	NO APLICA	0%	$ 16.200
		Degradación de los soportes de almacenamiento de la información	NO APLICA	0%	$ 16.200
		Errores de los usuarios	NO APLICA	0%	$ 114.800
		Errores del administrador	NO APLICA	0%	$ 16.200
		Errores de monitorización (log)	NO APLICA	0%	$ 16.200
		Errores de configuración	NO APLICA	0%	$ 114.800
		Escapes de información	NO APLICA	0%	$ 43.200
		Alteración accidental de la información	NO APLICA	0%	$ 37.800
		Destrucción de información	NO APLICA	0%	$ 21.600
		Fugas de información	NO APLICA	0%	$ 43.200

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Manipulación de los registros de actividad (log)	NO APLICA	0%	$ 19.530
		Manipulación de la configuración	NO APLICA	0%	$ 32.400
		Suplantación de la identidad del usuario	NO APLICA	0%	$ 21.600
		Abuso de privilegios de acceso	NO APLICA	0%	$ 43.200
		Uso no previsto	NO APLICA	0%	$ 16.200
		Acceso no autorizado	NO APLICA	0%	$ 18.900
		Repudio	NO APLICA	0%	$ 114.800
		Modificación deliberada de la información	NO APLICA	0%	$ 18.900
		Destrucción de información	NO APLICA	0%	$ 21.600
		Divulgación de información	NO APLICA	0%	$ 18.900
		Robo	NO APLICA	0%	$ 43.200
BD usuarios EPS	$ 90	Interrupción de otros servicios y suministros esenciales	NO APLICA	0%	$ 145.800
		Degradación de los soportes de almacenamiento de	NO APLICA	0%	$ 145.800

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		la información			
		Errores de los usuarios	Instalación de programas sólo por personal capacitado y autorizado.	50%	$ 516.600
		Errores del administrador	NO APLICA	0%	$ 145.800
		Errores de monitorización (log)	NO APLICA	0%	$ 145.800
		Errores de configuración	Configuración correcta de privilegios, perfiles de usuarios.	60%	$ 413.280
		Escapes de información	Aplicación de Políticas de confidencialidad de la información	50%	$ 194.400
		Alteración accidental de la información	Prohibición de medios de almacenamiento externo, deshabilitar puertos USB de los equipos de cómputo, en caso de ser autorizados medios extraíbles, tomar las medidas preventivas de no dejarlos expuestos, guardarlos en sitios seguros	60%	$ 136.080
		Destrucción de información	NO APLICA	0%	$ 194.400
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 155.520
		Manipulación de los registros de actividad (log)	NO APLICA	0%	$ 175.770
		Manipulación de la configuración	Sistemas de monitoreo de integridad	50%	$ 145.800

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Suplantación de la identidad del usuario	NO APLICA	0%	$ 194.400
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 155.520
		Uso no previsto	NO APLICA	0%	$ 145.800
		Acceso no autorizado	NO APLICA	0%	$ 170.100
		Repudio	Aplicación de políticas de seguridad en cuanto a integridad de la información	40%	$ 619.920
		Modificación deliberada de la información	NO APLICA	0%	$ 170.100
		Destrucción de información	NO APLICA	0%	$ 194.400
		Divulgación de información	NO APLICA	0%	$ 170.100
		Robo	Políticas de escritorio limpio, implantación de seguridad en las instalaciones, monitorización de la red, asignación de perfiles de acuerdo a sus funciones	60%	$ 155.520
BD proveedores	$ 90	Interrupción de otros servicios y suministros esenciales	NO APLICA	0%	$ 145.800
		Degradación de los soportes de almacenamiento de la información	NO APLICA	0%	$ 145.800
		Errores de los usuarios	Instalación de programas sólo por personal capacitado y autorizado.	50%	$ 516.600

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Errores del administrador	NO APLICA	0%	$ 145.800
		Errores de monitorización (log)	NO APLICA	0%	$ 145.800
		Errores de configuración	Configuración correcta de privilegios, perfiles de usuarios.	60%	$ 413.280
		Escapes de información	Aplicación de Políticas de confidencialidad de la información	50%	$ 194.400
		Alteración accidental de la información	Prohibición de medios de almacenamiento externo, deshabilitar puertos USB de los equipos de cómputo, en caso de ser autorizados medios extraíbles, tomar las medidas preventivas de no dejarlos expuestos, guardarlos en sitios seguros	60%	$ 136.080
		Destrucción de información	NO APLICA	0%	$ 194.400
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 155.520
		Manipulación de los registros de actividad (log)	NO APLICA	0%	$ 175.770
		Manipulación de la configuración	Sistemas de monitoreo de integridad	50%	$ 145.800
		Suplantación de la identidad del usuario	NO APLICA	0%	$ 194.400
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 155.520

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Uso no previsto	NO APLICA	0%	$ 145.800
		Acceso no autorizado	NO APLICA	0%	$ 170.100
		Repudio	Aplicación de políticas de seguridad en cuanto a integridad de la información	40%	$ 619.920
		Modificación deliberada de la información	NO APLICA	0%	$ 170.100
		Destrucción de información	NO APLICA	0%	$ 194.400
		Divulgación de información	NO APLICA	0%	$ 170.100
		Robo	Políticas de escritorio limpio, implantación de seguridad en las instalaciones, monitorización de la red, asignación de perfiles de acuerdo a sus funciones	60%	$ 155.520
contabilidad	$ 200	Interrupción de otros servicios y suministros esenciales	Stock de papel para impresión, tóner de impresoras, unidades para realización de backups.	60%	$ 129.600
		Degradación de los soportes de almacenamiento de la información	Mantenimiento preventivo o reemplazo de medios de almacenamiento como discos duros, memorias, cintas.	50%	$ 162.000
		Errores de los usuarios	Instalación de programas sólo por personal capacitado y autorizado.	50%	$1.148.000
		Errores del administrador	Revisión de configuraciones y actualizaciones	50%	$ 162.000
		Errores de monitorización (log)	NO APLICA	0%	$ 324.000

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Errores de configuración	Configuración correcta de privilegios, perfiles de usuarios.	60%	$ 918.400
		Escapes de información	Aplicación de Políticas de confidencialidad de la información	50%	$ 432.000
		Alteración accidental de la información	Prohibición de medios de almacenamiento externo, deshabilitar puertos USB de los equipos de cómputo, en caso de ser autorizados medios extraíbles, tomar las medidas preventivas de no dejarlos expuestos, guardarlos en sitios seguros	60%	$ 302.400
		Destrucción de información	Guardas en sitios seguros unidades externas de almacenamiento donde se grabe información confidencial, procedimiento adecuado de las copias de seguridad, prohibir acceso de personal no autorizado a sitios restringidos.	40%	$ 259.200
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 345.600
		Manipulación de los registros de actividad (log)	NO APLICA	0%	$ 390.600
		Manipulación de la configuración	Sistemas de monitoreo de integridad	50%	$ 324.000
		Suplantación de la identidad del usuario	Monitoreo del tráfico, autenticación de usuarios	60%	$ 172.800
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 345.600
		Uso no previsto	Políticas de uso adecuado de los recursos asignados para actividades laborales	60%	$ 129.600

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Acceso no autorizado	Tomar medias sobre el ingreso a las instalaciones de la empresa, configuración adecuada de firewall, IDS, implementación de políticas de escritorio limpio, uso de contraseñas para acceso al sistema	60%	$ 151.200
		Repudio	Aplicación de políticas de seguridad en cuanto a integridad de la información	40%	$1.377.600
		Modificación deliberada de la información	Aplicar políticas de integridad de la información	60%	$ 151.200
		Destrucción de información	Guardas en sitios seguros unidades externas de almacenamiento donde se grabe información confidencial, procedimiento adecuado de las copias de seguridad, prohibir acceso de personal no autorizado a sitios restringidos.	40%	$ 259.200
		Divulgación de información	aplicar políticas de confidencialidad de la información	40%	$ 226.800
		Robo	Políticas de escritorio limpio, implantación de seguridad en las instalaciones, monitorización de la red, asignación de perfiles de acuerdo a sus funciones	60%	$ 345.600
Mercadeo	$ 100	Interrupción de otros servicios y suministros esenciales	NO APLICA	0%	$ 162.000
		Degradación de los soportes de almacenamiento de la información	NO APLICA	0%	$ 162.000
		Errores de los usuarios	Instalación de programas sólo por personal capacitado y autorizado.	50%	$ 574.000

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Errores del administrador	NO APLICA	0%	$ 162.000
		Errores de monitorización (log)	NO APLICA	0%	$ 162.000
		Errores de configuración	Configuración correcta de privilegios, perfiles de usuarios.	60%	$ 459.200
		Escapes de información	Aplicación de Políticas de confidencialidad de la información	50%	$ 216.000
		Alteración accidental de la información	Prohibición de medios de almacenamiento externo, deshabilitar puertos USB de los equipos de cómputo, en caso de ser autorizados medios extraíbles, tomar las medidas preventivas de no dejarlos expuestos, guardarlos en sitios seguros	60%	$ 151.200
		Destrucción de información	Guardas en sitios seguros unidades externas de almacenamiento donde se grabe información confidencial, procedimiento adecuado de las copias de seguridad, prohibir acceso de personal no autorizado a sitios restringidos.	40%	$ 129.600
		Fugas de información	Prohibición de uso de redes sociales, políticas de escritorio limpio, medios extraíbles almacenados correctamente, destrucción de papel reciclado con información confidencial, seguridad en oficinas, cuarto técnico, requisa de paquetes en la entrada del edificio.	60%	$ 172.800
		Manipulación de los registros de actividad (log)	NO APLICA	0%	$ 195.300
		Manipulación de la configuración	Sistemas de monitoreo de integridad	50%	$ 162.000
		Suplantación de la identidad del usuario	Monitoreo del tráfico, autenticación de usuarios	60%	$ 86.400

Anexo F. (Continuación)

Activo	Valor en Millones de $	Amenaza	Descripción Salvaguarda	Reducción del Riesgo	Nueva cuantificación
		Abuso de privilegios de acceso	Monitorear el acceso al sistema de acuerdo a privilegios establecidos a los usuarios	60%	$ 172.800
		Uso no previsto	NO APLICA	0%	$ 162.000
		Acceso no autorizado	NO APLICA	0%	$ 189.000
		Repudio	Aplicación de políticas de seguridad en cuanto a integridad de la información	40%	$ 688.800
		Modificación deliberada de la información	NO APLICA	0%	$ 189.000
		Destrucción de información	Guardas en sitios seguros unidades externas de almacenamiento donde se grabe información confidencial, procedimiento adecuado de las copias de seguridad, prohibir acceso de personal no autorizado a sitios restringidos.	40%	$ 129.600
		Divulgación de información	NO APLICA	0%	$ 189.000
		Robo	Políticas de escritorio limpio, implantación de seguridad en las instalaciones, monitorización de la red, asignación de perfiles de acuerdo a sus funciones	60%	$ 172.800

Fuente: El autor.