# ANÁLISIS Y PLAN DE TRATAMIENTO DE RIESGOS PARA LOS ACTIVOS DE LA INFORMACIÓN DEL CUERPO DE BOMBEROS VOLUNTARIOS DE TUNJA

SAMANTA LORENA SIERRA MAFLA
ARLEY FELIPE GAMBASICA ESQUIVEL

UNIVERSIDAD SANTO TOMÁS
DIVISIÓN DE CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y CONTABLES
FACULTAD DE CONTADURÍA PÚBLICA
TUNJA
2019

# ANÁLISIS Y PLAN DE TRATAMIENTO DE RIESGOS PARA LOS ACTIVOS DE LA INFORMACIÓN DEL CUERPO DE BOMBEROS VOLUNTARIOS DE TUNJA

SAMANTA LORENA SIERRA MAFLA
ARLEY FELIPE GAMBASICA ESQUIVEL

Trabajo de grado para optar al título de
Contador Público

Directora
Mg. NATALY YOHANA CALLEJAS RODRÍGUEZ

UNIVERSIDAD SANTO TOMÁS
DIVISIÓN DE CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y CONTABLES
FACULTAD DE CONTADURÍA PÚBLICA
TUNJA
2019

**Nota de aceptación**

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Tunja, 18 de noviembre de 2019.

**Dedicatoria**

El presente trabajo investigativo lo dedicamos principalmente a Dios, por llenarnos de sabiduría, entereza, dedicación y darnos fortaleza para continuar en este proceso de obtener uno de los anhelos más deseados, nuestro sueño de obtener nuestro título de pregrado con una investigación.

A nuestras familias, especialmente a nuestros padres, Susana Esquivel, Luis Gambasica, Liliana Mafla, Felipe Sierra por su amor, trabajo y sacrificio en todos estos años, gracias a ustedes hemos logrado llegar hasta aquí y convertirnos en quienes somos. Es un orgullo y un gran privilegio de ser sus hijos, son los mejores padres, abnegados, amorosos y nuestros ejemplos a seguir. Esperamos ser un orgullo para ustedes.

A todas las personas que nos apoyaron y han hecho que este proyecto se realice con éxito en especial a aquellos que nos abrieron las puertas, que confiaron en nosotros y compartieron sus conocimientos, al Teniente Darío Alberto Pedreros Guerra, al Cuerpo de Bomberos Voluntarios de Tunja y a la Señora Marlen Madero por acogernos y permitirnos aportar un pequeño granito de arena desde nuestra investigación a esta valiosa institución que realiza tan loable labor.

Agradecemos a nuestros docentes de la facultad de Contaduría Pública de la Universidad Santo Tomás de Tunja, por haber impartido sus conocimientos a lo largo de la preparación de nuestra profesión, de manera especial, A nuestra tutora investigadora y docente Nataly Yohana Callejas que estuvo incondicionalmente con nosotros, guiándonos, leyendo cada uno de nuestros escritos y ayudándonos a mejorarlos, ella quien nos compartió herramientas importantes para avanzar en cada parte de este proyecto, por su paciencia, exigencia y rectitud como docente, muchas gracias.

**Tabla de Contenidos.**

## Lista de tablas

**Lista de figuras.**

## Lista de ilustraciones.

## 1. Título:

ANÁLISIS Y PLAN DE TRATAMIENTO DE RIESGOS PARA LOS ACTIVOS DE LA INFORMACIÓN DEL CUERPO DE BOMBEROS VOLUNTARIOS DE TUNJA

# 2. Planteamiento del Problema u Oportunidad

## 2.1 Descripción del problema u oportunidad

Generalmente las organizaciones reciben información por medio de diferentes fuentes que pueden llegar a ser internas o externas, la cual debe someterse a una clasificación y disposición en relación a su propósito, de manera que de forma consolidada facilite la toma de decisiones y pueda estar disponible al momento que sea requerida. Como resultado de lo anterior, es recomendable que se tomen medidas en cuanto al uso, manejo y disponibilidad de la información, pues esta es "un valioso activo del que depende el buen funcionamiento de una organización", así como aspectos estratégicos que direccionan gerencialmente la operación de las mismas. (Instituto Nacional de Tecnologías de la Comunicación, 2010)

Ante la necesidad de proteger estos datos, se han desarrollado diferentes sistemas que procuran la gestión adecuada de la información y orientan el tratamiento que debe darse para que salvaguardar estos activos intangibles de gran valor. Como lo menciona Novoa (2015), los sistemas de gestión para la seguridad de la información, SGSI, son unas herramientas corporativas que permiten solucionar problemas de seguridad en especial cuando se habla de seguridad informática, por medio del uso de mecanismos como el análisis de riesgos, la mejora y mantenimiento en la protección de la información, con el objetivo de garantizar la prosperidad del negocio en el futuro, apoyados de normas como las ISO 27001, que establecen criterios y procedimientos para cumplir el propósito de resguardar estos activos.

Colombia en el año 2016, fue referente a nivel Latinoamérica, al registrar un 60% de empresas con cumplimiento de requisitos y certificaciones en calidad de sus procesos de seguridad de la información, sin embargo, en la actualidad ese porcentaje representa grandes empresas establecidas en el territorio nacional, dejando rezagadas a las pymes, las cuales no han logrado incorporar medidas que les permitan proteger sus datos y con ello, realizar una gestión eficiente de los activos de la información. (Revista Portafolio, 2016)

## 2.2 Formulación del problema u oportunidad

A pesar de que en Colombia se tiene un marco normativo desarrollado, que evidencia la importancia del tratamiento y seguridad de los datos generados en las operaciones comerciales que se dan día a día, muchas pymes no cuentan con el conocimiento de las diferentes acciones que pueden llevar a cabo para gestionar de manera adecuada los activos de la información; como políticas al interior de la organización, contratos de confidencialidad al momento de realizar acuerdos con otras entidades, o en el momento que se contrata un empleado, tratamiento de las bases de datos de proveedores, análisis de precios, retroalimentación de clientes, entre otros; que de revelarse, podría generar pérdidas de recursos y oportunidades de negocio.

Por otra parte, la vulnerabilidad de la información puede acarrear sanciones de parte de organismos de control, encargados de supervisar el tratamiento de datos en entidades que, por sus actividades operacionales, son receptoras de información de carácter confidencial, como es el caso del Cuerpo de Bomberos Voluntarios de Tunja, una entidad encargada de proteger la vida y los bienes de los boyacenses; así como realizar una gestión integral y prevención del riesgo contra incendios y eventualidades conexas mediante el uso recursos públicos, que genera a partir de sus procesos, un volumen significativo de datos y no cuenta con los controles adecuados para garantizar la protección de la información.

Lo anterior, sumado a la implementación de nuevas tecnologías para la administración de los procesos y gestión de las áreas que componen la estructura organizacional de la entidad, revelan un panorama de riesgos tanto internos como externos para el tratamiento de la información generada, pues existe desconocimiento en el manejo adecuado de los datos por parte del personal contratado, no se tienen copias de seguridad de la información contable de la empresa, ni direccionamiento de cómo y dónde debe reposar dicha información, no se tienen copias digitalizadas de documentos laborales, comerciales, y recientemente, la entidad sufrió una ataque por parte de un ex empleado que salto las barreras de seguridad e ingreso al sistema de información, ocasionando pérdidas operativas y económicas graves.

## 3. Justificación

La necesidad de transparencia en los procesos internos y los inconvenientes en el manejo de la información de las organizaciones, ha provocado un aumento en la sensibilización de las mismas, por generar un mayor control sobre sus operaciones, buscando mecanismos que permitan tratar los datos de forma eficiente, convirtiendo al control interno, en una herramienta eficaz para identificar, prevenir, mitigar o corregir errores que puedan afectar de manera directa o indirecta los activos de la empresa relacionados con la gestión de los sistemas de información.

Fenómenos como la globalización e incorporación de conceptos en las organizaciones como el de gestión de la calidad total, hacen que los procesos de control interno cobren mayor relevancia con la exigencia normativa de medidas que garanticen la calidad y contribuyan al fortalecimiento de la imagen corporativa, a partir de la implementación de prácticas que otorgan mayor credibilidad y diferenciación frente a la competencia. (Pascual, 2014) Así mismo, se evidencia la necesidad de establecer pasos para la formulación e implementación de medidas que permitan proteger un activo de gran relevancia como lo es la información, y del cual dependen todas las áreas organizacionales como lo son las estratégicas, las financieras, las comerciales y de producción, en el marco de sistemas de información cada vez más complejos, abiertos e integrados.

Por lo anterior, esta investigación pretende realizar un análisis diferencial y el plan de tratamiento de riesgos para los activos de la información del Cuerpo de Bomberos Voluntarios de Tunja, en el marco de los principios de control interno generalmente aceptados, considerando criterios para el análisis de la gestión del riesgo contemplados en la norma ISO 27001 de Tecnología de la Información, técnicas de seguridad y sistemas de gestión de la seguridad de la información y la metodología MAGERIT, de manera que se ofrezca a la entidad herramientas para la identificación y tratamiento de riesgos inherentes a la información, garantizando un ambiente seguro para los usuarios internos y externos.

# 4. Objetivos

## 4.1. Objetivo General

Realizar un análisis y el plan de tratamiento de riesgos de los activos de la información para el Cuerpo de Bomberos Voluntarios de Tunja, considerando la norma ISO 27001: Tecnología de la Información, técnicas de seguridad y sistemas de gestión de la seguridad de la información.

## 4.2. Objetivos Específicos

**1.** Establecer la metodología y criterios para el análisis de la gestión del riesgo en el Cuerpo de Bomberos Voluntarios de Tunja.

**2.** Contextualizar y generar un análisis diferencial de la situación actual de Cuerpo de Bomberos Voluntarios de Tunja, de acuerdo a la metodología identificada.

**3.** Desarrollar un plan de tratamiento de riesgos y amenazas asociados al Sistema de Gestión de Seguridad de la Información del Cuerpo de Bomberos Voluntarios de Tunja.

# 5. Metodología

## 5.1. Método de Investigación

La presente investigación es aplicada, que según autores como Humberto Ñaupas, Elías Mejía, Eliana Novoa Y Alberto Villagómez, se caracteriza porque busca solucionar inconvenientes que ocurren en cualquier actividad económica, en especial al hablar de temas inherente a sus procesos de producción, circulación de bienes y servicios, problemas administrativos y en general todas las dificultades asociadas a la ineficiencia al interior de una organización. (Ñaupas, Mejía, Novoa, & Villagómez, 2014) y que, para el caso de esta investigación, se evidencia en el uso de teorías y metodologías para el análisis y tratamiento de riesgos relacionados con la gestión de la información.

Por otra parte, el nivel de la investigación es descriptivo, que teniendo en cuenta la opinión de Iván Cruzatti, se diferencia de los demás niveles de investigación, en que esta se ocupa de examinar la situación en tiempo presente y se complementa con aspectos matemáticos; considerando la identificación de rasgos y características del problema a resolver. (Cruzatti, 2008), y se evidencia en esta investigación a partir de la descripción detallada de todos los hechos que se presentan a diario en relación al tratamiento de los datos y manejo de la información del Cuerpo De Bomberos Voluntarios De Tunja.

## 5.2. Fuentes técnicas de recolección de la información

### 5.2.1. Fuentes Primarias:

Dentro de las fuentes primarias se tiene el testimonio del Comandante del Cuerpo De Bomberos Voluntarios De Tunja, la Jefa de Contabilidad, el Ingeniero de sistemas del Cuerpo De Bomberos Voluntarios De Tunja y el profesional de soporte externo en el área de sistemas; testimonios que se levantaron a partir de instrumentos como entrevista semiestructurada realizada directamente por los investigadores.

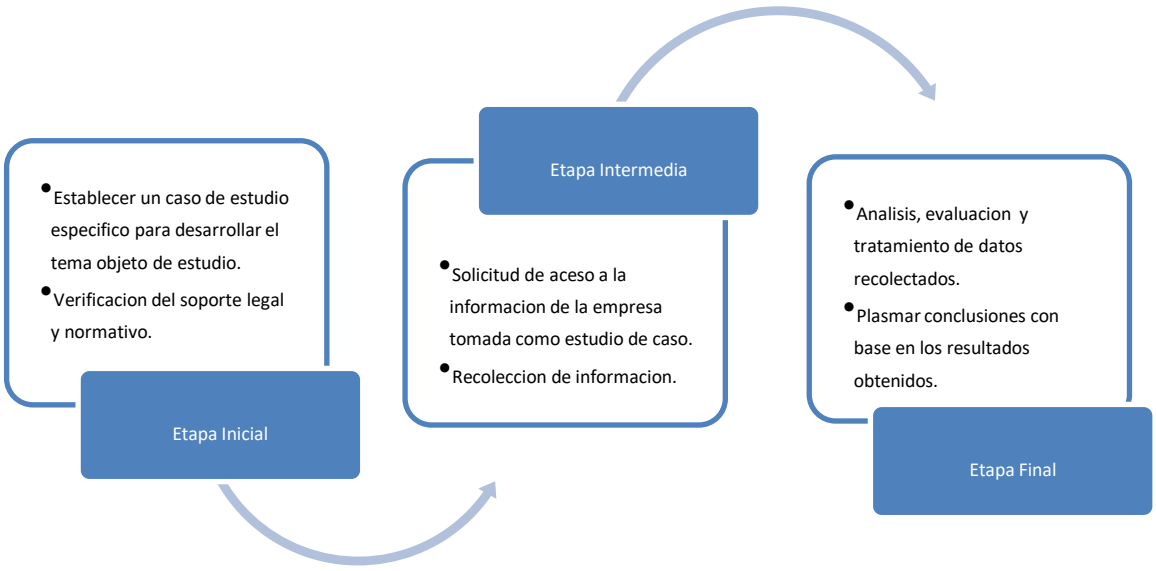
Se elaboraron fichas diagnósticas y de reporte de hallazgos, con información suministrada por las áreas de comunicaciones, comando, departamento contable y financiero, y el área de soporte técnico del Cuerpo de Bomberos Voluntarios de Tunja.

### 5.2.2. Fuentes Secundarias:

A partir de técnicas como el análisis documental se revisaron fuentes secundarias como la Normativa ISO vigente, artículos de revistas científicas en áreas económicas, administrativas y de auditoria, blogs especializados en seguridad de la información, libros académicos y científicos, tesis y artículos de investigación de repositorios de Universidades nacionales e internacionales.

## 5.3. Procedimiento Metodológico.

*Figura 1: Procedimiento Metodológico.*




Fuente: Elaboración propia.

# 6. Marco Referencial.

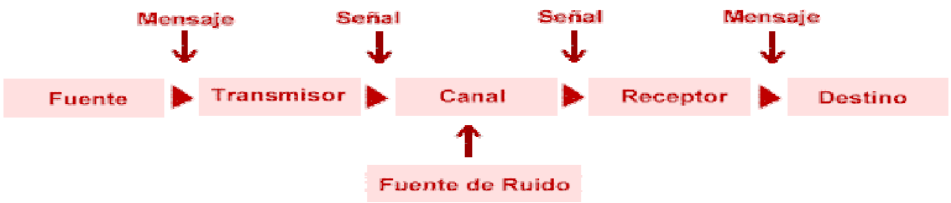
## 6.1. Marco Teórico.

### 6.1.1 Capítulo 1: Tecnologías de la Información y las comunicaciones.

#### 6.1.1.1 Teoría de la Información o Teoría Matemática de la comunicación

Cuando se habla acerca del estudio de las tecnologías de la información y la comunicación, inicialmente se debe considerar la propuesta realizada por Claude E. Shannon a finales de la década del 40 y que se caracterizó por tratar los elementos básicos que permiten la transmisión de mensajes. En la obra "The Mathematical Theory of Communication" se expone de forma sencilla un sistema de comunicación de la siguiente manera: la fuente de la información elige un determinado mensaje entre varios y el transmisor convierte dicho mensaje que fue elegido en una señal que será transferida a través del medio de comunicación al receptor. De esta manera, el receptor pasa a hacer las veces de transmisor, pero de forma opuesta transfigurando la señal en un mensaje que pasará más adelante al destinatario. En la figura que a continuación se presenta, en términos más simples, se expone que, en el momento que una persona habla con otra, el cerebro es la fuente de información, la otra persona el destinatario, el sistema vocal es el transmisor y su oído con su octavo par de nervios craneanos, es el receptor. (Lopez, 1998)

*Ilustración 1: Teoría de la Información o Teoría Matemática de la comunicación.*




Fuente: Peralta (2016)

Como resultado de lo anterior, los términos empleados por Shannon y Weaver en poco tiempo pasaron a formar parte de la cotidianidad y hoy en día no se puede negar la importancia de esta teoría en el ámbito de la comunicación y la información en el hemisferio occidental. De acuerdo a Marshall McLuhan, la gran influencia que este modelo ha tenido para los medios de información y comunicación es fundamental para la base de todas las teorías occidentales contemporáneas, principalmente por lo que él considera como

un modelo de plomería de un artefacto de hardware para un contenido de software. Como se ha podido demostrar, esta teoría se encuentra vinculada con preceptos que rigen la transmisión y el procesamiento de datos, desempeñando un rol fundamental en lo que tiene que ver con la información, además de abarcar temas como la competencia de los sistemas de comunicación para lograr transmitir y en el proceso de recopilar la información.

#### 6.1.1.2 La Comunicación.

El término "comunicación" generalmente cumple con tres características las cuales son en primer lugar polisemia, haciendo referencia a que es una palabra que se utiliza en un sinfín de contextos, luego, se encuentra la ambigüedad debido a la confusión del matiz de su significado y por último la multidimensionalidad, teniendo en cuenta la gran variedad de situaciones que puede ser empleada. Esta teoría, por tanto, presenta dos enfoques según (Aguado, 2004):

- El primer enfoque toma la comunicación únicamente en el campo social, cultural y tecnológico, limitando el concepto al intercambio de información.
- El segundo enfoque considera el concepto de "comunicación" en los diferentes ámbitos que se puede utilizar y establecer, de forma que convierte el concepto en algo más universal, teniendo en cuenta el uso delimitado que se le puede dar.

Debido a la orientación más generalizada del segundo enfoque y también por la realidad que representa en la cotidianidad de cualquier ser humano, será el que se tendrá en cuenta para analizar los principios que lo conforman. Por consiguiente, los principios que convergen para darle un sentido tan "general" al concepto de la comunicación son los siguientes:

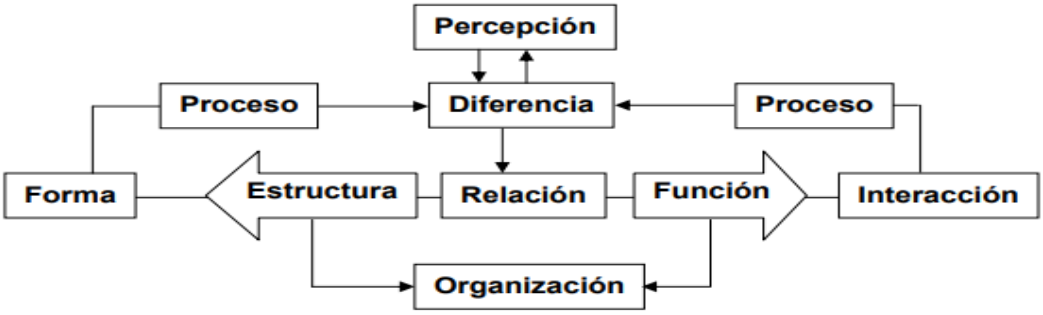
- Principio de relación: este principio es considerado como uno de los más representativos de la comunicación, en vista a que independientemente del contexto, la comunicación siempre buscará el encuentro entre dos o más elementos.
- Principio de diferencia/ semejanza: así como la relación desempeña un rol esencial para la comunicación, el principio de diferencia/ semejanza destaca la comunicación como la capacidad fisiológica de percepción a la diferencia por

parte de quien observa, colocando así a la comunicación como el tráfico y producción de diferencias.

- Principio de estructura forma: uno de los papeles más relevantes que tiene la comunicación cuando es empleada, consiste en dar forma, destacar o enfatizar sobre cierta base. Lo anterior se ve reflejado por la forma que normalmente se aprecia el entorno en el cual estamos, ya que no se concibe como un conjunto de elementos independientes, sino como un conjunto de elementos que interactúan entre sí.
- Interacción/ función: este principio se refiere al cambio que regularmente se da en la estructura, lo cual se entiende como un cambio presumible para todos los elementos que conforman la estructura. (Aguado, 2004)

A través del siguiente esquema, se refleja el funcionamiento de los principios anteriormente mencionados.

*Ilustración 2: Teoría de la Comunicación.*




Fuente: Aguado (2004)

Adicionalmente de los principios, es necesario hablar del papel que desempeña la organización y el proceso, ya que el primero se encarga de vincular la estructura y la función, en contraste con el proceso, que tiene la tarea de fortalecer la idea de diferencia que conforma la observación. (Aguado, 2004)

La comunicación es un análisis con un propósito amplio y universal que, obliga a considerar una gran variedad de aspectos que provienen de la relación de estos principios y así mismo de forma individual logran ser agregados por medio de interrelaciones de

cambio que organizacionalmente cobra valor si se relaciona con la gestión de cualquier activo que comunica o informa algún dato relevante para la toma de decisiones. (Aguado, 2004)

**6.1.1.3 Teoría de los sistemas.**

La Teoría General De Sistemas fue desarrollada por el biólogo Ludwig von Bertalanffy, para atender circunstancias propias de la biología, tanto así que, desde la década de 1930 él percibió que la investigación que se estaba desarrollando en aquel campo tenía muchos vacíos, especialmente a raíz de lo imperante que fue por entonces el método científico cartesiano, el cual no lograba explicar fenómenos esenciales de la vida. Sin embargo, como consecuencia del impacto que tuvo esta teoría por aquella época, su aplicación trascendió a otros campos de estudio. Es importante resaltar que, esta teoría ocasionó un cambio de paradigma por la visión holística que propuso, marcando una notable distinción con las teorías anteriores que eran consideradas mecanicistas. (Peralta, 2016)

La Teoría General De Sistemas se utilizó en diferentes disciplinas, destacando su contribución en el mundo de las organizaciones, donde logro instaurar elementos específicos para interpretar sucesos que ocurren día a día en las empresas, conduciendo a una nueva forma de entender las organizaciones, ya que anteriormente eran asimiladas como un conjunto de elementos que interactúan entre sí, en el contexto que actúan, y en la actualidad, es la forma en que se entiende el conjunto de elementos que sistemáticamente solucionan los problemas, sobresaliendo respuestas creativas y agradables. (Peralta, 2016)

Tomando a consideración la nueva visión de la Teoría General De Sistemas en el ambiente administrativo, años después surgieron nuevos modelos con características similares, entre las que se destacan las siguientes:

- Herbert Simón, Toma De Decisiones: Herbert Simón planteo teorías del proceso de toma de decisiones basándose del marco de la Teoría General De Sistemas acerca del comportamiento de las personas y las empresas, dando resultados como la racionalidad limitada, la cual trata que los individuos toman decisiones que deriven efectos no tan óptimos. De igual manera, Herbert Simón también se caracterizó por

cuestionar la teoría de la burocracia de Weber, debido a que encontró inconvenientes de esta teoría al tratar de exponer comportamientos al interior de la empresa.

- Modelo de Tavistock de organización sociotécnica: este modelo surgió a causa de las dudas que generaba la aplicación del modelo Tayloriano en empresas dedicadas a la minería en Inglaterra, puesto que aquellas organizaciones mineras que ponían en práctica métodos mecanicistas, no tenían la productividad esperada. Debido al problema presentado, miembros del instituto de Tavistock produjeron sistema asentado en los principios de la Teoría General De Sistemas.

La Organización cómo Sistema Abierto: en el modelo de Kahn y Katz se considera a la organización como un sistema abierto, teniendo en cuenta especialmente sus características, entendiéndose como la energía que es recibida del entorno y que posteriormente será enviada de nuevo al entorno para que al final se realimente con el propósito de preservar el sistema. (Peralta, 2016)

Como se demostró, fue tal el cambio de paradigma de esta teoría en el ambiente organizacional que, teorías administrativas que datan desde la administración científica de Taylor hasta la más reciente por aquel entonces como la teoría de la burocracia de Weber, se juzgaron por lo inflexibles que parecían frente a la innovadora Teoría General De Sistemas. Es así que, la reciente teoría representó una oportunidad para investigar detalles que antes no eran posibles por el método científico, contribuyendo de este modo a vislumbrar nuevos conceptos. (Peralta, 2016)

#### 6.1.1.4 Tecnología de la información

Las tecnologías de la información o también conocida por su abreviatura como TIC, son un término que actualmente abarca varios elementos tecnológicos que van más allá de un ordenador y tiene en cuenta un espectro de tecnologías que están relacionadas con el uso, manejo y recopilación de datos. De acuerdo a la Organización Para La Cooperación y el Desarrollo Económico (OCDE), las TIC son definidas como sistemas tecnológicos en los cuales, se recibe, administra y procesa la información, favoreciendo a los procesos

comunicativos entre dos o más partes. (Organización Para La Cooperación Y El Desarrollo Económico, 2010)

Así mismo, hay que considerar que las TIC comprenden un escenario que está caracterizado por promover el vínculo entre dos o más individuos, gracias a la implementación de diferentes redes las cuales tienen el firme propósito de permitir una comunicación interactiva mediante el empleo de distintas tecnologías incluyendo las tradicionales (teléfonos, televisores, radio, entre otros). De igual modo, uno de los aspectos más característicos que tienen las tecnologías de la información es el acelerado ritmo de cambio y difusión que están provocando en la forma de vida de cada ser humano, por medio del progreso en la capacidad de almacenamiento, procesamiento y difusión de información, generando una mejora en la calidad de vida y reduciendo la desigualdad en el acceso de bienes y servicios. (Avella & Parra, 2013)

#### 6.1.1.5 Computador tecnología de la información

*Tabla 1: Generalidades del Computador.*

| Elemento | Concepto. |
|---|---|
| Historia | El origen del computador se remonta al año 3000 A.C. con el invento del Ábaco, en vista a que fue el primer instrumento en operar por medio de datos. Muchos años después se llegó a crear el invento que actualmente usamos, gracias a las importantes contribuciones que se dieron en el siglo XX entre los que se destacan nombres como John V. Atanasoff y de Konrad Fuse y el cuerpo de investigación de IBM encabezado por Howard Aiken por los desarrollos en el campo de la electricidad. Más adelante se produjo uno de los avances más significativos con la aparición del primer ordenador eléctrico denominado ENIAC.<br>Como se mencionó en el párrafo anterior, el siglo XX fue un periodo muy enriquecedor para el desarrollo del computador, en especial por la competencia de grandes compañías como Intel, Hewlett Packard, Apple, IBM, NCR, entre otras, las cuales tenían una disputa feroz por cautivar la atención del cliente. (Mora, y otros, 2013) |
| Funciones | Se puede afirmar que el computador es una máquina encargada de procesar información, gracias a componentes del hardware y el software. |

| | |
|---|---|
| | Al hablar de forma general, uno de los aspectos que más sobresalen al utilizar un computador a diario es en el instante de ejecutar un programa, debido a que es un proceso que inicia cuando la CPU registra la orden, transmite las órdenes de manera secuencial para garantizar que las instrucciones lleven la secuencia adecuada. Adicionalmente la unidad de control (también se encuentra en la CPU) coordina y temporiza las funciones, recopilando la instrucción desde la memoria y posteriormente la instrucción viaja por el bus desde la memoria hasta la CPU. Mientras esto ocurre el contador de programa aumenta de uno en uno para preparar la siguiente orden. Como última acción la instrucción actual es analizada gracias a un decodificador, el cual establece lo que realizará la instrucción.<br>Además, es necesario resaltar que, aunque el computador es considerado al día de hoy como un elemento indispensable en la vida de las personas, muy pocas conocen acerca del funcionamiento interno, el cual depende de programas que requieren un idioma propio como el lenguaje de máquina, programación tipo C, el lenguaje de Pascal, entre otros. (Montilla, Atencio, & Ruíz, 2009) |
| Componentes | Los componentes del computador son herramientas que son imprescindibles para recibir y procesar diferentes tipos de datos y transformarlos en información catalogada como provechosa para los usuarios.<br>Entre los dispositivos se puede contemplar aquellos que son de entrada, salida o mixto. (Ochoa, Armenta, Pizá, & Gonzalez, 2009) |
| Dispositivos de entrada | Se definen como los dispositivos por medio de los cuales se introduce información en el ordenador. Entre los más generales tenemos los mencionados a continuación. Entre los más destacados están los siguientes: ratón, teclado, scanner, entre otros. (Vazquez, 2012) |
| Dispositivos de salida | Los dispositivos de salida son aquellos por medio de los cuales se puede obtener, visualizar o extraer la información procesada en el computador, dentro de los más comunes están los mencionados a continuación: monitor, impresora, altavoz, entre otros. (Rosero, 2006) |
| Dispositivos de entrada y salida | Los periféricos de entrada/salida permiten la comunicación con el procesador y demás componentes del computador, con las unidades para el almacenamiento auxiliar o externo como los discos o memorias permitan que ingresemos o extraigamos información del computador, de esta forma trasladar información de un ordenador a otro, transportarla, editarla, almacenarla y guardarla (Santillán, 2016) Dentro de los más comunes, están los mencionados a |

| | |
|---|---|
| | continuación: pantalla táctil, impresora multifuncional, módem, switch, router, entre otros. (Espinosa, Ruiz, & Cantero, Introducción a la informática (4a. ed.), 2006) |
| Software | Se puede definir como el conjunto de componentes internos en un sistema informático que permiten el funcionamiento del computador, el cual depende de un grupo de elementos lógicos que ayudan a que el computador efectué diferentes tareas establecidas. (Santillán, 2016) |

Fuente: Elaboración propia a partir de las fuentes consultadas y citadas en cada aparte.

#### 6.1.1.6 Redes de Computadores.

Las redes de computadores, es una agrupación de instrumentos electrónicos conectados a un aparato físico por intermedio de una serie de conexiones como cables, fibras o incluso medios inalámbricos. Es preciso señalar, que una red para que sea considerada efectiva y confiable, es necesario que cumpla con tres características las cuales son: el rendimiento (haciendo énfasis en el tiempo de respuesta). Después se encuentra la fiabilidad que tiene la red, examinando el fallo que puede tener y la capacidad de continuar transmitiendo la información ante alguna adversidad. Por último, está uno de los aspectos más relevantes, ya que trata la seguridad de los datos que la red puede ofrecer, para mantener a salvo la información de los usuarios. (García, Gomez, Molina, & Rubio, 2017)

##### 6.1.1.6.1 Contexto.

Con la aparición de los primeros ordenadores, se presentó la necesidad de interconectar un ordenador a otro para obtener una comunicación muy parecida a la que tienen los seres humanos comúnmente al entablar una conversación. Aunque con el surgimiento de los primeros ordenadores no se generó una comunicación tan eficiente como al día de hoy debido a que muy pocos tenían acceso (universidades, grandes empresas, organismos estatales, etc.), con el transcurrir de los años se inventaron mecanismos para permitir la transferencia de información como sucedió con el modem. Al inicio, la idea de crear el modem surgió como consecuencia de separar un terminal de la unidad central al momento de conectarse y de esta forma buscar otras opciones con lo cual, la mejor solución fue realizarlo por medio de una red telefónica ya que evitaba tener que instalar una infraestructura como la de aquella época y con el uso de la red telefónica se

podía llevar acabo con un aparato que ajustara los bits a una determinada red. (Barceló, Iñigo, Martí, Peig, & Perramon, 2004)

Posteriormente se presentaron mayores avances por medio de la red por paquetes, la cual tenía como principal punto a favor que los recursos exclusivamente se empleaban cuando realmente se estaba empleando. Más adelante, para solucionar distintos inconvenientes que ocurrían al intentar intercambiar información entre los computadores (ya que implicaba el uso de varios elementos), se estimuló el uso de modelos estructurados como la arquitectura de protocolos, contribuyendo a tener un sistema más organizado debido a que se trabaja por niveles y permitía al usuario tener una conectividad más cooperativa. Además de los avances anteriormente mencionados, otro hecho a tener en cuenta fue el cambio de la red telefónica que pasó de ser analógica a digital, permitiendo realizar muchas mejoras como optimizar la calidad en la recepción de las señales y convertir la transmisión de la red en una más veloz. Durante este proceso, las empresas de telefonía sustituyeron los enlaces internos por señales digitales, llevando a los hogares un gran número de beneficios por medio de una comunicación que integraba muchos servicios y era meramente digital (Barceló, Iñigo, Martí, Peig, & Perramon, 2004)

Por último, no se puede dejar de mencionar el acontecimiento que ha generado la telefonía móvil en la vida diaria de las personas, sobre todo en el campo de las comunicaciones, llegando a romper barreras cuando se trata de enviar información de un lugar a otro. Desde la perspectiva de las comunicaciones, los celulares deben ser observados como una evolución de la red telefónica clásica, en la medida que el sistema GSM realiza ciertos cambios como que, en vez de utilizar un cable la forma de enlace se ejecuta con una antena y el respectivo móvil. (Barceló, Iñigo, Martí, Peig, & Perramon, 2004)

#### 6.1.1.6.2 Tipos de redes.

Teniendo a consideración la evolución de las redes de computadores a lo largo de la historia, se ha hecho necesario clasificar las redes de acuerdo a su alcance, método de conexión y topología, como consecuencia de los avances que ha tenido la informática para progresar en volver la comunicación más accesible y romper los límites de la distancia.

Al clasificar las redes de acuerdo a su alcance, es imperioso nombrar las redes más conocidas las cuales son: red de área local (LAN), red de área metropolitana (MAN) y red de área amplia (WAN). La red de área local (LAN), es un tipo de red privada que es utilizada por los hogares, en el trabajo y en los colegios o universidades. Algo que caracteriza a este tipo de redes, es que su extensión está limitada, lo que genera que el tiempo de trasferencia no sea tan bueno. De igual manera, la red de área metropolitana es un tipo de red similar a la red de área local, con la gran diferencia que tiene un tamaño muy superior y ésta puede ser público o privada. Así mismo, en el tipo de redes por alcance se encuentra la red de área amplia, que suele ser una red que envía datos de un host a otro y está compuesta por subredes las cuales son: líneas de comunicación (permite transferir bits de un ordenador a otro) y una serie de computadores que están conectadas a una línea de transmisión. De igual manera, se encuentra el tipo de redes clasificado por su método de conexión y se divide exclusivamente en redes guiadas y no guiadas. Las redes guiadas, son aquellas que se encuentran conectadas por redes físicas como es el caso del cable coaxial, fibras ópticas, entre otros. En segunda instancia están las redes no guiadas, que se caracteriza porque no están conectadas a través de un medio físico como es el caso del láser, radiofrecuencias, entre otros. (Cedano, Cedano, Rubio, & Vega, 2014)

**6.1.1.6.3 Topologías de red.**

Otra topología muy destacada es la topología tipo estrella, la cual, se distingue porque tiene un punto central que permite conectar los ordenadores de una manera idéntica a los radios de una rueda. Como efecto de esta característica, radica el principal problema que podría tener la topología tipo estrella, ya que si llega a suceder algún fallo en el nodo base (ubicado en la parte central), estropearía todo el funcionamiento de la red. Producto de la importancia que tiene el nodo central, en la mayoría de los casos se toman medidas al respecto para disminuir la probabilidad de riesgo. Otro aspecto a resaltar en este tipo de topología, es el modularidad, dado que facilita aislar una estación cuando presente algún inconveniente de manera rápida y simple. (Abantos, 2014)

De igual manera, existe la topología tipo círculo o anillo que suele ser reconocida fácilmente, en vista que los ordenadores están conectados en una onda cerrada. Por medio de este tipo de conexión, la información es transmitida en un sentido por medio del anillo,

gracias a un paquete de datos (testigo), facilitando la transferencia entre los diferentes nodos, hasta llegar al camino destinado. La principal desventaja que presenta la topología tipo círculo, es el cableado de red en el anillo, ya que es de las más complejas teniendo a consideración el costo por cable y la obligación que se tiene al introducir dispositivos llamados unidades de acceso multiestación. (Abantos, 2014)

Por último, está la topología tipo árbol la cual reúne aspectos de la topología bus con la estrella, agrupando subredes tipo estrella a un bus, permitiendo obtener una red más extensa. Por lo general este tipo de red se emplea en la televisión por cable y en redes locales analógicas de banda ancha. (Vásquez, 2010)

#### 6.1.1.6.4 Servidores.

El servidor, es un computador que permite compartir recursos entre varias estaciones ya sea en el área de trabajo o donde sean necesarios una serie de servidores que estén enlazados mediante una red informática. Cuando se habla de recursos que pueden ser compartidos, se puede llevar a cabo esta acción por medio del hardware con medios como el disco duro, impresora, entre otros. De la misma manera, el software también dispone de servicios como el correo electrónico o en general el internet, para ejecutar este proceso. (Patterson & Hennessy, 2011)

Al tratar el tema de los servidores, existe una gran variedad de servidores que contribuyen a los usuarios a desempeñar diferentes funciones entre los que se destacan los siguientes tipos de servidores:

- Servidor web.
- Servidor de archivos.
- Servidor de e –mail.
- Servidor de base de datos.
- Servidor de videojuegos.

### 6.1.1.7 Información.

El término información, es un término que abarca un número significativo de definiciones, como es el caso de la investigación realizada por Angulo Marcial (Marcial,

2018), encontrando más de mil definiciones acerca de este concepto y demuestra el sin fin de ideas que tiene el ser humano de un asunto tan relevante como es la información. Por lo tanto, el concepto que se tendrá a consideración, agrupa los conceptos que brinda la real academia española en relación a este tema:

> La información es considerada como aquel mensaje o anuncio generado por un individuo, el cual puede contribuir para esclarecer una situación o contribuir para elegir la decisión más razonable, en base al contenido o los detalles que suministra la misma. (Marcial, 2018)

#### 6.1.1.7.1 Contexto.

El escenario en el que la información se desarrolla desde inicios del siglo XXI, es cada vez más fundamental ya que ha logrado trascender la vida de las personas, llegando a afirmar que los seres humanos viven en "la sociedad de la información".

La sociedad de la información se refiere a la importancia de los sistemas y redes de la comunicación en aspectos esenciales de la sociedad como la economía, la política, las costumbres y demás piezas catalogadas como componentes esenciales en el ámbito social. Al tener en cuenta las distintas opiniones que desencadena este concepto, se puede afirmar que existe un escenario muy variable en cuanto al juicio que esta temática provoca. Hay quienes piensan que al vivir en una sociedad donde la información ha tomado un papel tan preponderante, es oportuno mencionar las consecuencias que este tipo de sociedad ha inducido, tal es el caso del nivel de dependencia que al día de hoy la tecnología ha asumido al mencionar cambios elementales que contribuyeron a permitir la transformación del mundo globalizado que muchas personas ven con buenos ojos, a pesar que la información continua muy limitada en consideración al acceso que habitualmente la mayoría de las personas no gozan, mientras que los principales medios de comunicación son manejados por organismos privados preocupados por intereses económicos y cuando son públicos sirven de propaganda política para el gobierno de turno. (Islas & Gutierrez, 2004)

#### 6.1.1.7.2 Información en la empresa

Dado el volumen de información fundamental para el análisis que manejan las empresas actualmente, se convierte en algo esencial el hecho de reconocer la información como uno de los activos más relevantes para mantener a una empresa competitiva en un mercado determinado.

Los sistemas de información han impactado de forma notable el mundo empresarial de los últimos años, como consecuencia de las prestaciones que actualmente ofrece la tecnología en un escenario que muy poco pensado en el siglo anterior. Aunque los sistemas de información han provocado decepciones para algunas empresas (en virtud del desconocimiento acerca de la importancia que debe tener la información), lo más recomendable es iniciar con un diagnóstico del sin fin de privilegios que esta herramienta contribuye al interior de las empresas, tomando la información como eje primordial para la correcta toma de decisiones. Así mismo, a medida que han pasado los años la competencia entre las organizaciones se vuelve más compleja, teniendo en cuenta las innovaciones que diariamente surgen para cautivar la atención de los clientes y la facilidad con la cual puede comunicarse un individuo desde cualquier parte del mundo con un proveedor que ofrezca un bien a menor precio y de mejor calidad. Según Luis Díaz y Miguel Navarro, la mejor opción que disponen las empresas para competir en el mercado es por medo de un sistema de información que sirva como una acción estratégica, haciendo énfasis en optimizar la calidad de los procesos, con la finalidad de conocer mejor las necesidades que tienen los clientes y ofrecer un bien o servicio final. (Díaz & Navarro, 2014)

**6.1.1.7.3 Seguridad de la información en la empresa.**

El notable desarrollo tecnológico de los últimos años, ha permitido la facilidad para que el ser humano logre comunicarse con otros individuos en cuestión de segundos, dando como resultado que exista un aumento en el intercambio de información, teniendo como principal protagonista de este acontecimiento el internet. Infortunadamente, de la misma manera que progresa el internet, los delincuentes han creado mecanismos con el objetivo de acceder a los datos privados ya sea de personas o empresas, con miras de cometer actos delictivos que podrían poner en riesgo principalmente la privacidad y la integridad de la información privada. Para ser más específico, en el caso de las empresas el panorama puede

convertirse en una situación de alerta constante, debido al volumen de documentos, datos personales e informes obtenidos de forma externa o interna que más adelante son utilizados para varios fines (en especial cuando se trata de tomar decisiones); teniendo que asumir constantemente los miembros de una organización, controles que ayuden a contrarrestar y salvaguardar riesgos inherentes a la información.

Tal como afirmaba el premio Nobel de economía Herbert Simón, la información es un aspecto esencial en la organización cuando se trata de tomar decisiones, ya que es considerado un medio imprescindible para tener un conocimiento más amplio de la situación y así poder elegir la opción más adecuada. Debe ser tal el grado de importancia que tiene la información al interior de un ente económico, que debería ser obligatorio implementar medidas para que se regule el manejo de los archivos e informes adquiridos durante el ciclo normal del negocio, dado que como se mencionó anteriormente, de la información depende que algún miembro de la organización logre elegir la mejor decisión para la entidad, teniendo en cuenta que éste debe tener un pensamiento alineado con los objetivos de la organización. (Gallego, 2007)

De igual manera en el escenario colombiano por medio del Instituto Colombiano De Normas Técnicas Y Certificación, ha venido trabajando desde hace varios años por recomendar a las empresas del país, buenas prácticas inherentes a temas de seguridad de la información, como consecuencia de la importancia que en la actualidad se le da a este asunto y por consiguiente, las medidas que debe asumir una empresa (independientemente de tipo, tamaño o razón social) con respecto a la protección de la información que utiliza en el ciclo normal del negocio, tal como se menciona en el siguiente párrafo:

La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debería estar apropiadamente protegida (Instituto Colombiano de Normas Técnicas y Certificación, 2013).

### 6.1.2 Capítulo 2: Seguridad de la Información.

#### 6.1.2.1 Definición.

Como se mencionaba anteriormente, la información tiene un rol esencial para la vida de las personas a causa de los avances tecnológicos que han llevado a la humanidad a tener un mejor nivel en la calidad de vida. No obstante, es necesario recalcar el alcance que tiene la información, logrando abarcar un escenario que va más allá de un ordenador o de otro aparato tecnológico. Aun así, dada la importancia que tiene la información, es obligatorio implementar medidas que ayuden a minimizar los riesgos situados en el ambiente por el cual se moviliza la información, sin dejar de lado cada elemento del sistema por más mínimo que parezca.

De esta manera, al consultar la definición de seguridad de la información según lo establece la Norma ISO 27001 versión 2005, se fija lo siguiente:

La preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad. (Instituto Colombiano de Normas Técnicas y Certificación, 2005)

#### 6.1.2.2 Objetivos de la Seguridad de la Información.

De acuerdo al contenido de la norma, se busca cumplir con una serie de procedimientos (establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar), mediante la creación de un documento enfocado al Sistema De Gestión De La Seguridad De La Información que recopile los riesgos inherentes a la información, teniendo en cuenta una visión general de la actividad que desarrolla la empresa. Así mismo, la norma es clara al explicar las condiciones para llevar a cabo la implementación de distintos controles encaminados a proteger los errores que la organización tiene en cuanto al manejo de la información, ya sea en un caso particular o en cada elemento que compone el ciclo por el cual se moviliza la información.

Continuando con el contenido de la norma, las características que son consideradas esenciales en la elaboración de los objetivos, son los siguientes: 1. Ser coherentes con la política de seguridad de la información; 2. Ser medible (si es posible); 3. Tener en cuenta

los requisitos de la seguridad de la información aplicables, y los resultados de la valoración y el tratamiento de los riesgos; 4. Ser comunicados; 5. Ser actualizados, según sea apropiado; 6. Lo que se va hacer; 7. Qué recursos se requerirán; 8. Quién será responsable; 9. Cuando se finalizará; 10. Cómo se evaluarán los resultados.

Ahora bien, cuando los altos mandos de una organización toman la decisión de aplicar medidas que involucren la mejora en la seguridad de la información, los objetivos que se plantean dependen profundamente de la situación al interior de la misma y de varios factores que son decisivos para alcanzar el éxito de la empresa. Teniendo en cuenta la poca similitud entre la gran mayoría de las empresas, el planteamiento de los objetivos está sujeto a un análisis previo del contexto interno y externo, haciendo muy difícil que los objetivos sean exactamente los mismos en dos o más empresas.

**6.1.2.3 Servicios de la Seguridad de la Información.**

La implementación de la norma ISO 27001, se caracteriza por el acatamiento de un conjunto de recomendaciones encaminadas a la protección del activo más valioso que tienen las empresas hoy en día “la información”.

Al tener a consideración las necesidades que tienen las empresas, la información representa un papel fundamental en la eficiencia de las actividades que debe realizar un ente económico, lo cual obliga a incurrir en una serie de medidas encaminadas a salvaguardar la información. Por lo tanto, en vista a la vulnerabilidad en la que puede estar la información y de igual forma para cumplir los objetivos de la seguridad de la información, la norma ISO 27001 por medio de las recomendaciones, busca establecer, implementar, mantener y mejorar un sistema de seguridad de la información teniendo en cuenta el contexto de la organización, con la finalidad de preservar la confidencialidad, la integridad y la disponibilidad de la información.

**6.1.2.4. Elementos Vulnerables en el Sistema Informático.**

Discutir acerca del tema de la seguridad, constantemente será asociado con la falta de certeza dado que, aunque se apliquen los estándares más altos para proteger una determinada cosa, la incertidumbre estará presente volviendo en algo necesario hablar de

niveles de seguridad. En cuanto al sistema informático, actualmente ha tomado mucha importancia la protección, en la medida que a diario se presentan más problemas en asuntos relacionados con la informática, como consecuencia de las debilidades que encuentran diariamente los delincuentes. (Santos, 2014)

Al observar los elementos de un sistema informático que se pueden encontrar en un estado de vulnerabilidad, se clasifica habitualmente en: amenazas lógicas, amenazas físicas y amenazas en personas.

#### 6.1.2.4.1. Amenazas lógicas.

Las amenazas lógicas son todos aquellos programas que pueden estropear el sistema, ya sea porque se crearon con ese objetivo (malware) o por error como es el caso de los bugs o los agujeros. Entre los programas que pueden ocasionar problemas al sistema, según Santos (2014), están los siguientes:

#### 6.1.2.4.2. Amenazas físicas.

Las amenazas físicas, son aquellas fallas que pueden afectar el sistema informático por medio de un error o daño al hardware. Dentro del conjunto de amenazas más conocidas están los siguientes tipos:

- Hurtos, entorpecimiento y destrozo del sistema.
- Alteraciones del servicio de electricidad como cortes.
- Circunstancias atmosféricas máximas que ocasionarían fallas en el sistema.
- Calamidades provocadas por la naturaleza.

Como se logró evidenciar, en el conjunto de amenazas físicas existen varias que son muy poco probables, pero aun así muy nocivas para el sistema por lo que se vuelve indispensable tomas acciones ante este tipo de eventualidades.

#### 6.1.2.4.3. Personas que pueden constituir riesgos.

Sin lugar a dudas, al examinar un tema de tanta importancia para el sistema informático como son las amenazas, es inevitable no hablar del riesgo que causan las personas ya sea de forma voluntaria o involuntaria. Actualmente, se ha vuelto muy común

escuchar casos en las que algunas personas mal intencionadas emplean por intermedio de un software códigos que, al instante de ser activados accederán a la información privada del usuario con el único fin de cometer actos ilícitos. A pesar que este tipo de prácticas se han vuelto muy reiterativas, no se puede olvidar que diariamente también existe un alto grado de probabilidad que algún miembro de la empresa cometa errores con consecuencias severas para la organización.

A continuación, se nombrarán los riesgos más comunes que provocan los seres humanos en el sistema informático según Santos (2014):

- Personal.
- Ex- empleados.
- Hacker.
- Intrusos remunerados.

**6.1.2.5. Seguridad en Redes.**

Durante los últimos años, la seguridad en redes ha tomado cada vez un papel más necesario independientemente de la ocupación que se esté hablando, en vista de la incidencia que cumplen las redes al ejecutar una determinada acción. Como consecuencia de las exigencias del mercado en el presente, los profesionales deberán conocer temas que van más allá del área en la cual se desenvuelven, situando la seguridad en redes como un aspecto esencial para cumplir correctamente sus funciones. Sin embargo, la seguridad en redes no es un asunto exclusivamente del campo laboral, debido a las repercusiones que ha tenido en el siglo XXI para la sociedad en general, principalmente por el auge de internet que a diario se está reinventando con el fin de implementar cambios y ser más eficaz.

De igual modo, la humanidad ha venido desarrollando avances importantes a partir del surgimiento de la Revolución Industrial, destacando en el presente los sistemas, puesto que hacen presencia en prácticamente cualquier entorno de las grandes urbes. Pese a que pocas personas se plantean la idea de analizar cada objeto que se emplea a diario, el entorno en la mayoría de veces está marcado por la presencia de máquinas y redes ya sea públicas o privadas, que prestan un servicio para mantener a los seres humanos interconectados. En este orden de ideas, examinar el avance de la red es muy significativo en la medida que se

puede observar su funcionamiento, el cual depende de miles y miles de ordenadores interconectados entre sí, que no para de crecer con el objetivo de brindar un servicio cada vez más superior y de este modo lograr los beneficios que ofrece internet. No obstante, las ventajas que una red facilita a los seres humanos con el propósito de ejecutar diferentes tareas, suele tener tropiezos producto de una gran variedad de amenazas (lógica, física y humana), evidenciando lo complejo de tener una seguridad en la red, la cual permita mantener la tranquilidad y por lo tanto el funcionamiento correcto del sistema. (Díaz, Armendáriz, Ruiz, & Castro, 2014)

#### 6.1.2.6. Consecuencias de la Falta de Seguridad.

Considerar el valor que tiene la información en la actualidad, en algunas ocasiones es una tarea tediosa dado lo significativa que puede ser la información al interior de una organización. En este orden de ideas, los efectos por no proteger la información pueden derivar desde distintos puntos, causando consecuencias incalculables para una empresa, a causa que, en muchas oportunidades lo más afectado es la imagen y el buen nombre de una compañía. De tal manera, cundo se toma la decisión de implementar los estándares establecidos en la ISO 27000, se acepta una serie de prácticas y acciones orientadas a resguardar el activo más importante que actualmente poseen las empresas.

Estudiar las consecuencias o efectos que pueden surgir por la ausencia de seguridad de la información, sería como pensar un sinfín de escenarios puesto que las amenazas y errores son muy numerosos y es un tema que cada día se está reinventando. En nuestros días, es común observar que muchas personas o empresas fijen esfuerzos para proteger los datos y archivos que contiene un computador a través de un antivirus, pero con el inconveniente que se ignora o no se tiene el conocimiento suficiente para aplicar medidas en contra de las amenazas físicas. De acuerdo al sitio web preventionworld, en el contexto empresarial los errores humanos son tan frecuentes, que regularmente se escriben artículos en relación a este asunto y los resultados en la web son numerosos y aun así la complejidad que cada error se repita con las mismas características es casi imposible (Tasaico, 2015). En este sentido, si se evalúan los errores humanos en el entorno de la seguridad de la información, la situación es igual de compleja considerando que las circunstancias no siempre van a ser las mismas y los efectos de igual manera incalculables.

### 6.1.3. Capítulo 3: Activos de la información.

Al tratar los activos de la información de una organización, implica abarcar una gran variedad de temas que ayudarán a comprender lo que es un activo de la información, la necesidad de tenerlos organizados, la propiedad, la clasificación y la valoración que debe tener cada activo según las características de la organización.

#### 6.1.3.1. Activos de la información.

La norma ISO 27001 versión 2013 contiene una serie de recomendaciones que permiten asegurar todos los datos que conforman los activos de la información, los cuales sino cuentan con los controles adecuados podrían estar en una situación crítica de riesgo. De acuerdo a la política de seguridad de la información en la Universidad Distrital De Caldas, un activo de la información se puede definir como "Datos o información que se almacena en cualquier tipo de medio y que es considerada como sensitiva o crítica" (Caldas, 2011). De igual manera, los activos de la información desempeñan un papel relevante dado que hacen posible cumplir las funciones y los objetivos de la organización.

Adicionalmente, los activos de la información están conformados por un conjunto de datos pertenecientes a un ente económico. En este recurso, se puede guardar en un medio físico o virtual, desempeñando un papel fundamental en el logro de objetivos de una organización. En la actualidad, la información tiene una connotación económica en consecuencia a la importancia en la toma de decisiones de una empresa, de modo que su protección es convierte en algo necesario.

#### 6.1.3.2. Inventarios de activos.

Teniendo en cuenta el papel fundamental de los activos de la información al interior de las organizaciones, es imprescindible identificar, recolectar, clasificar (según el nivel del riesgo) y por último asegurarlo para mantener un orden. De igual manera, la elaboración del inventario de los activos se considera muy relevante para implementar un SGSI, tanto así que la Norma ISO 27001 en el anexo A al tratar la gestión de activos, la parte del inventario se convierte en una tarea indispensable al considerar la identificación de los

activos y las respectivas medidas de seguridad para dar cumplimiento a esa parte del anexo. (Instituto Colombiano de Normas Técnicas y Certificación, 2013)

Así mismo, la elaboración del inventario de activos implica evaluar una serie de aspectos catalogados como fundamentales, cuando se decide hacer la recolección de aquellos datos que merecen un grado de protección debido a la importancia que tienen al interior de la organización. Por lo tanto, los aspectos a tener en cuenta son:

- Identificar el rol que cumple dentro de la empresa el activo de la información, para posteriormente analizar su grado de importancia
- Conocer los medios o vínculos por los que habitualmente el activo de la información es transferido.
- Comprobar la ubicación y los recursos que se utilizan para almacenar cada uno de los activos de la información.
- Reconocer las personas que custodian o de la cual depende el activo de la información.
- Distinguir el grado de acceso o disponibilidad que los terceros podría tener sobre el activo de la información.

De esta forma, se tendrán los datos suficientes para que a continuación se logre valorar los activos de la información considerando criterios establecidos por un Sistema De Gestión De La Seguridad De La Información como la confidencialidad, integridad y disponibilidad. (Gómez & Rivero, Elaboración del inventario de activos, 2015)

**6.1.3.3. Propiedad de los Activos.**

Para realizar un inventario que agrupe todos los activos de la información, es fundamental establecer varios aspectos, destacando la identificación del responsable que está a cargo de cada activo. Cabe mencionar que a medida que se conoce la persona encargada del respectivo activo, se podrán determinar elementos decisivos para sustentar un control efectivo y de este modo disminuir el riesgo ante alguna eventualidad. De esta forma, el compromiso que tiene el personal que maneja información de carácter confidencial en una organización debe responder a una serie de características básicas, las

cuales estén encaminadas a fortalecer la confianza, las buenas intenciones y la sabiduría para preservar a la confidencialidad, integridad y la disponibilidad de la información.

En este orden de ideas, conocer la persona bajo la cual está a cargo permitirá distinguir componentes básicos, resaltando por obvias razones la responsabilidad que debe tener la persona a cargo, la capacidad y los procedimientos que se deberán cumplir para superar incidentes, las cláusulas que comprometerán al personal involucrado a no divulgar información una vez no continúe en la organización, entre otras.

#### 6.1.3.4. Clasificación de Activos.

Para realizar la clasificación de los activos, se deberá hacer de acuerdo a la importancia, en términos normativos, sensibilidad y beneficios que tiene para una organización. La clasificación se divide en tres elementos los cuales son: activos puros, activos físicos y activos humanos. (Servicio Nacional De Aprendizaje, 2018)

##### 6.1.3.4.1. Activos puros.

Los activos puros están compuestos por diferentes elementos, los cuales se caracterizan por tratar varios aspectos intangibles como: patentes, licencias sistemas operativos, etc. aunque también se tiene en cuenta datos tangibles.

Los principales activos catalogados como puros son:

- Datos digitales: Financieros, legales, de investigación y desarrollo, estratégicos y comerciales, correo electrónico, contestadores, automáticos, bases de datos, entre otros).
- Activos tangibles: Personales, financieros, legales, de investigación y desarrollo, estratégicos y comerciales, correo tradicional/electrónico, FAX, entre otros).
- Activos intangibles: Conocimiento, relaciones y secretos comerciales, licencias, patentes, experiencia, conocimientos técnicos, imagen).
- Software de aplicación: Propietario desarrollado por la organización, de cliente, planificación de recursos empresariales.

- Sistemas operativos: Servidores, computadores de escritorio, computadores portátiles, servidores centrales, entre otros. (Servicio Nacional De Aprendizaje, 2018)

**6.1.3.4.2. Activos físicos.**

En el caso de los activos físicos, agrupa al conjunto de elementos fácilmente observables por cualquier miembro de la organización, así como también los medios que suelen ser empleados para ejecutar las labores diarias.

Los principales activos catalogados como físicos son los siguientes:

- Infraestructura: Edificios, centros de datos, habitaciones de equipos y servidores, armarios de red o cableado, oficinas, entre otros.
- Controles del entorno: Equipos de alarma, supresión contra incendio, sistemas de alimentación ininterrumpida, entre otros.
- Hardware: Dispositivos de almacenamiento y cómputo como
- computadoras de escritorio, estaciones de trabajo, portátiles, equipos de mano, entre otros.
- Activos de servicios: Servicios de autenticación de usuario y administración de procesos de usuario, enlaces, cortafuegos, servidores proxy, servicios de red, servicios inalámbricos. (Servicio Nacional De Aprendizaje, 2018)

**6.1.3.4.3. Activos Humanos.**

En este tipo de clasificación, se agrupa a todos los individuos que conforman la organización y maneja información o datos catalogados como sensibles.

Los principales activos catalogados como humanos son los siguientes:

- Empleados: personal, directivos, directores ejecutivos, arquitectos de software y desarrolladores, entre otros.
- Externos: trabajadores temporales, consultores externos o asesores especialistas, contratistas especializados, entre otros. (Servicio Nacional De Aprendizaje, 2018)

**6.1.3.5. Valoración de Activos.**

Dado que no todos los activos poseen el mismo grado de importancia al interior de una empresa, es necesario establecer ciertos criterios para definir la jerarquía a la cual pertenece cada activo y de esta manera implementar medidas al respecto. De este modo, cumplir la valoración de activos implica observar aquellas cualidades que lo convierten en un bien preciado para la organización.

Generalmente existen opiniones divididas con respecto a la valoración de activos, en vista que hay quienes consideran oportuno aplicar una valuación cuantitativa enfocada en la valoración económica y la valuación cualitativa que combine números del 0 al 10 y niveles que van desde bajo, medio y alto. Cabe mencionar que, en este tipo de valoración es indispensable aplicar criterios homogéneos con el propósito de realizar una evaluación objetiva. Aunque se encuentran una gran variedad de métodos al momento de investigar acerca de este tema, los más conocidos son las encuestas y las entrevistas, complementando al organizador a seleccionar un determinado grupo de individuos al interior de la empresa, que permitan representar las necesidades que actualmente tiene la organización. (Servicio Nacional De Aprendizaje, 2018)

En este sentido, al iniciar la valoración de activos es indispensable tener en cuenta tres aspectos relevantes para la seguridad de la información los cuales son: disponibilidad, confidencialidad e integridad.

#### 6.1.3.5.1. Disponibilidad

Este aspecto trata acerca de que la información debe ser accesible a partir del momento en que sea requerida. En algunas situaciones, la ausencia de este factor se puede generar con situaciones muy comunes como por ejemplo cuando no se logra ingresar al e-mail de la compañía, por razones que van desde el olvido de la contraseña hasta la denegación del servicio por un ataque al sistema. (Servicio Nacional De Aprendizaje, 2018)

#### 6.1.3.5.2. Integridad

Este término, se refiere a aquellas características que debe cumplir la información, las cuales son la razonabilidad y por otra parte que esté exenta de equivocaciones y alteraciones. En este orden ideas, la información no está libre de errores voluntarios e

involuntarios que tengan repercusiones en las decisiones. (Servicio Nacional De Aprendizaje, 2018)

#### 6.1.3.5.3. Confidencialidad

Al tratar la confidencialidad, existe cierta confusión con respecto a la disponibilidad ya que se cree que existe incompatibilidad cuando se habla de estos dos términos, por lo que en el término de confidencialidad hace la aclaración que la información sea únicamente accesible al personal con aprobación previa. En contexto, la definición que desea acercarse a lo que es la confidencialidad en la seguridad de la información es conocida como "need to know", concepto que aclara la necesidad que la información debe ser exclusivamente accesible a individuos o sistema autorizados. (Servicio Nacional De Aprendizaje, 2018)

### 6.1.4. Capítulo 4: Valoración de Riesgos.

Durante el proceso de la valoración de riesgos, se desarrolla la comparación de los resultados obtenidos en la evaluación de los riesgos en relación con los controles, es preciso señalar, que lo anterior se realiza con el propósito de establecer un mejor empleo y determinación de las políticas. Es necesario tener en cuenta previamente, el hecho de entender todas las partes que constituyen el control de todos los procesos, ya que permiten alcanzar información y de este modo elegir una decisión que podría generar efectos positivos o negativos teniendo en cuenta la calidad de la misma.

En la norma ISO 27001 versión 2013, la valoración de los riesgos que atañen la información se encuentra ubicada en el capítulo 6 que trata acerca de la planificación, como aquellas acciones que deben ser implementadas para tratar riesgos y oportunidades. De acuerdo a la Norma, es fundamental que la organización defina y aplique un proceso de valoración de riesgos de la información el cual cumpla con los siguientes pasos:

- Establezca y mantenga criterios de riesgo de la seguridad de la información que incluyan los criterios de aceptación y los criterios para realizar valoraciones de riesgos de la seguridad de la información.
- Asegure que las valoraciones repetidas de riesgos de la seguridad de la información produzcan resultados consistentes, válidos y comparables.
- Identifiquen los riesgos de la seguridad de la información.

- Analice los riesgos de la seguridad de la información
- Evalúe los riesgos analizados para el tratamiento de riesgos.

Adicionalmente, se sugiere que la organización mantenga información documentada de los procesos que lleve a cabo. (Instituto Colombiano de Normas Técnicas y Certificación, 2013)

#### 6.1.4.1. Riesgo.

De acuerdo a la definición propuesta por el diccionario de la Real Academia Española, la palabra riesgo representa una contingencia o proximidad de un daño (Real Academia Española, 2018). Cabe señalar que, el término riesgo suele ser empleado cuando se desea hablar de una situación de peligro, no obstante, existe una notable diferencia entre estas dos palabras, ya que el peligro es una probabilidad de accidente y riesgo es la posibilidad de un daño.

En el contexto de un Sistema De Gestión De Seguridad De La Información, se dice que los riesgos ocurren como consecuencia de dos aspectos fundamentales los cuales son: amenazas y vulnerabilidad. Conviene mencionar que, tanto las amenazas como las vulnerabilidades siempre convergen y no puede existir la una sin presencia de la otra. Además, las amenazas suelen tomar superioridad a las vulnerabilidades, ya sea que provenga de factores externos o internos. (Tarazona C. , 2007).

Así mismo, la Norma ISO 31000 versión 2011 para la Gestión De Riesgo, considera el riesgo como efecto de la incertidumbre sobre los objetivos. Por lo tanto, la realización del documento se justifica porque todas las organizaciones al ejecutar una determinada actividad, deben asumir un riesgo ya sea interno o externo en cada acción que es elaborada. En esta medida, la identificación, análisis, evaluación y tratamiento, son aspectos claves para gestionar el riesgo, eso sí, teniendo muy presente una serie de principios para que el proceso sea eficaz.

#### 6.1.4.2. Principios de la Gestión del riesgo.

Como se dijo anteriormente, el éxito de la gestión del riesgo depende en gran medida de una serie de principios encaminados a la eficacia. Como consecuencia de lo

anterior, los once principios que sugiere el Instituto Colombiano de Normas técnicas y certificación (2011) en la Norma ISO 31000 para la gestión del riesgo son:

**6.1.4.2.1. La gestión del riesgo crea y genera valor:** A través de la gestión del riesgo, se logran alcanzar varios objetivos y de igual manera optimizar varios aspectos de gran relevancia para la organización, como por ejemplo la seguridad humana, la protección del medio ambiente, la calidad de los productos, entre otros. (Servicio Nacional De Aprendizaje, 2018)

**6.1.4.2.2. La gestión de lo riesgo es una parte integral de todos los procesos de la organización:** En este sentido, la gestión del riesgo no puede tratarse como una labor independiente de las actividades y procesos que ejecuta una empresa a diario. En consecuencia, la gestión del riesgo debe ser considerada como un elemento fundamental en la parte administrativa, en virtud a la confianza otorgada para tomar buenas decisiones y así mismo promover para que la gestión del riesgo se convierta en algo inherente del espectro general de la compañía. (Servicio Nacional De Aprendizaje, 2018)

**6.1.4.2.3. La gestión del riesgo es parte de las decisiones:** Dada la importancia de las decisiones que se toman a diario, por medio de la gestión del riesgo se obtiene un plus ya que suele existir más información, permite otorgar más preminencia a ciertas acciones y analizar diferentes alternativas. (Servicio Nacional De Aprendizaje, 2018)

**6.1.4.2.4. La gestión del riesgo aborda explícitamente la incertidumbre:** Por medio de la gestión del riesgo, la incertidumbre se observa de forma más detallada, de dónde proviene y las acciones a tener en cuenta para ser tratada. (Servicio Nacional De Aprendizaje, 2018)

**6.1.4.2.5. La gestión del riesgo es sistemática, estructurada y oportuna:** Tener a consideración una perspectiva sistemática, estructurada y oportuna, ayudara a obtener resultados consistentes, comparables y confiables. (Servicio Nacional De Aprendizaje, 2018)

**6.1.4.2.6. La gestión del riesgo se basa en la mejor información disponible:** El proceso de la gestión del riesgo, se fundamenta de información que va desde datos históricos,

experiencia, retroalimentación de las partes involucradas, observación, previsiones y examen de expertos. No obstante, las personas encargadas de tomar decisiones tienen la obligación de considerar las limitaciones de las fuentes utilizadas. (Servicio Nacional De Aprendizaje, 2018)

**6.1.4.2.7. La gestión del riesgo está adaptada:** La gestión del riesgo debe estar encaminada de acuerdo al ambiente interno o externo y tener muy presenta el perfil del riesgo por parte de la organización. (Servicio Nacional De Aprendizaje, 2018)

**6.1.4.2.8. La gestión del riesgo toma a consideración los factores humanos y culturales:** Es importante reconocer las características que tienen individuos ya sea en el entorno externo o interno, ya que ayudará a entender si representa una oportunidad o amenaza para la organización. (Servicio Nacional De Aprendizaje, 2018)

**6.1.4.2.9. La gestión del riesgo es transparente e inclusiva:** El acercamiento entre todas las partes que componen a la organización, en especial aquella encargada en tomar las decisiones al interior de la organización, contribuirá a tener diferentes puntos de vista y de este modo también existirá una representación para todos. (Servicio Nacional De Aprendizaje, 2018)

**6.1.4.2.10. La gestión del riesgo es dinámica, reiterativa y sensible al cambio:** Las acciones que representan alteraciones en la organización y que se presentan a diario pueden provenir del entorno externo o interno, dando lugar a nuevas situaciones que significan en un riesgo u oportunidad. (Servicio Nacional De Aprendizaje, 2018)

**6.1.4.2.11. Facilita la mejora continua a de la organización:** Por el bienestar de la organización, la mejora continua tanto en los sistemas de calidad como a nivel general es necesario mediante el desarrollo e implementación de estrategias. (Servicio Nacional De Aprendizaje, 2018)

**6.1.4.3. Clasificación del riesgo.**

Considerar el número de riesgos a los que una organización está expuesta, es una tarea sumamente complicada puesto que, a diario los delincuentes buscan la forma de vulnerar el sistema y la protección actualmente existente no es un 100% segura. Por

consiguiente, la forma de clasificar los riesgos contempla un número significativo de acciones perjudiciales para una empresa, a través de una clasificación de grupos homogéneos que tiene como prioridad el daño que representa.

Así pues, los tipos de riesgos que existen son los siguientes:

**6.1.4.3.1. Riesgos internos:** Se refiere a los riesgos originados al interior de una organización.

**6.1.4.3.2. Riesgos externos:** Se refiere a los riesgos originados en el ambiente exterior de una organización.

**6.1.4.3.3. Riesgo de negocios:** Son aquellas decisiones inherentes a la actividad que desempeña la organización. Es considerado como uno de los riesgos más críticos.

**6.1.4.3.4. Riesgo inherente:** Este tipo de riesgos contempla la probabilidad de fallas en la información de tipo financiera, administrativa o en la parte operativa, previamente al analizar el éxito de los controles planeados y puestos en marcha por la empresa.

**6.1.4.3.5. Riesgo de auditoría:** Al ejecutar un programa de auditoría, existen métodos que nos alcanzan para encontrar todos los problemas más relevantes.

**6.1.4.3.6. Riesgo de control:** En este caso, los riesgos están relacionados con acciones de control interno, la cual relaciona directamente a la auditoría interna, en vista a que no se puede prevenir totalmente los errores o problemas en la organización. (Servicio Nacional De Aprendizaje, 2018)

**6.1.4.4. Fases para la valoración del Riesgo.**

Una vez se ha llevado a cabo el procedimiento de la valoración del riesgo, es necesario proceder con la identificación de los activos de la información y de esta forma establecer un valor para los elementos que fueron identificados. De este modo, la valoración del riesgo cumple una gran ayuda para la organización, ya que por medio de la identificación se podrá observar el nivel de impacto que originaría en el caso hipotético que caiga en las manos equivocadas.

Con la finalidad de ejecutar la valoración del riesgo, es indispensable tener a consideración dos etapas, las cuales son las siguientes:

**6.1.4.4.1. Identificación de riesgos:** Esta etapa permite definir cada uno de los activos que tiene la empresa, los riesgos a los que es propenso dicho activo y posteriormente se le da mayor importancia a los activos que se encuentran más expuestos y de acuerdo a la relevancia al interior de la organización. (Servicio Nacional De Aprendizaje, 2018)

**6.1.4.4.2. Identificación de controles:** De acuerdo a los riesgos hallados en la etapa anterior, se establece, organiza y se hace un continuo acompañamiento a los controles establecidos, con la finalidad de atender y eliminar los riesgos. (Servicio Nacional De Aprendizaje, 2018)

**6.1.4.5. Valoración del Riesgo.**

Una vez se ha llegado a esta etapa, es preciso contemplar la posibilidad que un riesgo llegue a ocurrir y el grado de afectación que puede generar para la organización. Para establecer el grado de ocurrencia de un riesgo, se tienen en cuenta los siguientes parámetros: Nada Frecuente, Poco Frecuente, Normal, Frecuente, Muy Frecuente.

*Ilustración 3: Valoración del Riesgo.*

| Valor | Frecuencia | Ocurrencia |
|---|---|---|
| 0.2 | Nada frecuente | No ha sucedido. |
| 0.4 | Poco frecuente | Sucede cada 10 años. |
| 0.6 | Normal | Sucede una vez al año. |
| 0.8 | Frecuente | Sucede mensualmente. |
| 1 | Muy frecuente | Sucede diariamente. |

Fuente: Servicio Nacional De Aprendizaje (2018)

El paso a seguir consiste en determinar el grado de impacto para el activo teniendo en cuenta la probabilidad de ocurrencia, acto seguido se procederá a determinar el deterioro a través de los siguientes ítems: Insignificante, Menor, Moderado, Mayor y Catastrófico.

*Ilustración 4: Nivel de Degradación.*

| Valor | Degradación | Ocurrencia |
|---|---|---|
| 0.2 | Insignificante | El activo no sufre daños que impidan su operación. |
| 0.4 | Menor | El activo sufre daños y puede continuar operando. |
| 0.6 | Moderado | El activo sufre daños y su operación es restringida. |
| 0.8 | Mayor | El activo sufre daños que impiden su operación y puede recuperar dentro del tiempo tolerable para la operación. |
| 1 | Catastrófico | El activo sufre daños irreparables y la operación se altera considerablemente. |

Fuente: Servicio Nacional De Aprendizaje (2018)

En vista a que ya se halló la probabilidad que un riesgo ocurra y la estimación del impacto, a continuación, se realizará el cálculo del riesgo inherente y el riesgo marginal.

**6.1.4.5.1. Riesgo Inherente:** Los riesgos inherentes, se refiere a aquellas amenazas intrínsecas de la materia, originadas por diferentes motivos como fallas, problemas e inconvenientes los cuales, de forma individual o grupal podrían generar serias complicaciones a la organización. Para resolver las complicaciones, se han creado controles compuestos por la alta gerencia con el propósito de disminuir su probabilidad de ocurrencia.

Los riesgos inherentes más comunes, son:

- Riesgo de crédito.
- Riesgo financiero.
- Riesgo operacional.
- Riesgo de tecnología de la información.
- Riesgo Calidad de Servicio y Transparencia de la Información.

Para el cálculo del riesgo inherente se utiliza la siguiente fórmula:

Riesgo inherente = frecuencia * degradación.

- Frecuencia: Es el valor obtenido de la probabilidad de que ocurra una amenaza.
- Degradación: Es el valor obtenido de la estimación de impacto. (Servicio Nacional De Aprendizaje, 2018)

**6.1.4.5.2. Riesgo Marginal:** El riesgo marginal, trata acerca del límite que pueden tener las amenazas al interior de la organización.

Para el cálculo del riesgo marginal se utiliza la siguiente fórmula:

Riesgo marginal = Riesgo inherente * Marginalidad

- Riesgo inherente: Es calculado en el tema anterior (riesgo inherente).
- Marginalidad**:** Es el valor obtenido en la evaluación de control del riesgo. (Servicio Nacional De Aprendizaje, 2018)

## 6.2. Marco Conceptual.

### 6.2.1. Activo:

Se identifican los activos de información de mayor importancia asociados a cada Sistema de Procesamiento de la Información en su respectivo proceso, con sus Responsables y su Ubicación, para luego elaborar un inventario con dicha información. (Ministerio del Interior de Colombia, 2014)

La información es un activo que la compañía considera esencial para las actividades de la empresa y debe ser protegida de acuerdo con los principios de confidencialidad, integridad y disponibilidad. (Celsia, 2014)

Cuando se habla del concepto “activo” en el contexto de la seguridad de la información, hace referencia a todo tipo de documentos, bases de datos, CD´S, USB, etc. En el cual se encuentran almacenados datos que son catalogados al interior de una organización como esenciales, para desempeñar su respectiva actividad económica.

### 6.2.2. Amenaza:

Una amenaza, en términos simples, es cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan. (Tarazona C. H., 2013)

Es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas. (Instituto Nacional De Ciberseguridad, 2017)

Una amenaza es cualquier evento que puede afectar al activo de un sistema de información, provocando un incidente de seguridad y produciendo efectos adversos (materiales o inmateriales) o pérdidas de información. (Tejada, 2014)

En el ambiente empresarial, al hablar de una amenaza esta puede significar un concepto muy general teniendo en cuenta el grado de riesgos que se presentan a diario en cada área de la organización, pero al enfocarlo en los sistemas de información, está relacionado con la posibilidad que se genere una pérdida de la información, como consecuencia de los errores y la vulnerabilidad que es el sistema de información.

### 6.2.3. Análisis del Riesgo:

Uso sistemático de la información para identificar las fuentes y estimar el riesgo. (Instituto Colombiano de Normas Técnicas y Certificación, 2005)

Proceso llevado a cabo para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

El análisis de riesgo está relacionado con el estudio minucioso de la información, con la finalidad de establecer, identificar y estimar las causas de posibles sucesos que pueden afectar el bienestar de la organización.

### 6.2.4. Control:

El control es el proceso de verificar el desempeño de distintas áreas o funciones de una organización. Usualmente implica una comparación entre un rendimiento esperado y

un rendimiento observado, para verificar si se están cumpliendo los objetivos de forma eficiente y eficaz y tomar acciones correctivas cuando sea necesario. (Anzil, 2010)

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. (Instituto Nacional De Salud, 2018)

El concepto de control, tiene que ver con comprobar, verificar, inspeccionar, vigilar e intervenir un determinado hecho, el cual representa un aspecto esencial para el desempeño al interior de una organización.

### 6.2.8. Vulnerabilidad:

Probabilidad de ocurrencia y los efectos que podrían suponer que se materializara la amenaza, es decir, que una amenaza explora la debilidad de un activo. (Fernández & Alvaréz, 2012)

Es la debilidad que puede presentar un activo sobre una amenaza. (Bolaños & Mora, 2013)

La vulnerabilidad hace referencia a lo indefenso que puede ser un sistema, en relación a diferentes ataques que podrían afectar gravemente el bienestar de un sistema de información en una organización.

### 6.2.9. Valoración del riesgo:

Proceso global de análisis y evaluación del riesgo. (Icontec, 2006)

Proceso de evaluar el riesgo que surge de un peligro teniendo en cuenta la suficiencia de los controles existentes y de decidir si el riesgo es aceptable o no. (Instituto Colombiano de Normas Técnicas y Certificación, 2007)

La valoración de riesgo establece diferentes variables como la como la identificación, el análisis y la evaluación, las cuales permiten cuantificarlo, medirlo y

establecer su nivel de afectación en la organización. La valoración es de gran importancia debido a que otorga a las organizaciones un método para establecer estrategias para mitigar los riesgos.

## 6.3. Marco Legal, normativo y Jurisprudencial.

### 6.3.1. Leyes, Normas, decretos, entre otros mandatos legales.

*Tabla 2: Leyes, Normas, decretos, entre otros mandatos legales.*

| NORMATIVIDAD RELACIONADA | DESCRIPCIÓN |
|---|---|
| **Constitución Política de Colombia artículo 15.** | De acuerdo al artículo 15 de la constitución política, todos los colombianos tienen derecho a la intimidad personal y familiar y a su buen nombre, por lo tanto, el estado está en la obligación de velar por respetarlo y promover que se respete. Así miso, los ciudadanos disponen del derecho a conocer, renovar y corregir los datos que se han recopilado en empresas públicas o privadas. |
| **Constitución Política de Colombia artículo 20.** | El estado deberá garantizar a las personas en general la libertad de manifestar y divulgar su forma de pensar y juicio, de igual manera, informar y recibir información verídica y objetiva. |
| **Ley 527 de 1999.** | Precisa y regula el ingreso y utilización de los mensajes de datos, E- commerce y firma digital y determina las instituciones encargadas de la certificación, así como otras disposiciones. |
| **La ley 1266 de 2008.** | Establece las disposiciones de todo lo inherente al Hábeas Data y reglamenta la información que comprende las bases de datos personales, especialmente al tratar temas financieros, crediticios, comerciales y la información que procede de otros países. |
| **Ley 1273 de 2009.** | Modifica el Código Penal e instaura un nuevo bien jurídico denominado “de la protección de la información y de los datos” y ayuda a resguardar los sistemas que emplean las tecnologías de la información y lo demás relacionado con las comunicaciones. |
| **La Ley 1581 de 2012.** | Decreta las disposiciones generales para la protección de datos, de esta forma determinar parámetros específicos para salvaguardar los datos registrados en alguna de las diferentes bases de datos, que permiten el uso, circulación, recolección y almacenamiento de información pública o privada. Para los datos financieros se encuentra establecida la Ley 1266 de 2008. |

| | |
|---|---|
| **Decreto 1377 de 2013.** | Se reglamentaron las políticas de tratamiento de datos personales tanto para quienes la administran como para quienes la suministran y para quienes figuran como titulares se estableció la autorización, en cumplimiento de la Ley 1581 de 2012. |
| **Decreto 886 de 2014.** | Se dictan disposiciones especiales para el artículo 25 de la Ley 1581 de 2012 (Régimen general de protección de datos personales). Estas disposiciones se refieren a los parámetros que deben contener las bases de datos personales sujetas a tratamiento que operan en el país, por lo cual se estableció la constitucionalidad condicionada del mencionado artículo y preciso que el registro nacional de bases de datos debe permitir "a cualquier persona determinar quién está haciendo tratamiento de sus datos personales para de esa forma garantizar que la persona pueda tener un control efectivo sobre sus datos personales al poder conocer clara y certeramente en qué bases se manejan sus datos personales. Por ende, el Gobierno Nacional tendrá en su labor de reglamentación que acudir a los estándares internacionales y a la experiencia de otros Estados en la materia para lograr que la finalidad antes descrita de este registro se cumpla" |
| **Resolución SIC No. 76434 de 2012.** | se expide por la Superintendencia de Industria y Comercio y por medio de ella se establecen las instrucciones inherentes a la protección de los datos personales, especialmente en relación a la Ley 1266 de 2008. |
| **Circular Externa SFC 052 de 2007.** | Por la cual la Superintendencia Financiera de Colombia incrementa los estándares de seguridad y calidad para el manejo de la información a través de medios y canales de distribución de productos y servicios que ofrecen a sus clientes y usuarios las entidades vigiladas por esta Entidad. |

Fuente: Elaboración propia.

### 6.3.2. Norma ISO 27001 VERSIÓN 2013.

El propósito por el cual fue creada esta norma, es con la finalidad de brindar una serie de sugerencias para establecer, implementar, mantener y mejorar de forma continua un sistema para la gestión de la seguridad de la información. Es importante mencionar que, los elementos anteriormente sugeridos, están sujetos a las exigencias que disponga el sistema, así como los objetivos, la protección, las actividades y las dimensiones que tenga la organización. Por último, esta norma incluye las condiciones para implementar la

valoración y el tratamiento de aquellos riesgos inherentes al sistema, ajustados a las características que tenga la organización.

Por otra parte, la norma es clara al referirse a la importancia de aplicar los numerales que van del 4 al 10 los cuales son: Contexto de la organización; Liderazgo; Planificación; Soporte; Operación; Evaluación del desempeño; Mejora.

Al tratar con el contexto de la organización, la norma en primer lugar habla acerca de la necesidad de conocer el contexto interno y externo del ente económico objeto de análisis dado el nivel de influencia que puede tener sobre el sistema de gestión de seguridad de la información. De igual manera, conocer aspectos como las aspiraciones que tienen las partes interesadas, el alcance y la utilidad que tendrá el sistema, son elementos fundamentales que la Norma ISO 27001 versión 2013 concibe en este numeral. (Instituto Colombiano de Normas Técnicas y Certificación, 2013)

Así mismo, otra parte relevante que nombra la Norma ISO 27001 versión 2013 tiene que ver con el liderazgo que debe demostrar la parte directiva durante el desarrollo del proceso. En primera medida, es fundamental que la alta dirección se comprometa a dar cumplimiento con la política y los objetivos de la seguridad de la información, integrar las condiciones que tiene el Sistema De Gestión De Seguridad De La Información, cerciorarse de la disponibilidad en los recursos para operar el SGSI manifestar a todos los miembros de la organización la importancia de tener una gestión de seguridad de la información eficaz y conforme a las condiciones del SGSI, entre otros. De igual modo, es relevante instaurar una política de la seguridad de la información que cumpla con una serie de requisitos como: que sea conforme con los objetivos de la organización, adicione los objetivos que menciona la Norma en el numeral 6.2, incorpore el compromiso que exige la aplicación del SGSI y tener muy presente la mejora continua. Finalmente, es primordial que la alta dirección confiera roles y responsabilidades de acuerdo a los requisitos que sugiere el sistema e informar la ejecución que ha tenido el SGSI. (Instituto Colombiano de Normas Técnicas y Certificación, 2013)

Uno de los puntos más significativos que tiene la norma es el numeral 6, el cual habla de la planificación. Este numeral es considerado como uno de los más importantes

que dispone la norma, puesto que señala unas ordenanzas que deberán cumplir las organizaciones que deseen a tener un SGSI más seguro, por medio de la asociación de otros elementos que tiene la Norma como lo es el numeral 4 que trata el análisis del contexto. De esta manera, la composición del numeral 6 está conformado por la valoración y el tratamiento de los riesgos, de acuerdo a unos requisitos que se complementan con la Norma ISO 31000 versión 2011 y el Anexo A que está al final de la Norma ISO 27001 versión 2013. Igualmente, están los objetivos que deben acatar las organizaciones, aspecto que, según lo avanzado hasta el momento, ha sido nombrado en diferentes partes como respuesta a la necesidad de cumplir los diez objetivos a lo largo del proceso. (Instituto Colombiano de Normas Técnicas y Certificación, 2013)

Posteriormente a la planificación viene la parte inherente a los soportes, conformada por cinco elementos que van desde la necesidad de contar con los recursos necesarios hasta la recopilación de la información documentada. Al tener presente los recursos, en la norma únicamente se menciona la necesidad de contar con los medios para cumplir con el propósito de establecer, implementar, mantener y mejorar el SGSI. Además, la competencia es otra de las tareas que hacen parte del soporte, convirtiendo a los altos directivos de una organización a establecer las acciones de aquellas personas que desempeñan una determinada labor en el SGSI, cerciorarse que las personas cuentan con las habilidades esenciales para que no ocurran errores involuntarios, entre otros aspectos. Por otra parte, la toma de conciencia y la comunicación son consideradas fundamentales para dar cumplimiento a las diferentes etapas que hacen parte del proceso de establecer, implementar, mantener y mejorar un SGSI. El último tema que hace parte del soporte es la información documentada, estimando una serie de aspectos básicos, la obligación de mantener actualizada la información y el control de la misma. (Instituto Colombiano de Normas Técnicas y Certificación, 2013)

La operación, es otro de los elementos fundamentales que dispone la norma, ya que se conecta con otros elementos que menciona la norma, principalmente el numeral 6.1. Que son las acciones para tratar los riesgos y las oportunidades y el numeral 6.2. Que son los objetivos del SGSI. (Instituto Colombiano de Normas Técnicas y Certificación, 2013)

# 7. Desarrollo: Resultados y Hallazgos

## 7.1. Capítulo 1: Metodología y criterios para el análisis de la gestión del riesgo asociados al Sistema de Gestión de la Información en el Cuerpo de Bomberos Voluntarios de Tunja.

En el capítulo 1, se explicarán las generalidades de los principales documentos que fueron indispensables para desarrollar este trabajo de investigación, destacando en primer lugar la Norma ISO 27001 versión 2013 como base central para entender los componentes claves que debe cumplir un Sistema de Gestión de la Seguridad Información, así como complemento de la Norma ISO 31000 versión 2011 que trabaja en conjunto con la Norma ISO 27001 versión 2013 en algunos aspectos (en especial al tratar temas relacionados con el riesgo) y la metodología para la gestión del riesgo "Magerit", la cual fue empleada para entender más a fondo el pasa a paso que se debe llevar a cabo al instante de analizar el estado del sistema de gestión de seguridad de la información.

En lo que concierne a la norma ISO 27001 versión 2013, se expondrán de forma resumida los ítems que son de obligatorio cumplimiento para ejecutar un análisis al sistema de gestión de seguridad de la información en cualquier organización. De acuerdo a lo que establece la Norma, los puntos que se deberán cumplir son los siguientes: Contexto de la organización, liderazgo, planificación, soporte, operación, evaluación de desempeño y mejora continua. Además de examinar esos elementos, en el desarrollo del presente trabajo también se tendrán en cuenta los anexos, en vista a que son un componente primordial para conocer más a fondo el estado actual de la empresa objeto de análisis.

Para el caso de la Norma ISO 31001 versión 2011, se tuvo en cuenta la penúltima versión debido a que es la que contempla la Norma ISO 27001 versión 2013 para entender más detalladamente los elementos inherentes a esta Norma como el conocimiento de la organización y el plan de tratamiento de riesgos. Es así que se explicarán de forma resumida todos los componentes que conforman esta Norma especializada en la gestión del riesgo, en la medida que una vez se llegue a la valoración y al plan de tratamiento de riesgos, la Norma ISO 27001 versión 2013 exige que se revisen los principios y directrices ya que las dos normas de calidad se encuentran alineadas.

Por último, la metodología hallada para entender mejor cada procedimiento del análisis del riesgo fue el libro I de Magerit, en especial la parte que trata el "método de análisis de riesgos". Las principales razones para escoger a Magerit ante otras metodologías son: que esta metodología está compuesta de varias sugerencias que fueron tenidas en cuenta desde el principio de la investigación, tiene muchos años de experiencia y ha sido aplicada innumerables veces en empresas reales, es de acceso gratuito y, por último, el libro I explica de manera muy detallada los pasos que se deben ejecutar para el análisis del riesgo. En resumen, los pasos son los siguientes: el primero consiste en determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación; más adelante determinar a qué amenazas están expuestos aquellos activos; después determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo; posteriormente estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza y por último estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

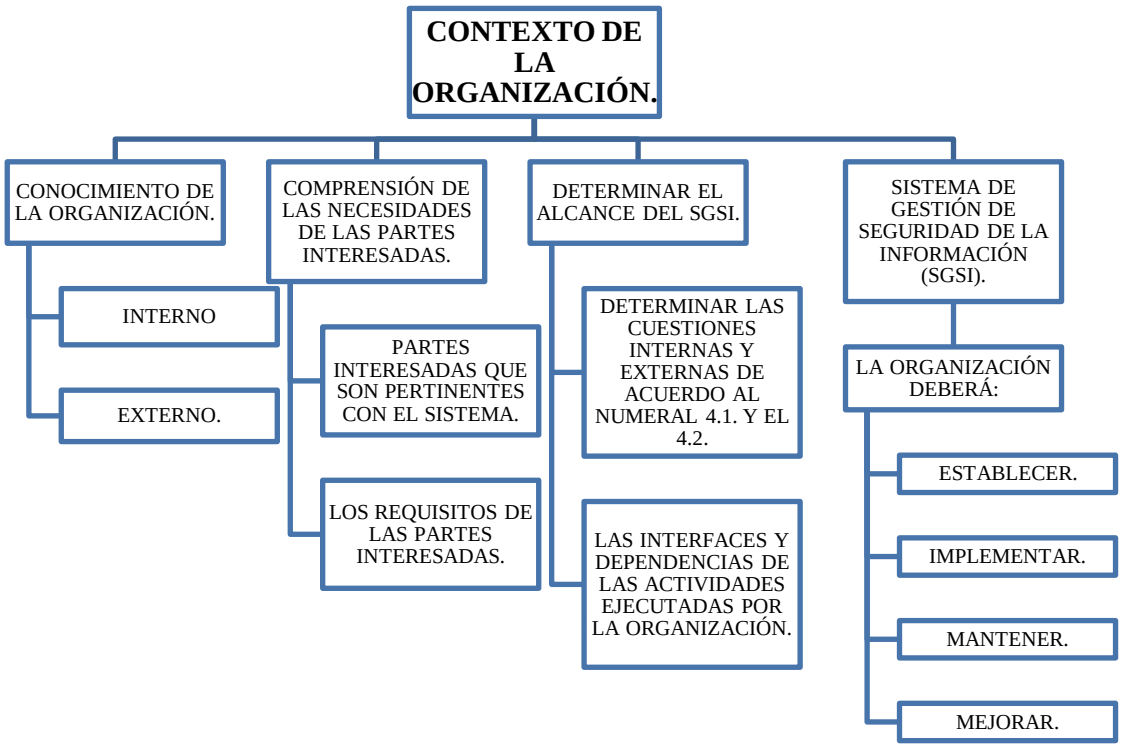
### 7.1.1 Norma ISO 27001 VERSIÓN 2013.

El propósito por el cual fue creada esta norma, es con la finalidad de brindar una serie de sugerencias para establecer, implementar, mantener y mejorar de forma continua un sistema para la gestión de la seguridad de la información. Es importante mencionar que, los elementos anteriormente sugeridos están sujetos a las exigencias que disponga el sistema, así como adicionalmente los objetivos, la protección, las actividades y las dimensiones que tenga la organización. Por último, esta norma incluye las condiciones para implementar la valoración y el tratamiento de aquellos riesgos inherentes al sistema, ajustados a las características que tenga la organización.

Por otra parte, la norma es clara al referirse a la importancia de aplicar los numerales que van del 4 al 10 los cuales son: Contexto de la organización; Liderazgo; Planificación; Soporte; Operación; Evaluación del desempeño y Mejora.

#### 7.1.1.1. Contexto de la organización.

*Figura 2: Contexto De La Organización.*

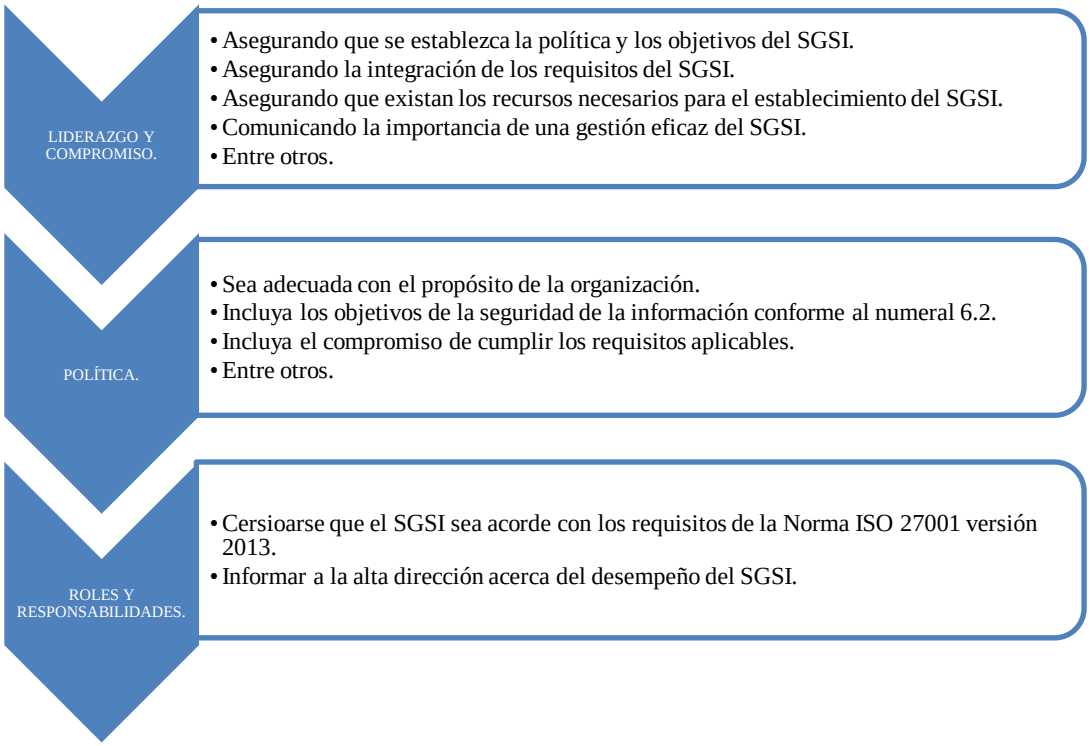



Fuente: Elaboración propia.

Al tratar con el contexto de la organización, la norma en primer lugar habla acerca de la necesidad de conocer el contexto interno y externo del ente económico objeto de análisis, dado el nivel de influencia que puede tener sobre el sistema de gestión de seguridad de la información. De igual manera, conocer aspectos como las aspiraciones que tienen las partes interesadas, el alcance y la utilidad que tendrá el sistema, son elementos fundamentales que la Norma ISO 27001 versión 2013 concibe en este numeral. (Instituto Colombiano de Normas Técnicas y Certificación, 2013)

### 7.1.1.2. Liderazgo.

*Figura 3: Liderazgo.*



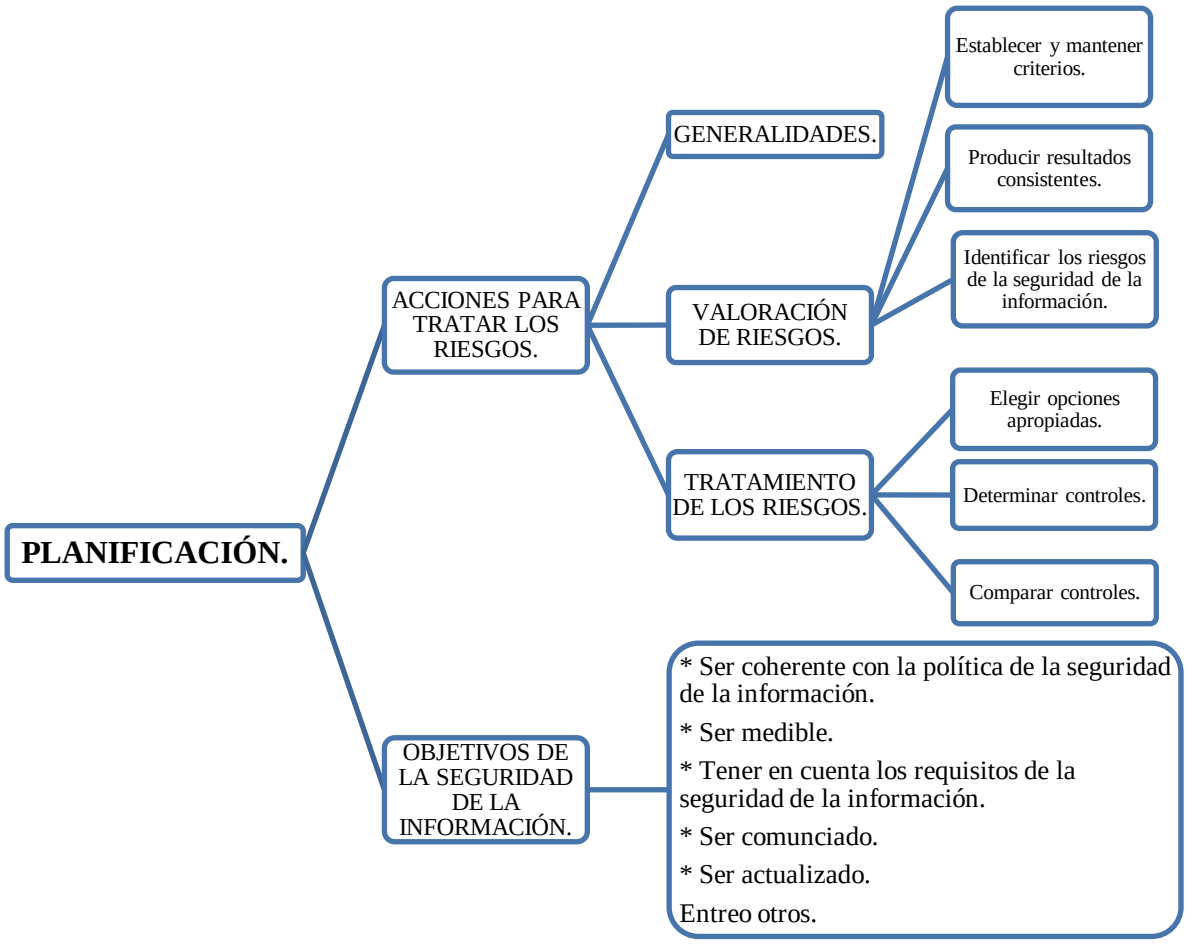

Fuente: Elaboración propia.

Así mismo, otra parte relevante que nombra la Norma ISO 27001 versión 2013 tiene que ver con el liderazgo que debe demostrar la parte directiva durante el desarrollo del proceso. En primera medida, es fundamental que la alta dirección se comprometa a dar cumplimiento con la política y los objetivos de la seguridad de la información, integrar las condiciones que tiene el Sistema De Gestión De Seguridad De La Información, cerciorarse de la disponibilidad en los recursos para operar el SGSI, manifestar a todos los miembros de la organización la importancia de tener una gestión de seguridad de la información eficaz conforme a las condiciones del SGSI. De igual modo, es relevante instaurar una política de la seguridad de la información que cumpla con una serie de requisitos como: que sea conforme con los objetivos de la organización, adicione los objetivos que menciona la Norma en el numeral 6.2 (Objetivos de la seguridad de la información), incorpore el compromiso que exige la aplicación del SGSI y tener muy presente la mejora continua. Finalmente, es primordial que la alta dirección confiera roles y responsabilidades de

acuerdo a los requisitos que sugiere el sistema e informar la ejecución que ha tenido el Sistema de gestión de seguridad de la información. (Instituto Colombiano de Normas Técnicas y Certificación, 2013)

**7.1.1.3. Planificación.**

*Figura 4: Planificación.*



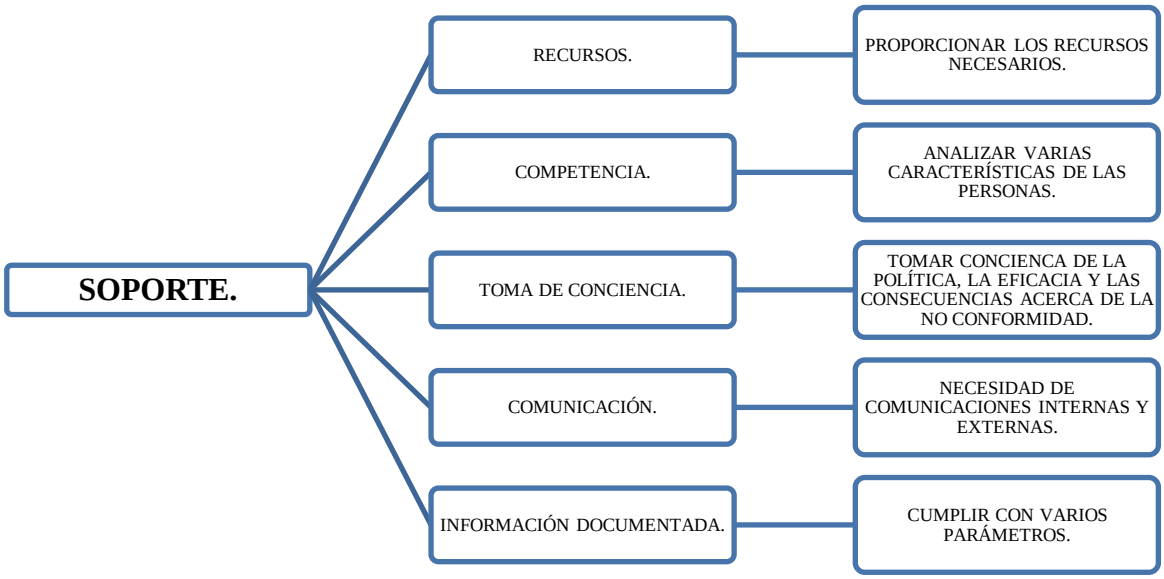

Fuente: Elaboración propia.

Uno de los puntos más significativos que tiene la norma es el numeral 6, el cual habla de la planificación. Este numeral es considerado como uno de los más importantes que dispone la norma, puesto que señala unas ordenanzas que deberán cumplir las

organizaciones que deseen tener un SGSI más seguro, por medio de la asociación de otros elementos que tiene la Norma como lo es el numeral 4 que trata el análisis del contexto. De esta manera, la composición del numeral 6 está conformado por la valoración y el tratamiento de los riesgos, de acuerdo a unos requisitos que se complementan con la Norma ISO 31000 versión 2011 y el Anexo A que está al final de la Norma ISO 27001 versión 2013. Igualmente, están los objetivos que deben acatar las organizaciones, aspecto que, según lo avanzado hasta el momento, ha sido nombrado en diferentes partes como respuesta a la necesidad de cumplir los diez objetivos a lo largo del proceso. (Instituto Colombiano de Normas Técnicas y Certificación, 2013)

#### 7.1.1.4. Soporte.

*Figura 5: Soporte.*



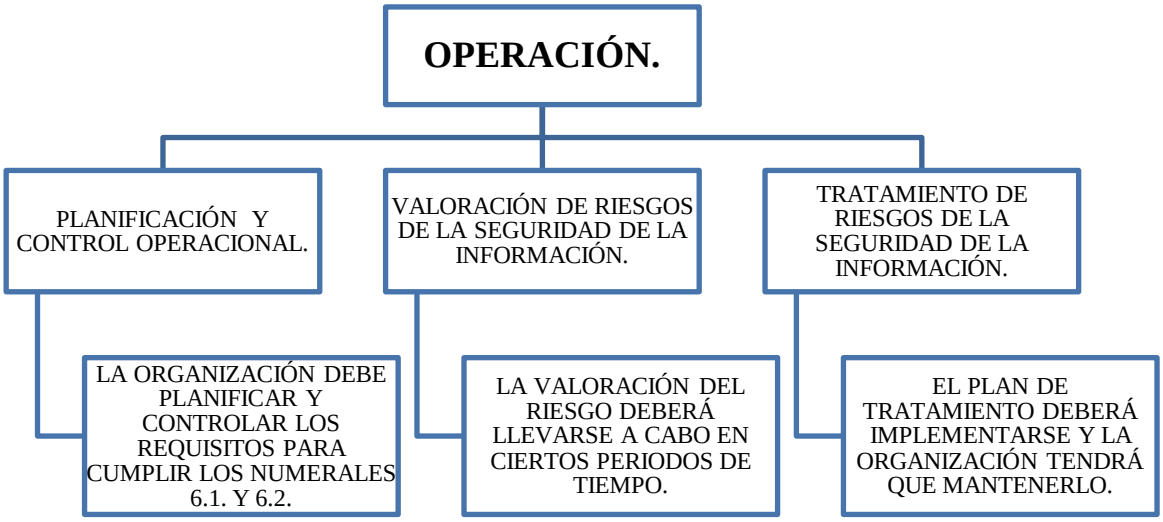

Fuente: Elaboración propia.

Posteriormente a la planificación viene la parte inherente a los soportes, conformada por cinco elementos que van desde la necesidad de contar con los recursos necesarios hasta la recopilación de la información documentada. Al tener presente los recursos, la norma únicamente menciona la necesidad de contar con los medios suficientes para cumplir con el propósito de establecer, implementar, mantener y mejorar el SGSI. Por otro lado, un elemento primordial es la competencia, convirtiendo a los altos directivos de

una organización en un eje fundamental para establecer las acciones de aquellas personas que desempeñan una determinada labor en el SGSI, cerciorarse que las personas cuentan con las habilidades esenciales para que no ocurran errores involuntarios, entre otros aspectos. Adicionalmente, la toma de conciencia y la comunicación son consideradas fundamentales para dar cumplimiento a las diferentes etapas que hacen parte del proceso de establecer, implementar, mantener y mejorar un SGSI. El último tema que hace parte del soporte es la información documentada, estimando una serie de aspectos básicos, la obligación de mantener actualizada la información y el control de la misma. (Instituto Colombiano de Normas Técnicas y Certificación, 2013)

**7.1.1.5. Operación.**

*Figura 6: Operación.*

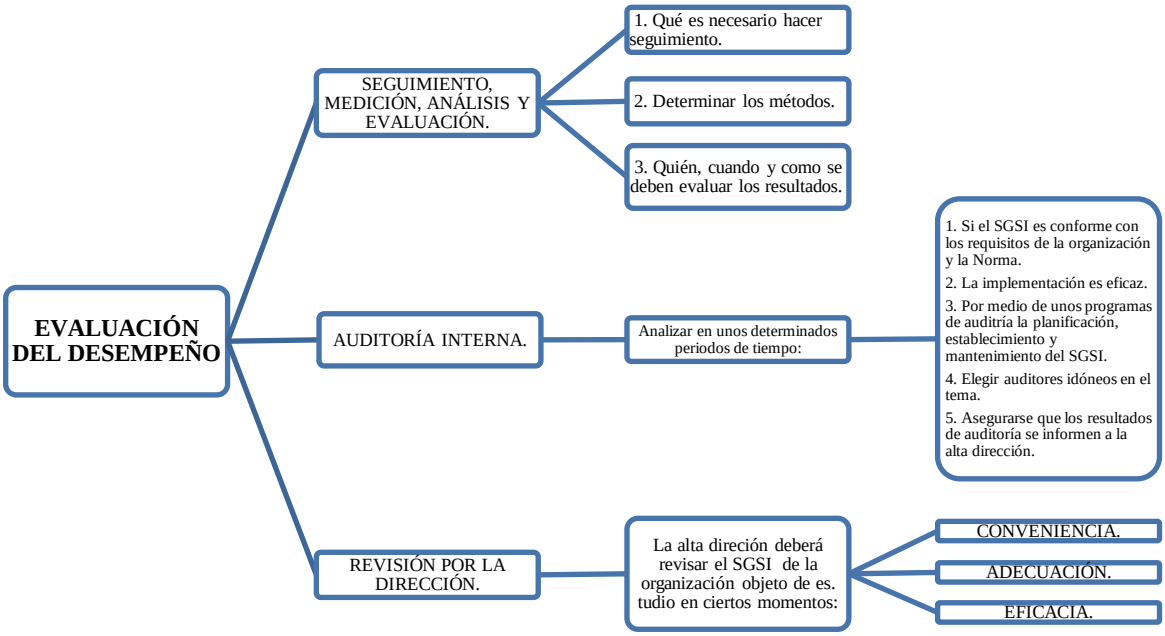



Fuente: Elaboración propia.

La operación, es otro de los elementos fundamentales que dispone la norma, ya que trabaja en conjunto con otros elementos mencionados en los pasos anteriores como el numeral 6.1. (las acciones para tratar los riesgos y las oportunidades), lo cual implica una valoración en determinados periodos de tiempo y el numeral 6.2. (Objetivos de la seguridad de la información y planes para lograrlos). (Instituto Colombiano de Normas Técnicas y Certificación, 2013)

### 7.1.1.6. Evaluación del Desempeño.

*Figura 7: Evaluación Del Desempeño.*

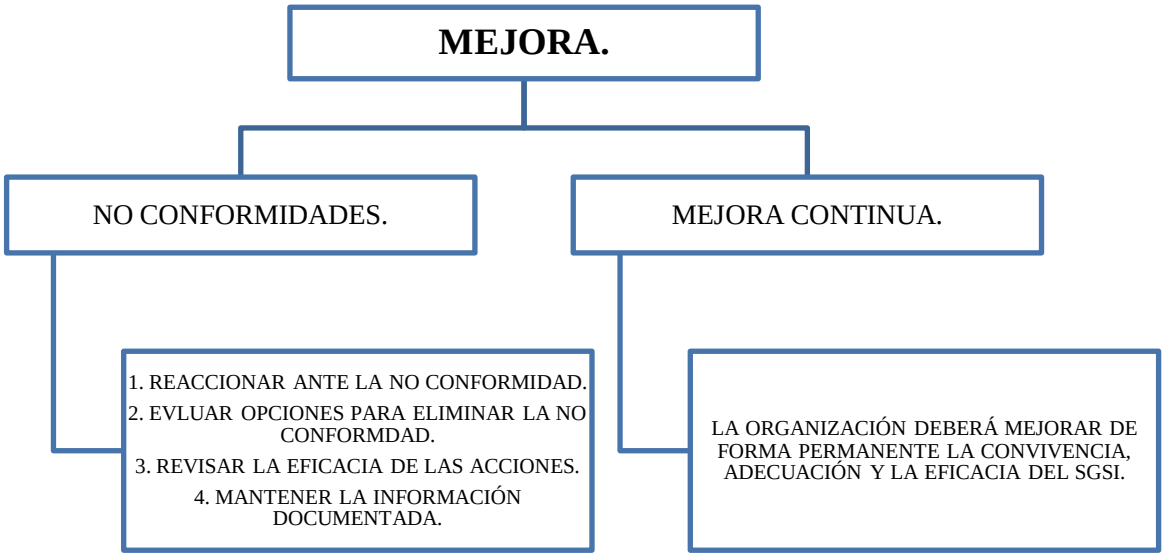



Fuente: Elaboración propia.

Teniendo en cuenta las acciones mencionadas hasta el momento, la etapa que va a continuación es la evaluación del desempeño. Esta etapa realiza un papel muy relevante durante el proceso en la medida que una vez se ha llegado a este punto de la lectura, se procederá a determinar el seguimiento, así como también medir y analizar el desempeño de la seguridad de la información con la ayuda de unos requisitos que establece el numeral 9.1. De la norma. Igualmente, para realizar una correcta evaluación del desempeño del SGSI, es necesario aplicar una auditoría interna en unos intervalos de tiempo determinados previamente, es indispensable precisar que, la auditoría se realizará acorde a las necesidades que tenga la organización y la norma. Por último, la revisión por parte de la alta dirección también es muy necesaria, puesto que se revisará la convivencia, adecuación y la eficacia. (Instituto Colombiano de Normas Técnicas y Certificación, 2013)

### 7.1.1.7. Mejora.

*Figura 8: Mejora.*




Fuente: Elaboración propia.

En última instancia se encuentra la mejora. Etapa que deberá ser implementada teniendo a consideración dos elementos, en primer lugar, las no conformidades y las acciones correctivas, comprometiendo de este modo un análisis primordialmente de las no conformidades, dada la obligación de poner en marcha acciones correctivas y, en segundo lugar, emplear la mejora continua, aspecto característico en las normas de calidad. (Instituto Colombiano de Normas Técnicas y Certificación, 2013)

### 7.1.2. ISO 31000 Versión 2011.

Independientemente del tipo de organización que se esté hablando, se puede decir que en todas inciden aspectos internos o externos los cuales provocan un escenario de total incertidumbre en cuanto al cumplimiento de los objetivos organizacionales. Se puede decir que, comúnmente el efecto generado a raíz de esta incertidumbre en el logro de los objetivos se denomina “riesgo”.

En este orden de ideas, es preciso afirmar que al momento por el cual los miembros de una entidad realizan una cierta acción, ésta será susceptible al riesgo. Para hacer frente a esta problemática los miembros de una organización están en la obligación de tomar cartas en el asunto, por medio de la gestión, análisis, evaluación y posible tratamiento

teniendo a consideración si el riesgo se puede tratar. Gracias a este proceso, los agentes involucrados tendrán que ser comunicados, con el objetivo de verificar los controles aplicados y socializar el tratamiento del riesgo en términos económicos para no gastar más recursos de los que se dispone.

Desafortunadamente, las organizaciones en general no emplean medidas adecuadas para gestionar el riesgo, trayendo como consecuencia errores que pueden empeorar aún más la situación. En esta medida, la Norma ISO 31000 versión 2011 ofrece una serie de principios necesarios para garantizar la eficacia de la gestión del riesgo. Por lo tanto, esta Norma sugiere para todas las organizaciones que decidan desarrollar, implementar y mejorar de manera reiterativa el marco de referencia, el cual tendrá como propósito integrar la gestión del riesgo en todos los procesos inherentes a la organización como pueden ser las políticas, la cultura organizacional, los valores corporativos, etc.

Cabe señalar que, la gestión del riesgo se ha venido desarrollando a lo largo de la historia empresarial y en diferentes sectores desde hace bastante tiempo, principalmente con el objetivo de poner en práctica distintas medidas que permitan garantizar una gestión del riesgo eficaz, coherente y eficiente. La perspectiva que tiene esta norma en cuanto a los temas relacionados con el riesgo, consiste en tratar como primera medida unos principios y directrices para la correcta gestión del riesgo, la cual pueda ser de forma sistemática, transparente y fiable, independientemente del contexto y alcance que se esté hablando. En este sentido y dado que en cada área de la organización implica un tratamiento del riesgo diferente, esta Norma contiene una parte denominada “establecimiento del contexto”, cuya finalidad se fundamenta en el proceso de la gestión del riesgo, se establezca el contexto con el propósito de observar aspectos generales como: los objetivos organizacionales, las partes involucradas, el entorno de la organización, entre otros factores.

Es así que, al momento de poner en marcha la gestión del riesgo, los beneficios que una organización puede obtener son innumerables, como es el caso de incrementar la posibilidad en el alcance de objetivos, incentivar una gestión eficiente, promover un ambiente de concientización al interior de los miembros de la organización en cuanto a su área de trabajo, dar cumplimiento a obligaciones legales, aumentar la credibilidad entre los

miembros involucrados, incrementar los controles, entre otros. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

Por último, esta Norma nombra las partes involucradas que más pueden sacar provecho del contenido sugerido, las cuales son:

- Las partes involucradas en la ejecución de la política de gestión del riesgo al interior del ente económico.
- Los individuos que tengan la responsabilidad de asegurar la eficacia de la gestión al interior del ente económico.
- Las personas que tienen la tarea de evaluar la eficacia de la gestión del riesgo al interior en la organización.
- Entre otro tipo de usuario interesados en la gestión del riesgo en la organización.

*Figura 9: Aspectos Relevantes De La Norma ISO 31000.*


Fuente: Elaboración propia.

**7.1.2.1. Objeto.**

La finalidad que tiene esta Norma reside en brindar una serie de principios e instrucciones para una excelente gestión del riesgo. Es preciso destacar que, esta Norma

está dirigida para cualquier tipo de empresa interesada en el manejo del riesgo y por otra parte, el tiempo de duración puede convertirse en algo infinito. (Instituto Colombiano De

*Tabla 3: Objeto*

Normas Técnicas Y Certificación, 2011)


Fuente: Elaboración propia.

**7.1.2.2. Principios.**

Como se ha venido mencionando, uno de los temas fundamentales que incluye la Norma ISO 31000 versión 2011 es un conjunto de diferentes elementos denominados como principios. Dichos principios están compuestos por 11 elementos, los cuales son los siguientes:

1. La gestión del riesgo crea y genera valor: una de las principales contribuciones que proporciona la gestión del riesgo, está relacionado con el aporte que realiza al interior de las organizaciones para alcanzar objetivos y mejorar aspectos generales. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

2. La gestión del riesgo es una parte integral de todos los procesos de la organización: debido a la gran importancia que tiene la gestión del riesgo en las organizaciones, es obligatorio que sea reconocida como una parte integral de todas las actividades que son ejecutadas a diario, por consiguiente, la alta dirección deberá tenerla en cuenta para todos los procesos. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

3. La gestión del riesgo es parte de la toma de decisiones: al hablar de la toma de decisiones, la gestión del riesgo contribuirá a través de unas sugerencias como elecciones informadas, preferir determinadas acciones y distinguir entre diferentes alternativas. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

4. La gestión del riesgo aborda explícitamente la incertidumbre: a causa de la incertidumbre, la gestión del riesgo trata sus causas y el posible tratamiento que se puede dar en una determinada situación. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

5. La gestión del riesgo es sistemática, estructurada y oportuna: a través de una proyección sistemática, pertinente y ajustada, ayudará a obtener resultados fiables, comparables y sólidos. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

6. La gestión del riesgo se basa en la mejor información disponible: para garantizar el éxito de la gestión del riesgo, es preciso contar con un flujo de información fiable tales como datos históricos, experiencia, opinión de las partes involucradas, evaluación de expertos, entre otros. Es necesario mencionar que, las personas que tienen la responsabilidad de tomar decisiones, tendrán la obligación de estar muy bien informados de la situación y tener muy presente las limitaciones de las fuentes consultadas. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

7. La gestión del riesgo está adaptada: la gestión del riesgo deberá tener concordancia con el ambiente, ya sea externo o interno. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

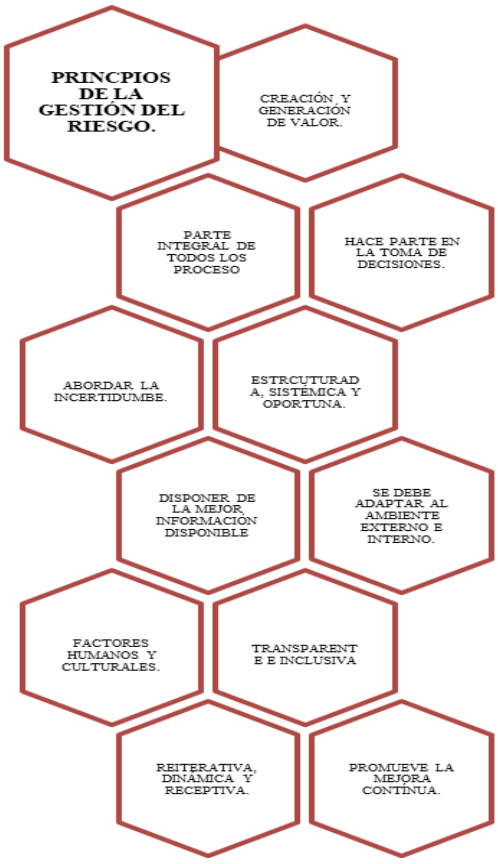
8. La gestión del riesgo toma en consideración los factores humanos y culturales: es necesario reconocer diversas características de los individuos (independientemente si es en el contexto externo o interno), en vista a que pueden beneficiar u obstaculizar el alcance de los objetivos organizacionales. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)
9. La gestión del riesgo es transparente e inclusiva: la participación de las partes involucradas y en especial aquellos que tienen la responsabilidad de tomar

decisiones, con el propósito de asegurar que la gestión del riesgo sea renovada y oportuna. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

**10.** La gestión del riesgo es dinámica, reiterativa y receptiva al cambio: como consecuencia de los cambios que se dan a menudo, la gestión del riesgo debe adaptarse continuamente al cambio así sea interno o externo. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

**11.** La gestión del riesgo facilita la mejora continua de la organización. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

*Figura 10: Principios*




Fuente: Elaboración propia.

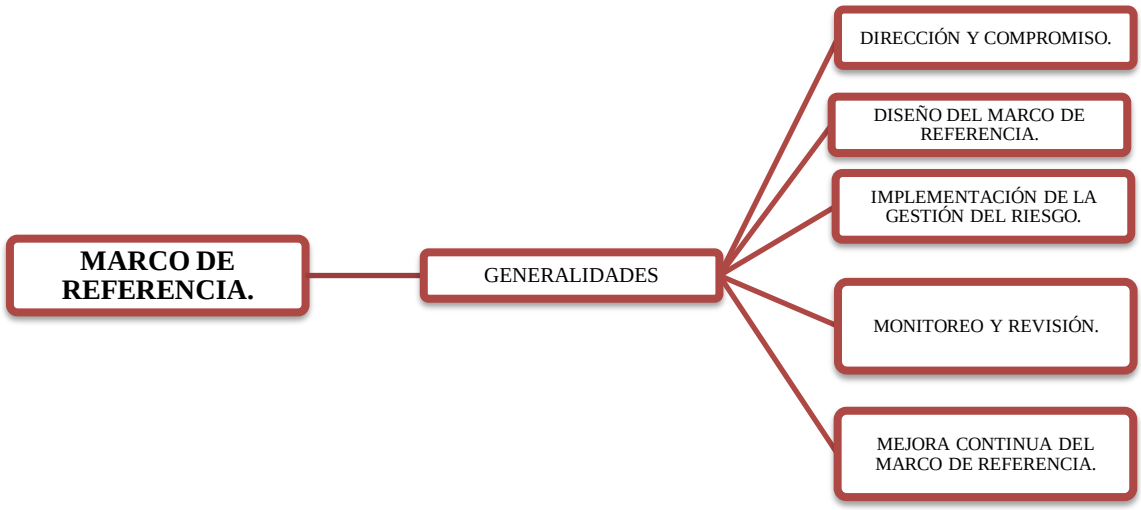
### 7.1.2.3. Marco de referencia.

**7.1.2.3.1 Generalidades:**

El logro de la gestión del riesgo depende de la eficacia del marco de referencia, el cual proporciona las bases y las disposiciones para que se pueda aplicar la gestión del riesgo en todos los rincones de la organización. Además de lo anterior, el marco de referencia suministra información del proceso de la gestión del riesgo, con el propósito que exista un reporte y posteriormente sea tenido en cuenta en la toma de decisiones y la explicación de lo que sucede a nivel general en la organización. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

Por otro lado, el marco no busca dar por terminado el sistema de gestión del riesgo actual, sino que tiene la finalidad de incorporar la gestión del riesgo a nivel general. Como consecuencia de lo anterior, las organizaciones deberán ajustar los ítems en concordancia a sus propias necesidades. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

*Figura 11: Marco de Referencia.*




Fuente: Elaboración propia.

**7.1.2.3.2. Dirección y compromiso:**

Con el propósito de introducir la gestión del riesgo y respaldar el posible éxito al interior de la organización, es necesario que exista una gran iniciativa de parte de la alta

dirección, tal como una buena planificación estratégica con el propósito de llevarlo a todos los rincones considerando un gran número de requisitos que menciona la Norma ISO 31000. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

*Figura 12: Dirección Y Compromiso.*


Fuente: Elaboración propia.

**7.1.2.3.3. Diseño del marco de referencia para la gestión del riesgo:**

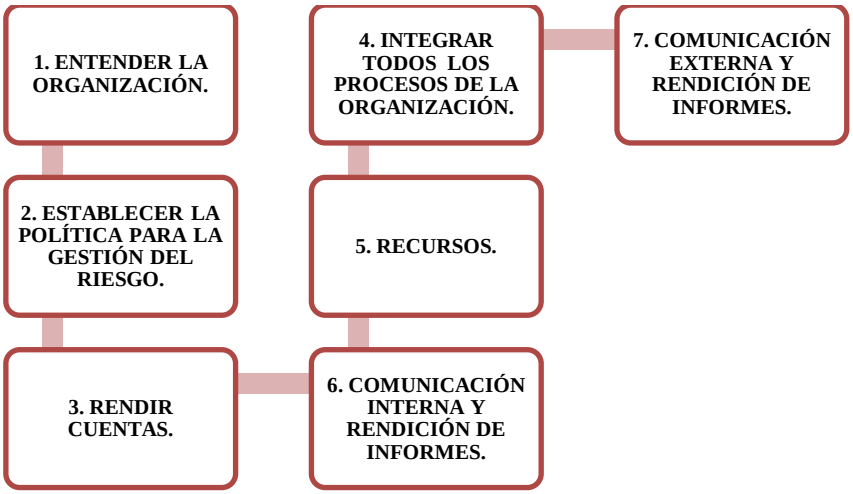
Para comprender el diseño del marco de referencia, es esencial conocer siete puntos los cuales serán explicado a continuación:

- Entender a la organización: previamente a la construcción y aplicación del marco de referencia, es importante entender el ambiente interno y externo de la organización objeto de análisis, debido a la incidencia que puede tener en el marco ya mencionado. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)
- Establecer la política para la gestión: para instaurar la política de la gestión del riesgo, se deberá atender a los objetivos organizacionales y uno requisitos como: el propósito que tiene la organización la gestionar el riesgo, la relación entre los objetivos y las políticas de la organización con la política para la gestión del riesgo, deberes y compromisos para la gestión del riesgo, como se deberán tratar los conflictos de intereses, entre otros. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)
- Rendición de cuentas: esta parte corresponde a todos los temas inherentes a la responsabilidad, autoridad y competencia, adicionalmente de incluir la

implementación y mantenimiento del proceso de la gestión del riesgo. Lo anterior se realizará gracias a: la identificación de los propietarios del riesgo, cómo se deben rendir cuentas para el desarrollo, implementación y el mantenimiento del marco y la manera de medir el desempeño. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

- Integración en los procesos de la organización: Como se ha mencionado en párrafos anteriores, la gestión del riesgo debe ser contemplada de modo general con todas las actividades de la organización, con la finalidad que la gestión del riesgo sea eficaz, oportuna y eficiente. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)
- Recursos: para garantizar el éxito de la gestión del riesgo, la organización deberá distribuir recursos de forma objetiva y de acuerdo a unos aspectos que la Norma recomienda como lo es: asignar los recursos esenciales para cada actividad, analizar muy bien a las personas que van a recibir dichos recursos, tener en cuenta programas de entrenamiento, entre otros. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)
- Establecer mecanismos para la comunicación interna y la presentación de informes: uno de los compromisos que debe asumir la alta dirección de la organización consiste en la comunicación interna, con el objetivo de mantener una rendición de informes, informar acerca del manejo de los recursos y la acción oportuna ante cualquier riesgo. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)
- Establecer mecanismos para la comunicación externa y la presentación de informes: por último, para realizar una correcta comunicación también se deberán tener en cuenta las partes externas involucradas, de acuerdo: los requisitos regales, otorgar una correcta retroalimentación en la comunicación y consultas, etc. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

*Figura 13: Diseño Del Marco De Referencia.*




Fuente: Elaboración propia.

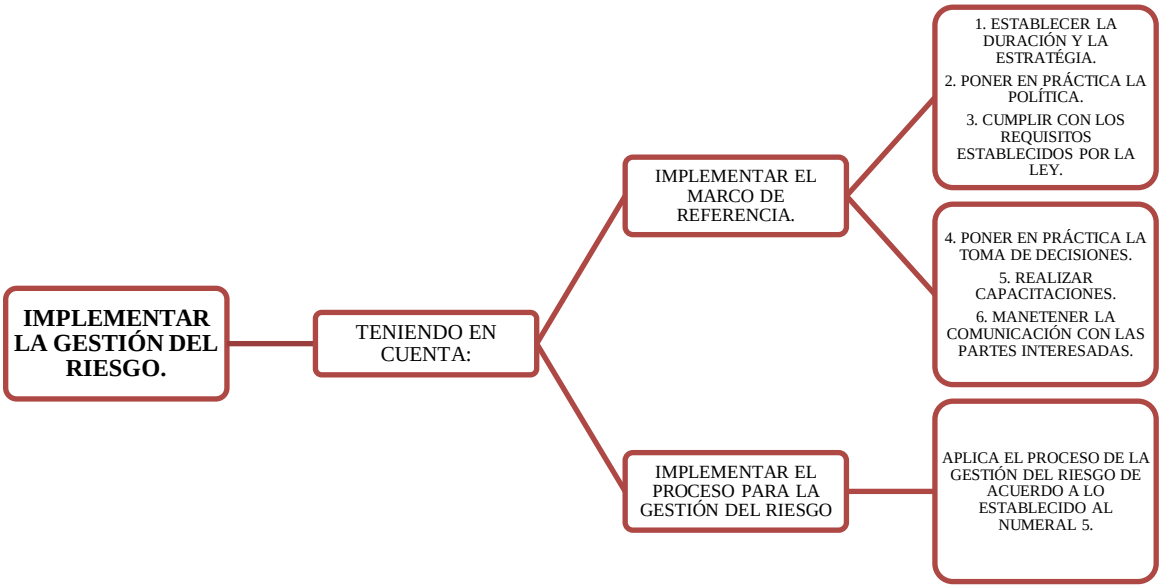
**7.1.2.3.4. Implementar la gestión del riesgo:**

Para aplicar la gestión del riesgo en la organización, se deberá tener en cuenta dos aspectos los cuales son:

- Implementar el marco de referencia: al iniciar la implementación del marco de referencia para la gestión del riesgo, es preciso considerar: la duración y organización para implementar el marco de referencia, asociar los procesos de la organización con la política de la gestión del riesgo, obedecer las obligaciones legales y normativas, ejecutar reuniones de información y entrenamiento, entre otros. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

- Implementar el proceso para la gestión del riesgo: se deberá aplicar el proceso de la gestión del riesgo conforme a lo descrito en el numeral 5. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

*Figura 15: Implementar la Gestión del Riesgo.*



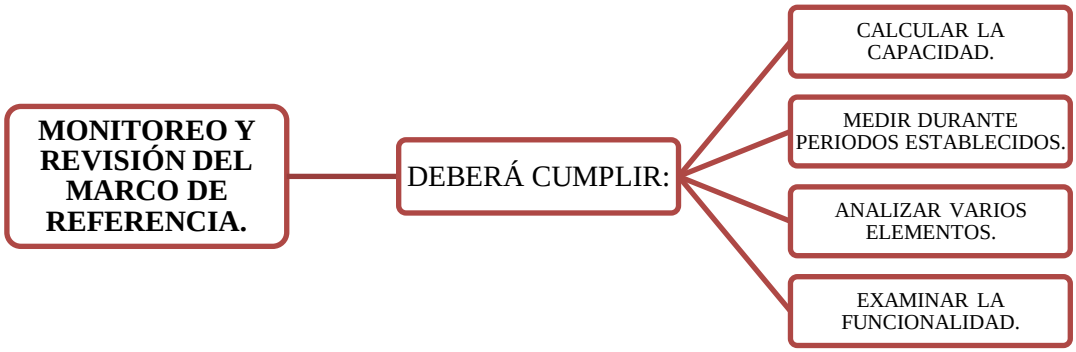

Fuente: Elaboración propia.

**7.1.2.3.5. Monitoreo y revisión del marco de referencia:**

Con el objetivo de garantizar la eficacia y la eficiencia de la gestión del riesgo, se deberán tener en cuenta los aspectos que serán mencionados a continuación:

- Calcular la capacidad de la gestión del riesgo teniendo en cuenta indicadores que tendrán que ser revisados constantemente. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)
- Medir durante periodos establecidos el avance teniendo en cuenta el plan para la gestión del riesgo y el rumbo que tome. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)
- Analizar si el marco de referencia, la política y el plan para la gestión del riesgo son pertinentes para las necesidades que tenga la organización. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)
- Examinar la funcionalidad del marco de referencia para la gestión del riesgo. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

*Figura 16: Monitoreo Y Revisión Del Marco De Referencia.*




Fuente: Elaboración propia.

**7.1.2.3.6. Mejora continua del marco de referencia:**

De acuerdo a los resultados alcanzados hasta el momento en el marco de referencia, es indispensable tomar acciones que permitan mejorarlo al igual que la política y el plan para la gestión del riesgo. Es primordial que estas actuaciones mejoren la gestión del riesgo en la organización. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

*Figura 17: Mejora Continua.*


Fuente: Elaboración propia.

**7.1.2.4 Proceso**

**7.1.2.4.1. Generalidades:**

La fase del proceso de la gestión del riesgo tiene la responsabilidad:

- Hacer parte de la gestión.
- Pertenecer a la cultura y las actividades.
- Estar ajustado a los procesos de la actividad económica de la organización. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

*Figura 18: Generalidades.*


Fuente: Elaboración propia.

**7.1.2.4.2. Comunicación y consulta:**

Para que exista un buen entendimiento, la comunicación entre las partes que tienen algún tipo de injerencia en el contexto interno o externo deberá tener lugar en cada fase del proceso.

Teniendo a consideración la importancia de la comunicación y la consulta, es primordial que se establezcan inicialmente planes para aplicar estos dos conceptos. El contenido de dichos planes tratará temas inherentes al riesgo como puede ser la naturaleza, las consecuencias y las acciones para tratarlos. Es preciso que, las partes que tengan la responsabilidad en la implementación, comprendan los motivos por los cuales se tomarán ciertas disposiciones. Por último, la comunicación con las partes involucradas aportará diferentes ideas según el punto de vista que tenga cada uno, arrojando resultados positivos en la toma de decisiones, ya que se contará con la experiencia y la opinión de individuos muy conectados con la organización, por lo que es necesario reconocer, apuntar y tener en cuenta dichos aportes. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

*Figura 20: Comunicación y Consulta.*


Fuente: Elaboración propia.

**7.1.2.4.3. Establecimiento del contexto:**

**7.1.2.4.3.1. Generalidades:**

Para establecer el contexto, es necesario integrar varios elementos como los objetivos, diseñar unos parámetros que se basen en aspectos externos e internos los cuales se tendrán en cuenta al tener que gestionar el riesgo y definir el alcance. Cabe mencionar que, aunque los parámetros que componen el establecimiento del contexto son muy similares a los nombrados en el marco de referencia, para este caso deberán llevarse a cabo de una forma más detallada, en especial con la relación que tendrán en el alcance del proceso para la gestión del riesgo. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

**7.1.2.4.3.2. Establecer el contexto externo:**

Conocer el ambiente externo es fundamental para estar más seguros que las partes involucradas (en este caso del contexto externo), serán partícipes en la formulación de los criterios del riesgo. Lo anterior se da, como consecuencia de lo imprescindible que es tomar en cuenta lo largo y ancho de la organización, lo cual incluye a profundidad las leyes vigentes y la opinión de las partes involucradas del ambiente externo. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

Por consiguiente, el contexto externo deberá incluir:

- Temas relacionados con el medio ambiente, la cultura, legal, financiero tecnológico, entre otros. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)
- Los impulsores que desempeñan un papel relevante en los objetivos de la organización. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)
- El tipo de relación que tienen las partes involucradas del ambiente externo y el punto de vista. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

**7.1.2.4.3.3. Establecer el contexto interno:**

Al hablar del contexto interno, se refiere a todos los componentes de la organización que pueden incidir en la manera en que se gestionara el riesgo. En este caso, es necesario nombrar aspectos como la cultura, las actividades, la infraestructura y las estrategias, los cuales serán tenidos en cuenta. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

Es necesario establecer el contexto por las siguientes razones:

- Porque la gestión del riesgo deberá tener muy presente el contexto de los objetivos organizacionales. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)
- Elementos como los objetivos y los criterios de una determinada actividad, se deberían tener a consideración de acuerdo a los objetivos organizacionales. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

También al hablar del ambiente interno, se deberá contar con: la estructura organizacional, funciones y deberes, políticas, objetivos y las estrategias para lograrlos, la capacidad que se tendrá en términos de recursos, cultura organizacional, entre otros. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

**7.1.2.4.3.4. Establecer el contexto del proceso para la gestión del riesgo:**

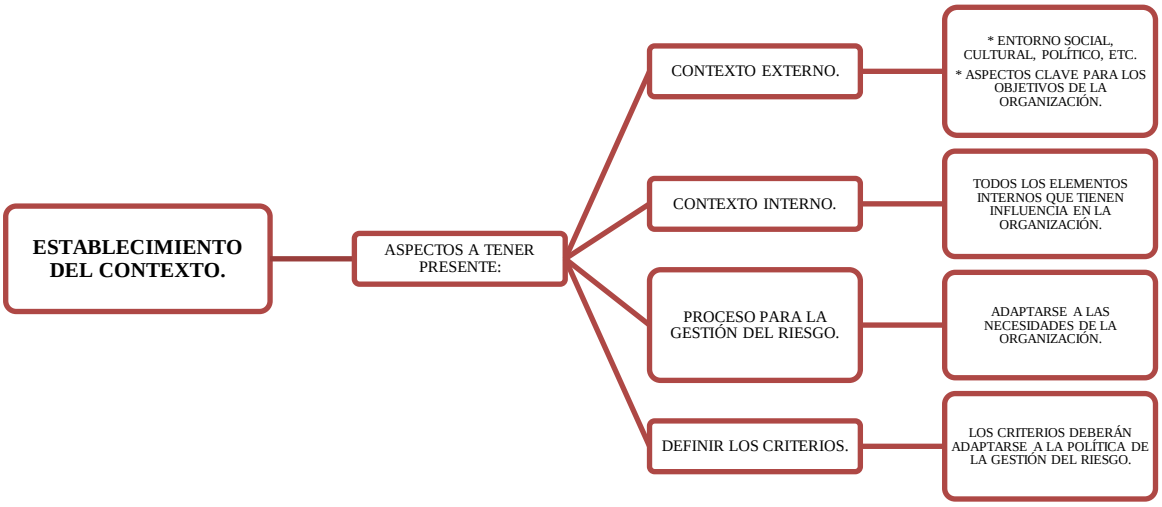
Es recomendable fijar los objetivos, estrategias, alcance y criterios de las labores que se ejecutarán en la organización o en el lugar donde tendrá lugar su aplicación. La

gestión del riesgo se deberá emplear tomando como referencia los recursos que serán empleados para poner en funcionamiento dicho proceso, al igual que los deberes y los registros que se deberán mantener. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

**7.1.2.4.3.5. Definir los criterios del riesgo:**

Uno de los aspectos claves que deberá definir la organización son los criterios, los cuales tendrán la finalidad de evaluar la relevancia que tendrán los riesgos. Para llevar a cabo lo anterior, es imprescindible evidenciar los valores, objetivos y los recursos con los que cuenta la organización. Además, ciertos criterios deberán incluir requisitos legales si así lo ordena la ley y dichos criterios tendrán que estar muy ligados a la política para la gestión del riesgo que se mencionan en el numeral 4.3.2. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

*Figura 21: Establecimiento del Contexto.*




Fuente: Elaboración propia.

**7.1.2.4.5. Valoración del riesgo**

**7.1.2.4.5.1. Generalidades:**

La parte de la valoración del riesgo, es considerada como el procedimiento general del reconocimiento del riesgo, examen del riesgo y la valuación del riesgo. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

**7.1.2.4.5.2. Identificación del riesgo:**

Para ejecutar adecuadamente la identificación del riesgo, en primera instancia se deberá conocer la naturaleza, los sectores involucrados, las causas y los posibles efectos que se podrían derivar por no tomar las medidas adecuadas. El principal objetivo que tiene la identificación del riesgo, es la realización de un registro muy completo considerando alterar el alcance de los objetivos.

Igualmente, es necesario agregar toda clase de riesgos, sin importar que la procedencia esté bajo control de la organización o su origen no sea evidente. Así mismo, es imprescindible que independiente del origen que tenga el riesgo, se incluyan los posibles escenarios que podrían provocar la no atención del riesgo.

Por último, la organización deberá implementar las herramientas y procedimientos que se ajusten a las necesidades que se presentan, los recursos que disponen, siempre y cuando cumpla con hacer frente a las amenazas. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

**7.1.2.4.5.3. Análisis del riesgo:**

El análisis del riesgo, significar ejecutar y entender el respectivo riesgo a tratar, el cual complementara posteriormente la evaluación del riesgo y las posibles medidas de si es necesario o no tratar los riesgos y las estrategias más apropiadas para llevar a cabo el tratamiento. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

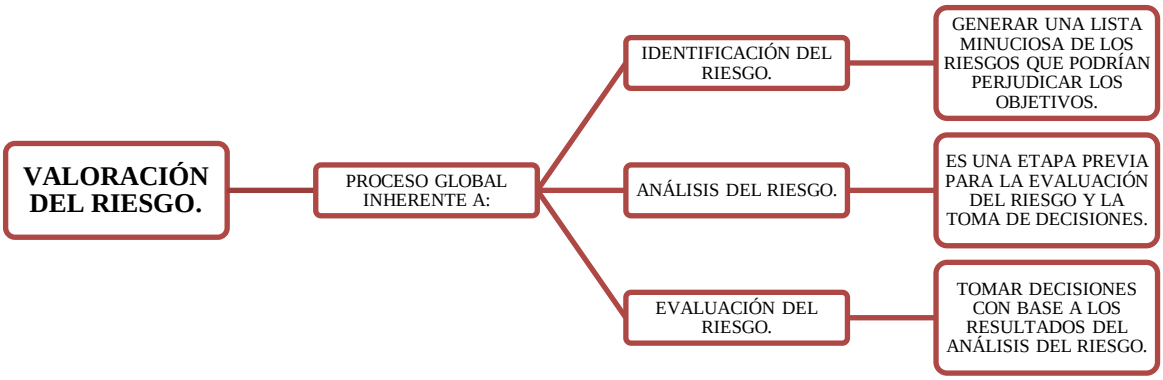
En el desarrollo del análisis del riesgo, se debe considerar el origen del riesgo, los resultados favorables o desfavorables y la posibilidad que dichos eventos se lleguen a presentar. Es preciso señalar que, una determinada situación puede generar varios resultados y en esa medida perjudicar los objetivos de distintas maneras. Del mismo modo, es primordial observar los controles que ya estén presente y la eficiencia y eficacia que han

tenido hasta el momento. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

### 7.1.2.4.5.4. Evaluación del riesgo:

La finalidad que tiene la evaluación del riesgo, consiste en posibilitar una mejora en la toma de decisiones, teniendo en cuenta los resultados del análisis, en referencia a los riesgos que implican un tratamiento y la preferencia que tendrán algunos dado el grado se urgencia. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

*Figura 22: Valoración del Riesgo.*




Fuente: Elaboración propia.

### 7.1.2.4.6. Tratamiento del Riesgo.

### 7.1.2.4.6.1. Generalidades:

El tratamiento del riesgo, implica tener que elegir entre una o varias opciones las cuales permitan corregir el riesgo y posteriormente poner en marcha la implementación. Durante esta etapa, es necesario aplicar un proceso cíclico que tenga en cuenta las siguientes opciones: contemplar la opción que algunos riesgos sean aceptables y en el dado caso que no sea así tomar las medidas más eficaces para el tratamiento. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

**7.1.2.4.6.2. Selección de las opciones para el tratamiento del riesgo:**

Al momento de elegir las opciones para el tratamiento del riesgo, es fundamental observar las alternativas que estén disponibles para tratar los riesgos, manteniendo un equilibrio entre los recursos que dispone y el empeño que se deberá tener frente a la implementación. Así mismo, es muy acertado contemplar la idea de tratar algunos riesgos de manera individual o en conjunto si es el caso, de acuerdo a la eficiencia que tenga el tratamiento. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

Durante el proceso, al contemplar las distintas alternativas para tratar el riesgo se deberá tomar en consideración la opinión de las partes involucradas y los canales de comunicación para mantener contacto con ellos. En el caso que la opción para tratar el riesgo tenga algún tipo de incidencia en otras áreas de la organización, las partes involucradas de las demás áreas deberán hacer parte en la toma de decisiones. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

Es importante mencionar, los efectos negativos que puede generar una opción de tratamiento, los cuales serán contemplados como una falla o la ineficacia de las acciones para tratar el riesgo. Por lo tanto, la vigilancia constante debe ser considerada como una parte en conjunto de este proceso, con la finalidad de garantizar que las acciones sean eficientes. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

**7.1.2.4.6.3. Preparación e implementación de los planes para el tratamiento del riesgo:**

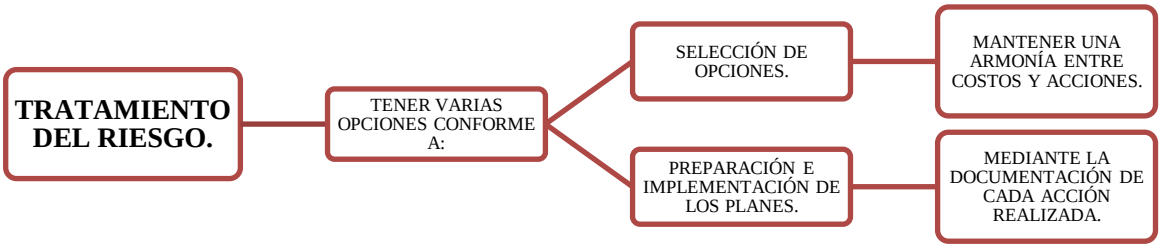
Uno los objetivos que tienen los planes para el tratamiento del riesgo consiste en mantener documentada la forma como se van a ejecutar las acciones para el tratamiento de los riesgos que fueron seleccionados. La información documentada deberá contener:

- Los motivos por los cuales se eligió una opción para el tratamiento del riesgo y las mejoras que se esperan. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

- Las personas que fueron responsables de admitir el plan y de igual manera los responsables de ponerlo en marcha. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)
- Las opciones sugeridas para tratar el riesgo. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)
- Entre otros. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

Así mismo, los programas para el tratamiento deberán englobar todos los procesos de gestión que tiene la organización y la opinión de los individuos involucrados. Las personas que tienen la responsabilidad de tomar decisiones y las demás partes que tienen algún tipo de incidencia, obligatoriamente deben estar informados del origen y las consecuencias del riesgo residual. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

*Figura 23: Tratamiento del Riesgo.*




Fuente: Elaboración propia.

**7.1.2.4.7. Monitoreo y revisión.**

El monitoreo y la revisión deberán ser tenidos en cuenta en el proceso de la gestión del riesgo, vinculando una comprobación y examen constantes los cuales pueden ser en periodos planificados o cuando sea necesario. Las actividades de monitoreo y revisión que se llevarán a cabo en la organización, contemplarán los procesos en general de la gestión

del riesgo con el objetivo de obtener múltiples beneficios como la garantía de controles eficaces y eficientes, el suministro de información se complementara para optimizar la valoración del riesgo, identificar alteraciones en el contexto externo e interno que puedan obligar a cambiar un determinado elemento del tratamiento del riesgo, entre otros. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

El progreso de la aplicación de los planes para tratar los riesgos, proveerá un suministro que mida el desempeño. Los resultados obtenidos podrán ser incluidos en las actividades generales de gestión del desempeño, medición e informe interno y externo de la organización. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

*Figura 24: Monitoreo y Revisión.*


Fuente: Elaboración propia.

**7.1.2.4.8. Registro del proceso para la gestión del riesgo.**

Las acciones realizadas por parte de la gestión del riesgo, tendrán un seguimiento de principio a fin, con el propósito de perfeccionar los fundamentos bajos los cuales se harán los registros y los instrumentos empleados en el proceso global. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

Al momento de realizar los registros, es esencial considerar los siguientes puntos:

- La necesidad que tendrá la organización para fomentar el estudio continuo.
- Las ventajas de usar la información recopilada en la gestión.
- Los recursos económicos y el empeño realizado en el diseño y sostenimiento de los registros.

- Observar las obligaciones legales, reglamentarios y funcionales para el tema de los registros.
- Las acciones que se deberán llevar a cabo para el acceso, recuperación y medios en los cuales se va almacenar la información.
- Lo susceptible que puede ser cierta información. (Instituto Colombiano De Normas Técnicas Y Certificación, 2011)

*Figura 25: Registro del Proceso.*


Fuente: Elaboración propia.

### 7.1.3. Magerit.

Es una metodología para el análisis y la gestión del riesgo que ha sido creada por el consejo superior de administración electrónica, como consecuencia del aumento en los sistemas de información en las empresas y por la importancia que tienen estos en el alcance de los objetivos organizacionales (Ministerio De Haciendas Y Administraciones Públicas De España, 2012). Cabe mencionar que, MAGERIT desde su inicio (1998) cuenta con tres actualizaciones, la última fue llevada a cabo en el año 2012 y tuvo como propósito alcanzar los siguientes objetivos:

- Generar conciencia en las organizaciones de los riesgos existentes y la obligación de realizar una gestión efectiva.
- Sugerir un método sistemático que permita analizar los riesgos originados por el manejo de las tecnologías de la información y las comunicaciones.
- Realizar una planificación oportuna para el tratamiento de los riesgos.

- Planificar procesos relacionados con la evaluación, auditoría, certificación, teniendo a consideración el caso. (Ministerio De Haciendas Y Administraciones Públicas De España, 2012)

Es preciso enfatizar la importancia que realiza MAGERIT a los temas concernientes al análisis de riesgos y el tratamiento de riesgos, estableciendo así una serie de pasos o acciones a desarrollar para dar cumplimiento al objetivo de mantener el sistema de seguridad de la información lo más estable posible (Ministerio De Haciendas Y Administraciones Públicas De España, 2012). Tal es el caso que en el capítulo 3, el cual nombra una serie de pasos que se encuentran constituidos de la siguiente manera:

### 7.1.3.1. Paso 1.

*Figura 26: Paso número 1 metodología MAGERIT.*

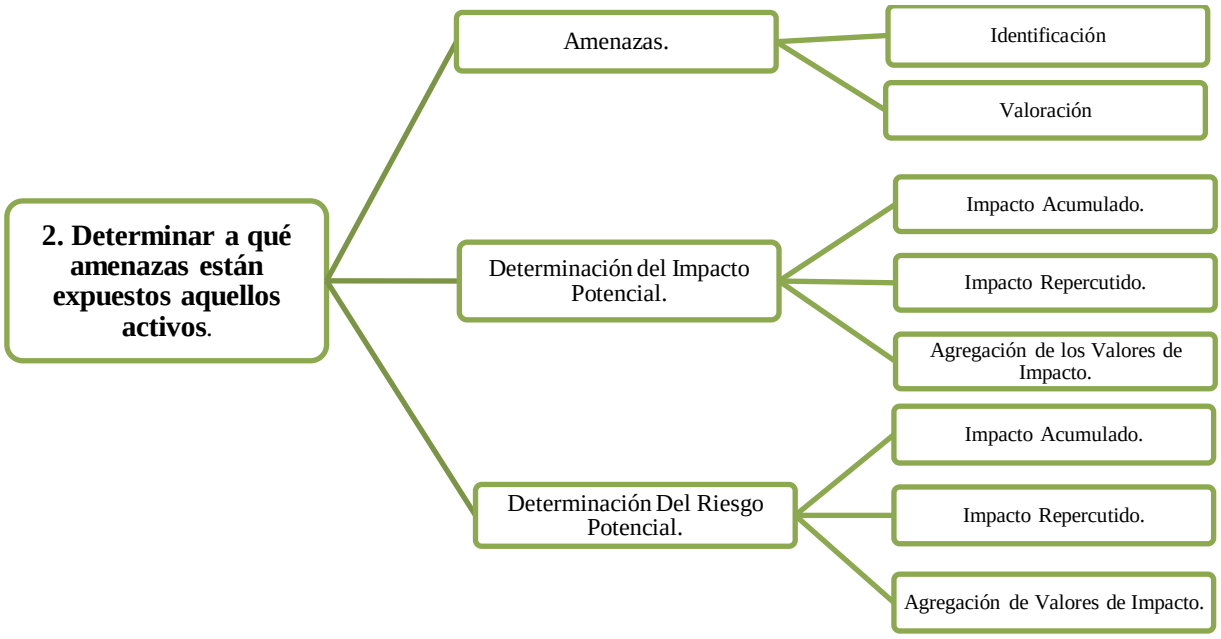

Fuente: Elaboración propia.

De esta forma, queda evidenciado en el paso uno todo el proceso que se debe ejecutar para dar cumplimiento a diferentes procesos, teniendo como gran factor de importancia la información que se maneja y los servicios que presta, adicionalmente, se

tiene a consideración una serie de características fundamentales para analizar los activos de acuerdo a la metodología que propone MAGERIT. (Ministerio De Haciendas Y Administraciones Públicas De España, 2012)

**7.1.3.2. Paso 2.**

*Figura 27: Paso 2 metodología MAGERIT.*

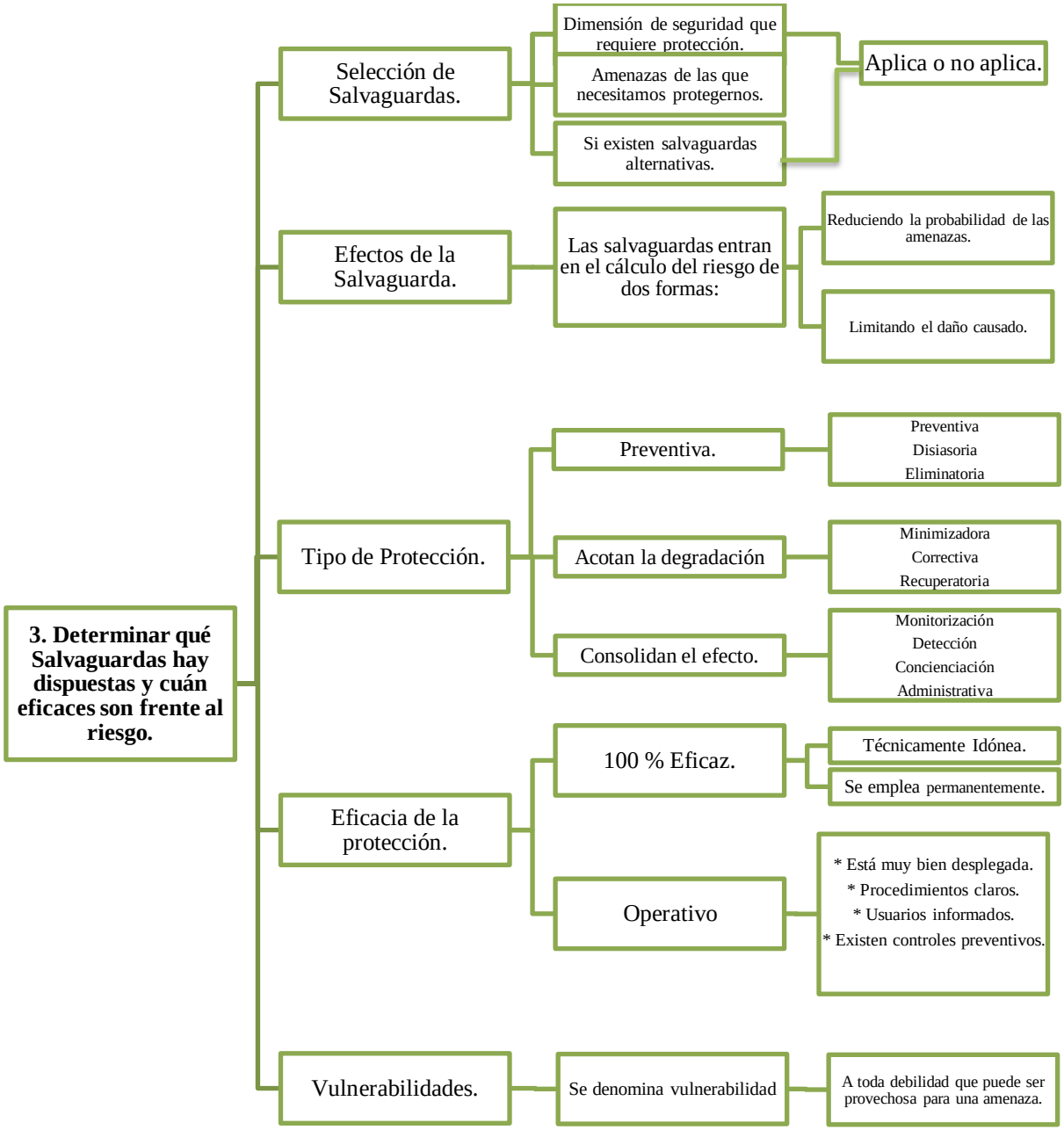



Fuente: Elaboración propia.

En el paso número dos, el cual trata la determinación de las amenazas a las que están expuestos los activos, se presentan como elementos fundamentales la explicación de lo que significa una amenaza en un Sistema De Seguridad De La Información, teniendo a consideración como se identifica y la forma como se debe valorar. Por otra parte, se trata la determinación del impacto potencial, elemento que explica de qué trata el impacto acumulado, impacto repercutido y agregación de los valores de impacto. Por último, está la determinación del riesgo potencial, elemento que trata los mismos temas que en la parte de la determinación del impacto potencial, pero esta vez enfocado en el riesgo. (Ministerio De Haciendas Y Administraciones Públicas De España, 2012)

*Figura 28: Paso número 3 metodología MAGERIT.*

### 7.1.3.2. Paso 3.



Fuente: Elaboración propia.

En el paso número 3, se desarrollan una serie de acciones encaminadas a reducir el riesgo llamadas en la metodología de MAGERIT como “salvaguardas”, las cuales caracterizan a esta etapa por tener a consideración cinco aspectos que ayudarán claramente en el proceso del análisis del riesgo, por intermedio de acciones. (Ministerio De Haciendas Y Administraciones Públicas De España, 2012)

En primer lugar, es necesario que de acuerdo a las opciones que brinda MAGERIT por medio de sus respectivas guías, se identifique la salvaguarda que mejor se ajusta al tipo de riesgo a tratar, acto seguido se procede a analizar los efectos que produjo la anterior acción para llegar a la conclusión de limitar el daño causado o reducir la probabilidad de la amenaza. (Ministerio De Haciendas Y Administraciones Públicas De España, 2012)

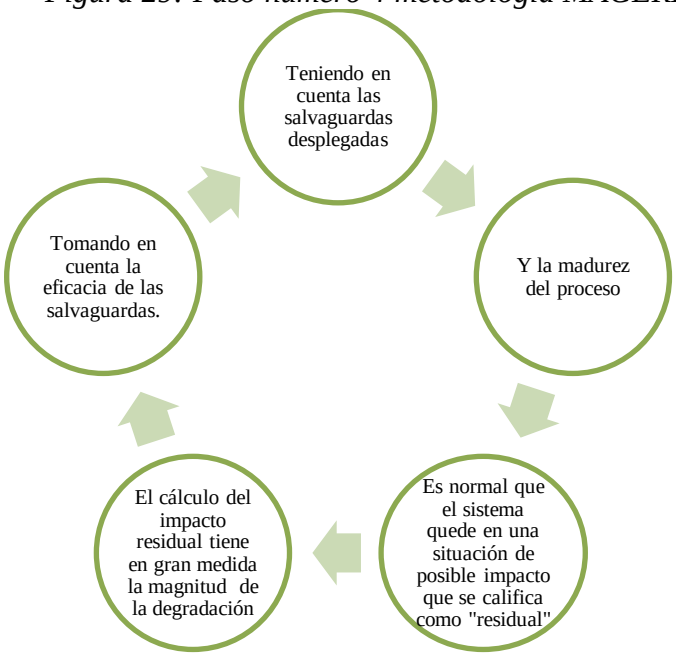
Posteriormente, se sugiere aplicar uno de los tres tipos de protección que aconseja MAGERIT, tomando a consideración más adelante la eficacia de la protección.

Por último, se dispone a examinar vulnerabilidades que tiene el sistema con el objetivo de observar muy detalladamente que no existan más fallas que podrían ser aprovechadas por las amenazas. (Ministerio De Haciendas Y Administraciones Públicas De España, 2012)

#### 7.1.3.4. Paso 4

El paso 4, consiste en determinar la situación en la que se encuentra el sistema una vez se tuvieron en cuenta las salvaguardas, esta parte del proceso se denomina impacto residual. Para realizar el cálculo del impacto residual, se toma únicamente la magnitud de la degradación, en vista que los activos no han cambiado y de igual manera sus posibles dependencias. Es propicio destacar que, la magnitud de la degradación hacer referencia a la eficacia de las salvaguardas (proporción de restar eficacia perfecta de la eficacia real). (Ministerio De Haciendas Y Administraciones Públicas De España, 2012)

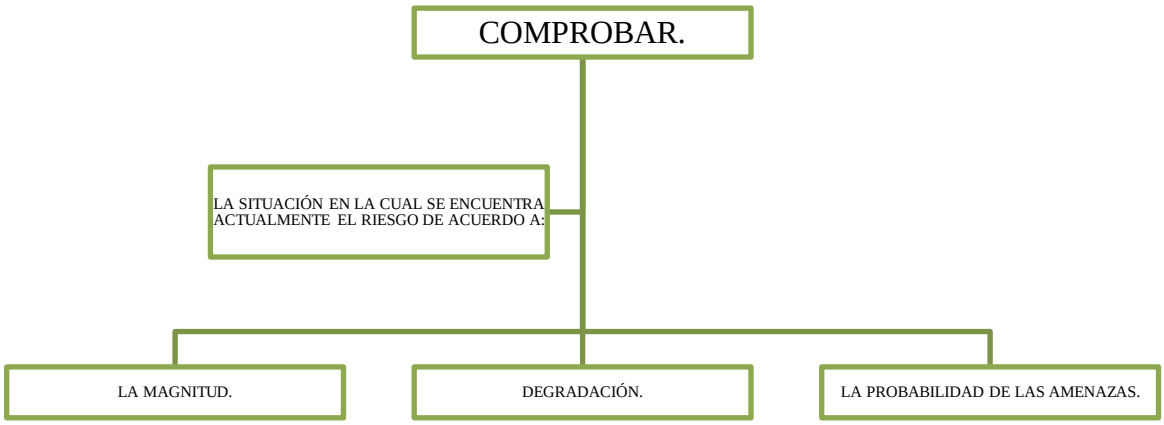
*Figura 29: Paso número 4 metodología MAGERIT.*




Fuente: Elaboración propia.

**7.1.3.5. Paso 5.**

*Figura 30: Paso número 5 comprobar - Magerit*




Fuente: Elaboración propia.

Al igual que el paso anterior, en esta etapa lo que se hace es analizar la situación del sistema principalmente con la ejecución de algunos cálculos, con la finalidad de obtener

el riesgo residual. De igual manera, para realizar la valoración no se tienen en cuenta los activos ni las posibles dependencias, pero sí la magnitud de degradación y la probabilidad de amenazas. En este caso es de gran ayuda el paso 4, debido a que se tiene en cuenta el resultado de la magnitud de la de gradación y en el otro factor a hallar. (Ministerio De Haciendas Y Administraciones Públicas De España, 2012)

## 7.2. Capítulo 2: Contextualización y análisis diferencial de la situación actual del Cuerpo de Bomberos Voluntarios de Tunja

A continuación, se hará una descripción de los aspectos generales del Cuerpo De Bomberos Voluntarios De Tunja, con la finalidad de conocer la historia, la actividad que realiza, el organigrama y el análisis diferencial el cual ayudará a comprender el estado actual de la entidad con respecto a la seguridad de la información.

### 7.2.1. Descripción De La Empresa.

La empresa que fue elegida para realizar la Implantación De Una Guía De La Norma ISO 27001 Versión 2013 es el Cuerpo De Bomberos Voluntarios de la ciudad de Tunja, una empresa sin ánimo de lucro dedicada a la Gestión Integral del Riesgo contra incendio, preparativos y atención de rescates e incidentes en todas sus modalidades. Esta organización fue fundada en el año 1966 por Luis Alberto Pedreros Montañez, Jorge Enrique Valderrama Jiménez y Guido Samuel Malagón Bravo, un grupo de personas con espíritu altruista y gran vocación para ayudar a la comunidad, los cuales desde el inicio tuvieron que afrontar muchos retos debido a que no contaban con los recursos, infraestructura, personal, entre otros elementos claves que fueron superados como consecuencia de la perseverancia de sus fundadores.

En la actualidad, esta entidad cumple con todos los requisitos legales que exige la ley bomberos y ha logrado constituirse como una entidad fundamental para el bienestar de la ciudad de Tunja, tanto así que en la actualidad cuenta con tres sedes destacando su sede central en la Calle 22 No 6-22, Sub Estación Nor Oriental Z-2 y La Estación Z3 se encuentra ubicada muy cerca al Sector de los Hongos, en la Avenida Oriental No. 1-136

### 7.2.2. Actividad.

En Colombia, “las instituciones organizadas para la prevención, atención y control de incendios, los preparativos y atención de rescates en todas sus modalidades inherentes a su actividad y la atención de incidentes con materiales peligrosos, se denominan Cuerpos de Bomberos”.

El Cuerpo de Bomberos Voluntarios de Tunja fue fundado el 23 de agosto de 1966, con la finalidad de brindar un "servicio público esencial", lo cual consiste en salvaguardar, los bienes y los recursos naturales de la sociedad Tunjana. En la actualidad es una entidad cívica, sin ánimo de lucro, de utilidad común, no gubernamental, de carácter privado, con autonomía administrativa y financiera, integrada por personas naturales.

El Cuerpo de Bomberos Voluntarios de Tunja como lo demás cuerpos de bomberos del país se rige por la ley General de Bomberos de Colombia 1575 de 2012, la Constitución Política de Colombia, el reglamento disciplinario contenido en el Decreto 953 de 1997, el reglamento general administrativo, operativo y técnico de los Bomberos de Colombia, los estatutos, reglamentos internos de la institución y demás normas concordantes.

### 7.2.3. Oferta De Productos Y Servicios.

El Cuerpo de Bomberos Voluntarios de Tunja presta los siguientes servicios:

- Gestión Integral del Riesgo contra incendio.
- Preparativos y atención de rescates en todas sus modalidades.
- Atención de incidentes en todas sus modalidades.
- Formación y capacitación en atención de siniestros.
- Recarga de Extintores y venta de elementos de seguridad.

En la siguiente tabla, se mostrarán algunas fotos relacionadas con todas las labores que realiza el Cuerpo De Bomberos Voluntarios De Tunja.

*Tabla 4: Servicios Prestados Por El Cuerpo De Bomberos Voluntarios De Tunja.*

| SERVICIO | REGISTRO FOTOGRÁFICO |
|---|---|
| | |

| | |
|---|---|
| **Atención de incendios** |     |
| **Atención y control de inundaciones** |   |
| **Rescate sub acuático** |  |
| **Manejo de abejas** |  |

| | |
|---|---|
| **Atención Prehospitalaria** |  |
| **Rescate en todas sus modalidades** |  |
| **Control de fugas de gas** |  |
| **Búsqueda y localización con bomberos caninos** | |

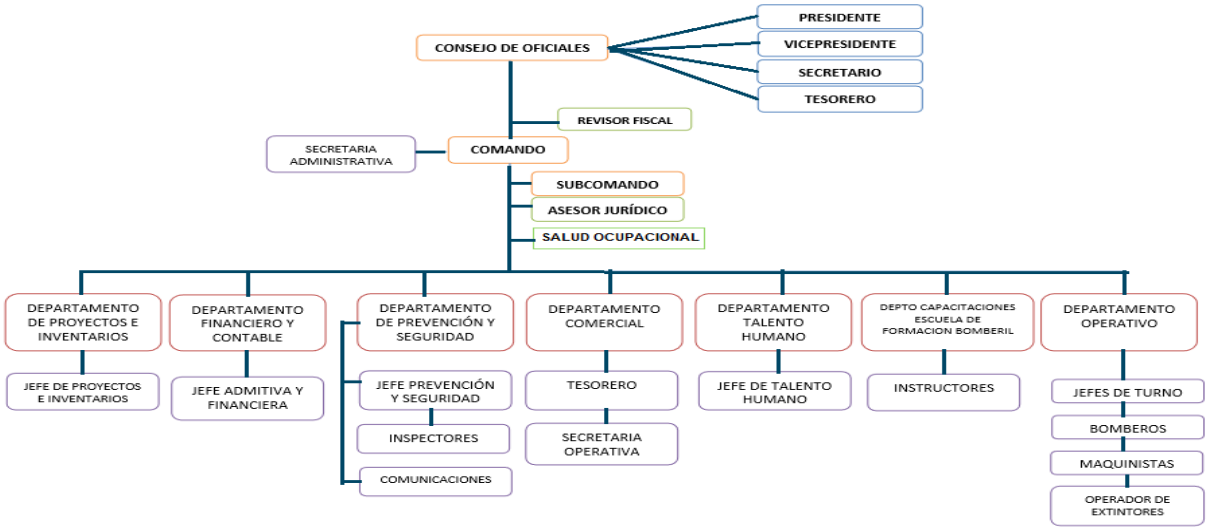
| | |
|---|---|
| |  |
| **Extricación vehicular** |  |
| **Capacitaciones** |   |
| **Rescate Vertical** |  |
| **Recarga de Extintores y venta** | |

| | |
|---|---|
| **de elementos de seguridad** |  |

Fuente: Elaboración propia.

### 7.2.4. Estructura organizacional.

*Ilustración 5: Organigrama Cuerpo De Bomberos Voluntarios De Tunja.*




Fuente: Cuerpo De Bomberos Voluntarios De Tunja.

### 7.2.5. Análisis diferencial del estado actual.

De acuerdo a los lineamientos establecidos por la norma ISO 27001 versión 2013, el presente trabajo está dirigido a analizar todas los controles y exigencias que la Norma determina como esenciales, para lo cual se tendrá en cuenta inicialmente el numeral 4 (contexto de la organización) hasta el numeral 10 (mejora continua), debido a que son los numerales de obligatorio cumplimiento que exige la Norma ISO 27001 versión 2013.

Posteriormente, se examinará el contenido del Anexo A el cual inicia desde el numeral 5 (políticas de la seguridad de la información) hasta el numeral 18 (cumplimiento). Lo anterior se llevará a cabo teniendo a consideración las medidas de seguridad y las normas asociadas a la seguridad de la información que la entidad tiene.

Gracias al análisis se podrá tener una mejor idea del estado actual de la entidad en temas inherentes a la seguridad de la información y será de gran ayuda para conocer los aspectos positivos o negativos en relación a la norma ISO 27001 versión 2013.

Conforme a lo anterior, se registrará el siguiente formato teniendo en cuenta los siguientes criterios:

**0= No se está ejecutando.**

**1= Está parcialmente ejecutado.**

**2= Está prácticamente ejecutado en su totalidad.**

**3= Su ejecución es total.**

*Tabla 5: Análisis Diferencial Del Estado Actual.*

| SECCIÓN | # | DESCRIPCIÓN | HALLAZGO POSITIVO | HALLAZGOS NEGATIVOS | VALOR |
|---|---|---|---|---|---|
| 4. Contexto de la organización. | | 4.1. Conocimiento de la organización. 4.2 Entendiéndolas necesidades y expectativas de las partes interesadas. 4.3. Determinando el alcance del SGSI. 4.4. Administración del sistema de gestión de seguridad de la información | | A modo general, se pudo evidenciar que en este ítem existe poco trabajo realizado por la entidad, al momento de tratar temas como: conocimiento de la organización, entender las necesidades y expectativa de las partes interesadas, y determinación del SGSI. | 0 |
| 5. Liderazgo. | | 5.1. Liderazgo y compromiso. 5.2. Política. 5.3. Roles de la organización, responsabilidad y autoridad. | | En cuanto al liderazgo, la entidad solo sobresalió en un aspecto (política) el cual es un eje fundamental del SGSI, pero con el gran punto negativo de no aplicarla en su totalidad. | 0 |
| 6. Planificación | | 6.1. Acciones para dirigir los riesgos y oportunidades. 6.2. Objetivos y planes para lograrlo. | | Existe muy poco material relacionado con el desarrollo de este ítem, el cual es fundamental para el SGSI. | 0 |
| 7. Soporte | | 7.1. Recursos. 7.2. Competencia. 7.3. Sensibilización. 7.4. Comunicación. 7.5. Información documentada. | | La parte de soporte aborda diferentes elementos, en los cuales no se logró una puntuación tan buena, aunque es uno de los pocos ítems que más sobresale. | 1 |
| 8. Operación. | | 8.1. Planificación y control operativo. 8.2. Evaluación riesgos seguridad de la información. 8.3. Tratamiento riesgos de seguridad de la información | | Ninguno de los ítems de este punto inherentes a la operación se encuentran aplicados. | 0 |

| | | | | | |
|---|---|---|---|---|---|
| 9. Evaluación del desempeño. | | 9.1. Seguimiento, medición, análisis y evaluación. 9.2. Auditoría interna. 9.3. Revisión de la dirección. | | Debido a la poca aplicabilidad en temas inherentes a la seguridad de la información. | 0 |
| 10. Mejoras. | | 10.1. No conformidades y acciones correctivas. 10.2. Mejora continua. | | Teniendo en cuenta las pocas acciones dirigidas a proteger la información, no se puede hablar de mejora continua y por lo tanto el valor es de cero. | 0 |
| 5. Políticas de la Seguridad de la Información | | 5. 1. Orientación de la dirección para la gestión de la seguridad de la información. 5.1.1. Políticas para la seguridad de la información. 5.1.2. Revisión de las políticas de seguridad de la información | | Uno de los puntos favorables para este ítem se da porque existe una política de seguridad de la información y aun así no ha sido implementada o socializada a los miembros de la organización. | 0 |
| 6. Organización de la Información | | 6.1. Organización interna. 6.1.1. Funciones de seguridad de la Información y las responsabilidades 6.1.2. Separación de deberes. 6.1.3. Contacto con las autoridades 6.1.4. Contacto con los grupos de interés especial 6.1.5. Seguridad de la información en la gestión de proyectos. 6.2. Dispositivos móviles y tele trabajo. 6.2.1. Política para dispositivos móviles. 6.2.2. Teletrabajo. | | Debido a la nula aplicabilidad de la política de SGSI, no se encuentran funciones definidas directamente vinculada con la seguridad de la información. | 0 |
| 7. Seguridad de los recursos humanos. | | 7.1. Antes de asumir el empleo. 7.1.1. Selección. 7.1.2. Términos y condiciones del empleo. 7.2. Durante la ejecución del empleo. 7.2.1. Responsabilidades de la dirección. 7.2.2. Toma de conciencia, educación y formación de la seguridad de la información. 7.2.3. Procesos disciplinario. 7.3. Terminación y cambio de empleo. 7.3.1. Terminación o cambio de responsabilidades de empleo. | | En el trabajo de contrato individual se establecen clausulas como la de confidencialidad, pero hace falta el debido establecimiento y fortalecimiento de controles antes y durante el proceso de contratación para verificar la idoneidad, competencia y nivel de confiabilidad en el personal que ingresa a la organización esto teniendo en cuenta que son elementos que contribuyen a fortalecer la seguridad de la información. | 1 |
| 8. Gestión de activos. | | 8.1.1. Inventario de activos. 8.1.2. Propiedad de los activos 8.1.3. Uso aceptable de los activos. 8.1.4. Devolución de activos. 8.2. Clasificación de la información. 8.2.1. Clasificación de la información. 8.2.2. Etiquetado de la información. 8.2.3. Manejo de activos. 8.3. Manejo de medios .8.3.1. Gestión de medios removibles. 8.3.2. Disposición de los medios. 8.3.3. Transferencia de los medios físicos. | | Al dar inicio a esta investigación la empresa se encontraba trabajando en establecer el inventario de activos, pues debido a la rotación del personal que tiene a cargo esta función no se ha podido empalmar y consolidar debidamente la información correspondiente a este aspecto. | 0,4285714 |
| 9. Control de acceso | | 9.1. Requisitos del negocio para control de acceso. 9.1.1. Política de control de acceso. 9.1.2. Accesos a redes y servicios de red. 9.2. Gestión de acceso a usuarios. 9.2.1. Registro y cancelación del registro de usuarios. 9.2.2. Suministro de acceso de usuarios. 9.2.3. Gestión de derechos de acceso privilegiado. 9.2.4. Gestión de información de autenticación secreta de usuarios. 9.2.5. Revisión de los derechos de acceso de usuarios. 9.3. Responsabilidades de los usuarios. 9.3.1. Uso de información de autenticación secreta. | | La entidad tiene controles muy débiles para restringir el acceso a los sistemas de información, por esta razón el nivel de vulnerabilidad es alto, también se evidencio un ataque a la seguridad de la información del que fue objeto esta organización en el último año. | 0,4615385 |

| | | | | | |
|---|---|---|---|---|---|
| | | 9.4. Control de acceso a sistemas y aplicaciones. 9.4.1. Restricciones de acceso a la información.<br>9.4.2. Procedimiento de ingreso seguro.<br>9.4.3. Sistema de gestión de contraseñas.<br>9.4.4. Uso de programas utilitarios privilegiados.<br>9.4.5. Control de acceso a códigos fuente de programas. | | | |
| 10. Criptografía. | | 10.1. Controles criptográficos. 10.1.1. Políticas sobre el uso de controles criptográficos. 10.1.2. Gestión de llaves. | | No halló una política relacionada con los controles criptográficos y se desconoce qué hacer en el caso que sean necesarios. | 0 |
| 11. Seguridad física y del entorno. | | 11.1. Áreas seguras.<br>11.1.1. Perímetro de seguridad física.<br>11.1.2. Controles de acceso físicos.<br>11.1.3. Seguridad de oficinas, recintos e instalaciones.<br>11.1.4. Protección contra amenazas externas y ambientales.<br>11.1.5. Trabajo en áreas seguras.<br>11.1.6. Áreas de despacho y carga.<br>11.2. Equipos.<br>11.2.1. Ubicación y protección de los equipos.<br>11.2.2. Servicios de suministro.<br>11.2.3. Seguridad del cableado.<br>11.2.4. Mantenimiento de equipos.<br>11.2.5. Retiro de activos.<br>11.2.6. Seguridad de equipos y activos fuera de las instalaciones.<br>11.2.7. Disposición segura.<br>11.2.8 Equipos de usuario desatendido.<br>11.2.9. Política de escritorio limpio y pantalla limpia. | | No se evidencio un control de acceso enfocado a resguardar datos confidenciales, tampoco para restringir el acceso a la información e identificar un responsable de las zonas que contienen información confidencial. Posterior al ataque a la seguridad de la información los equipos del cuarto de control fueron reubicados y se encuentran monitoreados por una cámara de vigilancia, adicionalmente no se encontró un registro que demuestre la periodicidad en la que se revisan el estado lógico y físico de los equipos, tampoco se halló un registro de ingreso o salida de equipos de la entidad. En la política, no se menciona algo referente a equipos desatendidos. | 0 |
| 12. Seguridad de las operaciones. | | 12.1. Procedimientos operacionales y responsabilidades. 12.1.1. Procedimientos de operación documentados. 12.1.2. Gestión de cambios. 12.1.3. Gestión de capacidad.<br>12.1.4. Separación de los ambientales de desarrollo, pruebas y operación.<br>12.2. Protección contra códigos maliciosos. 12.2.1. Controles contra códigos maliciosos.<br>12.3. Copias de respaldo. 12.3.1. Respaldo de la información.<br>12.4. Registro y seguimiento. 12.4.1. Registro de eventos. 12.4.2. Protección de la información de registro.<br>12.4.3. Registros del administrador y del operador. 12.4.4. Sincronización de relojes.<br>12.5. Control de software en sistemas operativos.<br>12.5.1. Instalación de software en sistemas operativos.<br>12.6. Gestión de la vulnerabilidad técnica.<br>12.6.1. Gestión de las vulnerabilidades técnicas. 12.6.2. Restricciones sobre instalación de software.<br>12.7. Consideraciones sobre auditorias de sistemas de información. | | Existen procesos inherentes a la seguridad de la información, pero su aplicabilidad es muy baja, debido a que en la entidad no se ha socializado la política de seguridad de la información. No se tiene establecido la capacidad de operación del sistema, el seguimiento recae en tres terceros.No se tiene un registro de los ataques que han ocurrido en los computadores de la entidad, así como tampoco la manera que los solucionaron.No se realizan simulacros para actuar ante la pérdida de información y el sistema se satura con frecuencia. No se encontró un registro que haga seguimiento a las actividades del administrador u operador.No se evidencia un control de los programas o las actualizaciones de software requeridas.No existen documentos acerca de las vulnerabilidades que está sometido el sistema de información y de esta manera tomar las medidas necesarias para resguardarlo.No se evidencia un control de los programas o las actualizaciones de software requeridas.No se ha realizado actividades de auditoría que permitan verificar el estado del sistema de información. | 0 |

| | | | | | |
|---|---|---|---|---|---|
| 13. Seguridad de las comunicaciones. | | 13.1. Gestión de la seguridad de las redes. 13.1.1 Controles de redes. 13.1.2. Seguridad de los servicios de red. 13.1.3. Separación en las redes. 13.2. Transferencia de información. 13.2.1. Políticas y procedimientos de transferencia de información. 13.2.2. Acuerdos sobre transferencia de información. 13.2.3. Mensajería electrónica. 13.2.4. Acuerdos de confidencialidad o de no divulgación. | | Los controles de redes se encuentran en actualización,no se evidencio un documento que comprenda todos los mecanismos que utilizan los ingenieros a cargo para mantener los servicios de red activos.No existe una separación de las redes, no existe ningún tipo de acuerdo con las partes externas que mantienen relación con la entidad. No existe algún tipo de acciones relacionadas con la protección de la información que es enviada a través de mensajería electrónica.En la entidad no existen acuerdos de confidencialidad o de no divulgación dirigido a parte del personal y agentes del ambiente externo. | 0 |
| 14. Adquisición, desarrollo y mantenimiento 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. 14.1.2. Seguridad de servicios de las aplicaciones en redes públicas. 14.1.3. Protección de transacciones de los servicios de aplicaciones. 14.2. Seguridad en los procesos de desarrollo y de soporte. 14.2.1. Política de desarrollo seguro. 14.2.2. Procedimientos de control de cambios en sistemas. 14.2.3. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación. 14.2.4. Restricciones en los cambios a los paquetes de software. 14.2.5. Principios de Construcción de los sistemas seguros. 14.2.6. Ambiente de desarrollo seguro. 14.2.7. Desarrollo contratado externamente. 14.2.8. Pruebas de seguridad de sistemas. 14.2.9. Pruebas de aceptación de sistemas. 14.3. Datos de prueba. 14.3.1. Protección de datos de prueba. | | Los requisitos que establece la política no han sido implementados una vez se creó y tampoco ha sido actualizada conforme con las necesidades que tiene la organización.No se encontraron documentos o reglas que permitan verificar el desarrollo seguro al interior de la organización.No hay un documento que permita entender los requerimientos mínimos que necesitan los programas que son utilizados a diario. No existe un documento que contenga una serie de principios enfocados en garantizar la construcción de sistemas seguros y por lo tanto su aplicación es nula. No se cuenta con unos parámetros que propicien el desarrollo seguro en acciones de integración y avances en desarrollo de sistemas.No existe documento o acta que ayude a comprobar el cumplimiento de ciertos criterios que son realizados mediante pruebas de aceptación de sistemas. No existe registro que permita constatar la forma como se han tratado los datos de prueba. | 0,153846154 |
| 15. Relaciones 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 los proveedores. 15.1.2. Tratamiento de la seguridad dentro de los acuerdos con los proveedores. 15.1.3 Cadena de suministro de tecnología de información y comunicación. 15.2. Gestión de la prestación de servicios de proveedores. 15.2.1. Seguimiento y revisión de los servicios de los proveedores. 15.2.2. Gestión de cambios en los servicios de los proveedores. | | En el contenido de la política de la información, no existen pautas para tratar con los proveedores. En los contratos que se hacen con los proveedores, no se evidencia algún tipo de estipulación que contribuya a garantizar medidas para proteger la información. No existe ningún tipo de acuerdo que se haga con los proveedores. Los servicios ofrecidos por los proveedores, no han sido auditados para establecer la calidad y deficiencias que presenta. En ningún documento se evidencia un control de los servicios prestados por los proveedores. | 0 |

| | | | | | |
|---|---|---|---|---|---|
| 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. Responsabilidades y procedimientos.16.1.2. Reporte de eventos de seguridad de la información.16.1.3. Reporte de debilidades de la información.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos.16.1.5. Respuesta de incidentes de seguridad de la información.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información.16.1.7. Recolección de evidencia. | | No se encontró un documento o acta que oriente a cada miembro de la organización con respecto al rol y las tareas que tiene para fortalecer la seguridad de la información.No se comprobó que la entidad tenga implementado, una serie de procedimientos que ayuden a comunicar los eventos relacionados con la seguridad de la información.No se tiene un proceso claro y conciso que oriente a los empleados a utilizar canales que permitan informar acerca de las debilidades que presenta el sistema de información.No existe una clasificación que guíe a los empleados a reconocer si un evento es un incidente que podría ocasionar un daño terrible al sistema o no. No existen procesos documentados que ayuden a solucionar algún percance en el sistema de seguridad de la información.No se encontró un registro que contribuya a fortalecer el sistema de seguridad de la información, a través de sucesos ocurridos en el pasado. No existen procedimientos que permitan documentar y soportar la información recolectada. | 0 |
| 17. Aspectos de seguridad de la información de la gestión de continuidad del negocio. | | 17.1. Continuidad de seguridad de la información.<br>17.1.1. Planificación de la continuidad de la seguridad de la información.<br>17.1.2. Implementación de la continuidad de la seguridad de la información.<br>17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información.<br>17.2. Redundancias.<br>17.2. Redundancias.<br>17.2.1. Disponibilidad de instalaciones de procesamiento de información. | | La entidad no tiene planes y procesos que den continuidad a la gestión de la seguridad de la información ante situaciones críticas. No existen lineamientos que establezcan la disponibilidad y accesibilidad que debe tener la información. | 0 |
| 18. Cumplimiento. | | 18.1.1. Cumplimiento de requisitos legales y contractuales.<br>18.1.2. Derechos de propiedad intelectual.<br>18.1.3. Protección de registros. 18.1.4. Privacidad y protección de información de datos personales.<br>18.1.5. Reglamentación de controles.<br>18.2. Revisiones de seguridad de la información.<br>18.2.1. Revisión independiente de la seguridad de la información.<br>18.2.2. Cumplimiento con las políticas y normas de seguridad.<br>18.2.3. Revisión del cumplimiento técnico. | | No se halló ningún documento que explique procedimientos o medidas a aplicar en situaciones de derecho de propiedad intelectual. La entidad no tiene registro o documento alguno que explique una serie de acciones para garantizar la protección de registros.A pesar que los miembros de la entidad mantienen la información en zonas seguras, no se ha hecho ningún tipo de categorización.No se examina la información de forma periódica, a pesar que la entidad cuenta con bases suficientes (como es la política de seguridad de la información) La entidad cuenta con un documento el cual contiene las políticas de seguridad de la información, no obstante, no se ha aplicado. Caso similar sucede con las normas de seguridad de la información, debido a que en el ambiente de la organización se desconoce su contenido. | 0 |

Fuente: Elaboración propia.

**Análisis.**

De acuerdo a los datos analizados, la entidad consiguió muy pocos puntos a favor en cuanto a los requerimientos que exige la Norma ISO 27001 versión 2013, debido a que en el examen elaborado no sobresalió un número significativo de ítems por tener una buena puntuación y, por el contrario, es más notorio el poco trabajo efectuado en beneficio de la seguridad de la información. Al respecto, se puede observar que la principal característica a destacar en este primer examen es el hallazgo de la política de seguridad de la información, en vista a que está debidamente elaborada y contiene los elementos suficientes para brindar medidas preventivas. No obstante, una de las principales causas para haber obtenido en general resultados tan desfavorables radica en que la política fue formulada hace mucho tiempo y hasta el momento ningún aspecto se ha implementado. De igual forma, las áreas que obtuvieron un resultado superior a 0 fue: soporte, seguridad de los recursos humanos, gestión de activos, control de acceso y Adquisición, desarrollo y mantenimiento de sistemas. Cabe señalar que, aunque estos ítems destacaron en relación con los demás elementos evaluados, la situación no es tan positiva en vista a que algunos en el promedio de todos los datos que lo conforman no logran superar a 1.

**Nota:** Para ver los valores de manera más detallada, es preciso revisar anexo: Tabla Análisis diferencial del Cuerpo de Bomberos Voluntarios de Tunja. xlsx

## 7.3. Capítulo 3: Plan de tratamiento de riesgos y amenazas asociados al Sistema de Gestión de Seguridad de la Información del Cuerpo de Bomberos Voluntarios de Tunja.

Por último, se llevará a cabo el análisis de los riesgos y amenazas que actualmente existen en los activos de la información del Cuerpo De Bomberos Voluntarios De Tunja, el cual constará de una recopilación que parte desde el inventario de activos de la información hasta el plan de tratamiento de las amenazas más significativas.

### 7.3.1. Inventario de Activos.

Los activos de la información son considerados como un elemento de gran importancia para las organizaciones, por lo tanto, es necesario establecer bajo qué nivel de seguridad se encuentran y de esta manera poder evitar las consecuencias que podrían ocurrir a causa la vulnerabilidad del activo. Como resultado de lo anterior, se requiere un método para dimensionar las acciones correctivas a ejecutar.

"Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de los activos de información más importantes de la organización" (Instituto Colombiano de Normas Técnicas y Certificación, 2013). A continuación, se encuentra el listado de activos de la información del Cuerpo de Bomberos Voluntarios de Tunja, con base en el cual se podrá realizar una clasificación teniendo en cuenta criterios que permitan identificar su nivel de autenticidad, criticidad, integridad, disponibilidad y trazabilidad.

A continuación, se elaborará el inventario de los activos de la información del Cuerpo de Bomberos Voluntarios de Tunja, de acuerdo al ámbito que pertenecen.

*Tabla 6: Inventario activos.*

| AMBITO | ACTIVO |
|---|---|
| INSTALACIONES | Estaciones<br>Repetidoras<br>Centro de procesamiento de datos principal<br>Sala eléctrica, ups, telecomunicaciones y radio comunicaciones |
| HARDWARE | Servidores<br>Equipos escritorio, portátiles<br>Equipos de comunicaciones<br>Equipos de radio comunicaciones y GPS<br>Equipos de seguridad perimetral (Cámaras)<br>Equipos de grabación<br>Planta telefónica |
| SOFWARE BASE | Windows 7, 8 y 10<br>Windows server 2012 |
| APLICACIONES | Bases de datos: SQL server 2014<br>Aplicativo contable: LGX versiones 10 y 11<br>Correo electrónico: Hotmail, Yahoo y Gmail<br>Antivirus: Trend Micro<br>Ofimática: Office 365<br>Webserver: IIS |

| | |
|---|---|
| | Monitoreo: Stencil<br>Posicionamiento: Google maps<br>Comunicaciones: MotoTRB |
| DATOS | Bases de datos corporativas: Contables, clientes, inspecciones, inventarios, emergencias |
| RED | Backups de contabilidad<br>Red de datos<br>Red de telefonía IP<br>Red de radio comunicaciones<br>Acceso a Internet |
| SERVICIOS | Internet<br>Intranet<br>Telefonía<br>Radios |
| EQUIPOS ADICIONALES | Sistema de alimentación UPS<br>Radios portátiles, móviles, base, repetidoras y antenas |
| PERSONAL | Operativos (Bomberos)<br>Administrativos<br>Soporte (Externos) |
| SOPORTES INFORMACIÓN | Archivo físico impreso<br>Discos duros de servidores y estaciones de trabajo<br>Discos externos información de Backups<br>Unidades de CD, DVD y Memorias extraíbles<br>Almacenamiento en internet (Nube) |

Fuente: Elaboración propia.

### 7.3.2. Valoración de los Activos.

Al identificar los activos de la información y clasificarlos de acuerdo a su clase, se determinará el grado de importancia y también se presumirá el daño que puede causar si se llega a encontrar afectado el nivel de disponibilidad, confidencialidad e integridad.

Conforme a lo anterior, se establece una tabla para la valoración de los activos y de esta forma se relacionará con la tabla anterior que contiene los activos de la información. Es necesario destacar que, la clasificación para la valoración de los activos queda definida con los siguientes parámetros: muy alto, alto, medio, bajo, muy bajo. Cabe mencionar que se definieron abreviaciones para cada una.

*Tabla 7: Clasificación Para La Valoración De Los Activos.*

| Categoría | Abreviatura | Valor |
|---|---|---|
| Muy Alto | MA | > 20.000.000 |
| Alto | A | < 20.000.000<br>> 10.000.000 |
| Medio | M | > 10.000.000<br>< 5.000.000 |
| Bajo | B | > 5.000.000<br>< 2.000.000 |
| Muy Bajo | MB | > 2.000.000<br>< 200.000 |

Fuente: Elaboración propia a partir del Libro I de Magerit.

### 7.3.3. Nivel de capacidad en la Seguridad de los activos.

El nivel de capacidad en la Seguridad de los activos de la información, es fundamental para establecer el grado de afectación que puede ser sometido un activo de la información como consecuencia del nivel de vulnerabilidad que se encuentre. De este modo, inicialmente se realizará una tabla denominada "Valoración del Panorama de Seguridad de los Activos", la cual agrupa las dimensiones de seguridad establecidas por la metodología para el análisis del riesgo "Magerit" como es la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad y que también se denomina de forma más resumida como "ACIDT" y de igual manera, contemplara una escala con valores de 0 a 10, teniendo muy presente los criterios asignados en la tabla "Nivel de afectación" con el fin de valorar la posible afectación de cada activo.

Cabe señalar que, algunos ítems serán valorados de forma individual o general en la parte de las "categorías", teniendo en cuenta que cumplen o no con todos los elementos planteados. De igual manera, los activos serán revisados de acuerdo a los criterios establecidos, el valor monetario, la importancia que tiene la información para el ente económico y en efecto a lo anterior se les asignaran un determinado valor

*Tabla 8: Nivel De Afectación.*

| Valor | Criterio |
|---|---|

| | |
|---|---|
| 10 | Afectación muy grave para la organización |
| 9 – 7 | Afectación grave para la organización |
| 6 – 4 | Afectación importante para la organización |
| 3 – 1 | Afectación menor para la organización |
| 0 | Irrelevante para la organización |

Fuente: Elaboración propia a partir del libro I de Magerit.

*Tabla 9: Valoración del Panorama de Seguridad de los Activos.*

| **VALORACIÓN PANORAMA DE SEGURIDAD DE LOS ACTIVOS** | | | | | | | |
|---|---|---|---|---|---|---|---|
| **AMBITO** | **ACTIVO** | **CATEGORIA** | **A** | **C** | **I** | **D** | **T** |
| INSTALACIONES | Estaciones | ALTO | | | | 9 | |
| | Repetidoras | MUY ALTO | | | | 7 | |
| | Centro de procesamiento de datos principal | MUY ALTO | | | | 10 | |
| | UPS, Telecomunicaciones, Sala Eléctrica | MUY ALTO | | | | 10 | |
| HARDWARE | Servidores | MUY ALTO | 6 | 10 | 8 | 9 | 10 |
| | Equipos escritorio, portátiles | MUY ALTO | 6 | 9 | 9 | 10 | 10 |
| | Equipos de comunicaciones | MUY ALTO | 8 | 10 | 7 | 9 | 7 |
| | Equipos de radio comunicaciones y GPS | MUY ALTO | 8 | 10 | 7 | 9 | 7 |
| | Equipos de seguridad perimetral (Cámaras) | MUY ALTO | 9 | 10 | 9 | 9 | 8 |
| | Equipos de grabación | MUY ALTO | 9 | 10 | 9 | 9 | 8 |
| | Planta telefónica | ALTO | 7 | 6 | 8 | 10 | 10 |
| SOFWARE BASE | Windows 7, 8 y 10 | MUY ALTO | 7 | 7 | 8 | 6 | 6 |
| | Windows server 2012 | MUY ALTO | 9 | 9 | 9 | 10 | 8 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| APLICACIONES | Bases de datos: SQL server 2014 | MUY ALTO | 10 | 10 | 10 | 10 | 10 |
| | Aplicativo contable: LGX versiones 10 y 11 | MUY ALTO | 10 | 8 | 9 | 9 | 9 |
| | Correo electrónico: Hotmail, Yahoo y Gmail | ALTO | 10 | 10 | 9 | 8 | 10 |
| | Antivirus: Trend Micro | ALTO | 10 | 7 | 8 | 10 | 8 |
| | Ofimática: Office 365 | ALTO | 6 | 5 | 5 | 8 | 5 |
| | Webserver: IIS | ALTO | 6 | 8 | 8 | 6 | 5 |
| | Monitoreo: Stencil | MUY ALTO | 10 | 10 | 10 | 10 | 10 |
| | Posicionamiento : Google maps | ALTO | 4 | 3 | 5 | 8 | 3 |
| | Comunicaciones: MotoTRB | ALTO | 9 | 10 | 9 | 10 | 10 |
| DATOS | Bases de datos corporativas | MUY ALTO | 10 | 10 | 10 | 10 | 10 |
| | Base de datos contables | MUY ALTO | 10 | 10 | 10 | 10 | 10 |
| | Base de datos clientes | ALTO | 10 | 10 | 10 | 10 | 10 |
| | Base de datos inspecciones | ALTO | 10 | 10 | 10 | 10 | 10 |
| | Base de datos inventarios | ALTO | 10 | 10 | 10 | 10 | 10 |
| | Base de datos emergencias | MUY ALTO | 10 | 10 | 10 | 10 | 10 |
| RED | Backups de contabilidad | MUY ALTO | | | | 10 | |
| | Red de datos | MUY ALTO | 10 | 10 | 10 | 10 | 10 |
| | Red de telefonía IP | MUY ALTO | | | | 8 | |
| | Red de radio comunicaciones | MUY ALTO | | | | 9 | |
| | Acceso a Internet | ALTO | | | | 9 | |
| SERVICIOS | Internet | ALTO | | | | 10 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Intranet | MEDIO | | | | 6 | |
| | Telefonía | ALTO | | | | 10 | |
| | Radios | ALTO | | | | 10 | |
| EQUIPOS ADICIONALES | Sistema de alimentación UPS | MUY ALTO | | | | 10 | |
| | Radios Portátiles | ALTO | | 10 | | 10 | |
| | Radios Móviles | ALTO | | 10 | | 10 | |
| | Radio Base | MUY ALTO | | 10 | | 10 | |
| | Repetidoras | MUY ALTO | | 10 | | 10 | |
| | Antenas | ALTO | | 10 | | 10 | |
| PERSONAL | Operativos (Bomberos) | MEDIO | | 10 | | 7 | |
| | Administrativos | ALTO | | 10 | | 10 | |
| | Soporte (Externos) | MUY ALTO | | 10 | | 10 | |
| SOPORTES INFORMACIÓN | Archivo físico impreso | MUY ALTO | 10 | 10 | 10 | 10 | 10 |
| | Discos duros de servidores y estaciones de trabajo. | MUY ALTO | 10 | 10 | 10 | 10 | 10 |
| | Discos externos información de Backups | MUY ALTO | 10 | 8 | 10 | 8 | 9 |
| | Unidades de CD , DVD y Memorias extraíbles | MUY ALTO | 5 | | 9 | 5 | |
| | Almacenamiento en internet (Nube) | MUY ALTO | | 8 | 9 | 7 | |

Fuente: Arango (2016)

## Análisis

De acuerdo a los resultados obtenidos en la tabla de valoración del panorama de seguridad de los activos de la información, se puede evidenciar que la mayoría de los elementos evaluados pueden ser catalogados como esenciales para el correcto funcionamiento de la entidad, puesto que obtuvieron una puntuación mayor a 7. En este orden de ideas, es necesario destacar la categoría de “datos” ya que, con ayuda del personal de soporte externo y administrativo, se llegó a la conclusión que aspectos como los datos suministrados por lo clientes, bases corporativas y demás elementos que componen este

ámbito, son los activos de la información más relevantes conforme a los parámetros que establece Magerit (autenticidad, confidencialidad, integridad, disponibilidad y trazabildad). Así mismo, activos de la información como: Ofimática: Office 365, Webserver: IIS, Posicionamiento de Google maps, intranet y unidades de CD, DVD y Memorias extraíbles, fueron los puntos que menor resultado alcanzaron, sin embargo, no quiere decir que tengan un grado de importancia irrelevante en vista a que el activo de la información que menor valor tuvo fue de 3. Como dato adicional, una gran parte de los elementos evaluados no cumplió con todas las dimensiones que establece Magerit, con lo cual pudo haber incidido en el resultado obtenido al final.

### 7.3.4. Análisis de Amenazas y Vulnerabilidades

Existen un gran número de amenazas y vulnerabilidades asociadas al tema tecnológico y por ende a los activos de la información. De manera tal que, es importante identificar las amenazas y de esta forma orientar de la mejor manera al sistema de gestión de seguridad de la información, con el propósito de disminuir el nivel de incertidumbre en las empresas. Además, al estar asociadas las amenazas y las vulnerabilidades, pueden actuar de manera conjunta y en la mayoría de los casos ocasionan daños o pérdidas en la integridad de la información que podrían poner en peligro el buen nombre de la organización afectada.

Teniendo en cuenta las vulnerabilidades que puede estar expuesta la organización, a continuación, se realizará un análisis de las amenazas que posiblemente afectan los activos de la información del Cuerpo de Bomberos Voluntarios de Tunja, elaborando una tabla de identificación de amenazas con el listado de las 20 amenazas más comunes, al igual que con el objetivo de reforzar aún más el análisis, se llevara a cabo una clasificación (fuente: natural, humano y entorno, agente generador, causa y efecto de la amenaza probable) que permita conocer con más detalle la situación de la entidad.

*Tabla 10: Identificación de Amenazas.*

| **TABLA IDENTIFICACIÓN AMENAZAS.** | | | | | |
|---|---|---|---|---|---|
| | | | | | |

| ID | AMENAZAS | FUENTE | | | AGENTE GENERADOR | CAUSA | EFECTO |
|---|---|---|---|---|---|---|---|
| | | Natural | Humano | Entorno | | | |
| **1** | Permitir la ejecución de un software malicioso. | | **X** | **X** | Personas irresponsables con los equipos. | Personas irresponsables, ausencia de antivirus, mal empleabilidad de navegación, carencias de buenas prácticas. | Ausencia de disponibilidad de la información, reducir la integridad y posible hurto. |
| **2** | Problemas en la estructura de la organización. | | **X** | | Personas maliciosas. | Política insuficiente, baja motivación de los empleados, problemas internos entre los empleados. | Ausencia de disponibilidad de la información, reducción de la integridad, ingreso de personal no autorizado, hurto. |
| **3** | Despojo de información. | | **X** | | Personas maliciosas | Falta de políticas, ausencia de controles, carencia de medidas criptográficas. | Falta de disponibilidad, pérdida en la imagen corporativa, vulneración del sistema. |
| **4** | Mala instalación en el cableado. | | | **X** | Empleados mal capacitados, escasez de recursos. | Poca importancia en la instalación. | Problemas de productividad, ausencia de disponibilidad. |
| **5** | Falta de mantenimiento. | | | **X** | Errores de la administración, problemas de la comunicación. | Poco interés por mantener en buen estado las cosas, falta de control y revisión. | Problemas de productividad, ausencia de disponibilidad, problemas de comunicación. |
| **6** | Inexistencia de parches. | | | **X** | Empleados no preparados. | No hay un software especializado en parches. | Desequilibrio en el sistema, procesos ejecutados de forma tardía, debilidad en el sistema. |
| **7** | Utilización de software no oficial. | | **X** | **X** | Empleados desinteresados, desconocimiento. | Ausencia de monitoreo en el SGSI, empleados no capacitados, carencia de recursos. | Problemas en el sistema, afectación a la reputación de la entidad, inconvenientes reglamentarios. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **8** | Ingreso de personal no autorizado. | | **x** | | Empleados no preparados, acciones dañinas. | Ausencia de medidas de inspección y vigilancia, inconvenientes en la aplicabilidad de la política. | Inconvenientes en el sistema, fuga de información, afectación en la reputación de la entidad, falta de disponibilidad. |
| **9** | Incapacidad. | | **x** | | Trabajadores de la entidad. | Carencia de interés en la salud de los trabajadores, sobrecarga laboral. | Disminución en la productividad, perjudica los proyectos en circulación, afectación en la imagen corporativa de la entidad. |
| **10** | Salida de personal. | | **x** | | Trabajadores de la entidad. | Falta de motivación, problemas de comunicación, inconvenientes personales. | Disminución en la productividad, perjudica los proyectos en circulación, afectación en la imagen corporativa de la entidad. |
| **11** | Eliminación y modificación. | | **x** | | Trabajadores de la entidad. | Carencia de control, insuficientes medidas criptográficas, problemas de inspección en el ingreso de personal externo a la entidad. | Fuga de información, afectación de la imagen corporativa. |
| **12** | Incendio | **X** | **x** | **X** | Trabajadores irresponsable, desastre natural, personal malintencionadas. | Desastres naturales, problemas internos, prácticas inadecuadas, falta de motivación. | Daño de información, problemas de disponibilidad. |
| **13** | Inconvenientes eléctricos. | **X** | | **X** | Falta de mantenimiento, ausencia de concientización, problemas en el servicio, desastre natural. | El mantenimiento no es contante, escasez de recursos, desastres naturales | Daño de información, problemas de disponibilidad. |
| **14** | Temblor | **X** | | | Desastre natural | Ubicación, zona de alto riesgo, gestor natural. | Daño de información, problemas de disponibilidad. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **15** | Falta de motivación. | | **X** | | Trabajadores de la entidad. | Poca motivación, inconvenientes de comunicación, falta de liderazgo, pocos ascensos. | Disminución en la productividad, perjudica los proyectos en circulación, entorno tenso. |
| **16** | Delegación de responsabilidades. | | **X** | | Trabajadores de la entidad. | Problemas de liderazgo, falta de claridad. | Disminución en la productividad, entorno tenso, liderazgo desconocido. |
| **17** | Técnicos que no son idóneos. | | **X** | | Trabajadores de la entidad. | Desconocimiento de sus deberes, falta de claridad, problemas en la contratación. | Disminución en la productividad, afectación de los proyectos en circulación, inconvenientes en el cumplimiento de objetivos. |
| **18** | Pérdida de equipos. | | **x** | **x** | Trabajadores de la entidad, agentes externos. | Falta de controles, inexistencia de controles de acceso. | Disminución de la productividad, pérdida de información. |
| **19** | Carencia de una metodología para la utilización de programas. | | **x** | | Falta de liderazgo, | Política del SGSI sin ser empleada, falta de liderazgo. | Uso inadecuado de los programas, Falta de eficiencia, |
| **20** | Terrorismo. | | **x** | **x** | Personas malintencionadas | Falta de controles, inexistencia de controles de acceso. | Daño y Perdida de la información, Difícil restauración de la información. |

Fuente: (Arango, 2016)

## Análisis

En la tabla 8: identificación de amenazas, se puede afirmar que, un gran número de posibles inconvenientes no provienen de fenómenos vinculados con la naturaleza, sino que radica de aspectos relacionados con el personal, lo cual se ve reflejado en otra sección de la tabla denominada como “agente generador”, evidenciando problemas como la presencia de personas malintencionadas, falta de liderazgo, trabajadores irresponsables, entre otros inconvenientes asociados al personal. Por lo tanto, al indagar las causas y efectos se puede evidenciar que, muchas de las amenazas descritas anteriormente, provienen principalmente de la ausencia de liderazgo por parte de los altos directivos, en momentos que es necesario

coordinar acciones encaminadas a poner en marcha procesos internos dirigidos a resguardar la información y como resultado (que incluso ya se ha venido presentando), la productividad ha venido cayendo notablemente (como los problemas ocurridos con el software contable presentados este año a causa de la persona encargada de hacer mantenimiento) perjudicando las actividades diarias de la entidad. En otro sentido, también se tuvieron a consideración amenazas ligadas a la fuente natural a pesar que el Cuerpo de Bomberos Voluntarios de Tunja está especializado en atender este tipo de riesgos, no obstante, en una circunstancia de catástrofe natural los activos de la información no pueden estar exentos de quedar en peligro así el riesgo no sea inminente.

Así mismo, teniendo en cuenta lo realizado anteriormente, se mostrará más adelante una tabla denominada "activos versus amenazas", con el fin de distinguir detalladamente la relación de cada activo con las amenazas detectadas. De esta manera, se conocerán los riesgos bajo los cuales cada activo está expuesto y será de gran ayuda para fijar por medio de valores numéricos el nivel de injerencia que tiene sobre cada activo la realización de la amenaza asociada. Es preciso mencionar que, debido al gran tamaño de la tabla será agregada como anexo.

#### 7.3.4.1. Relación Activos vs Amenazas

**Nota:** Revisar anexo: tablas para el análisis y tratamiento de los riesgos en el cuerpo de bomberos voluntarios de tunja.xlsx

**Análisis**

Como resultado de asociar las amenazas con los activos de la información, se pudo encontrar que la gran mayoría de recursos tienen una relación clara con aquellos sucesos que pueden poner en peligro el bienestar de la organización. En tal sentido, activos como servidores, equipos de seguridad perimetral, equipos de grabación, equipos de escritorio, webserver: IIS, entre otros, fueron los que más relación tuvieron con las amenazas anteriormente presentadas. En contraste, los activos de la información que tuvieron menos parentesco con los problemas enumerados fueron los siguientes: centro de procesamiento de datos, equipo de comunicaciones y computo, comunicaciones: motoTRB e intranet. Es preciso mencionar que, aunque los activos que mayor vinculación tuvieron con las

amenazas descritas son más propensos a estar expuestos, no se puede dejar de lado que la realización de una amenaza por más mínima que parezca puede dejar en jaque la estabilidad de la entidad.

Tras identificar la relación de cada uno de los activos con las diferentes amenazas, se analizará el impacto en diferentes dimensiones para la seguridad del activo y la frecuencia con la que ocurre el posible problema.

#### 7.3.4.2. Nivel de frecuencia.

El nivel de frecuencia se realizará de acuerdo a la regularidad en que ocurre un evento que pueda poner en peligro al activo de la información, según los parámetros establecidos en la tabla que se presentará a continuación. Es preciso enfatizar que, para realizar esta tabla se contó totalmente con la opinión de soporte externo.

*Tabla 11: Nivel De Frecuencia.*

| **NIVEL DE FRECUENCIA** | | |
|---|---|---|
| **EVALUACIÓN** | | **DESCRIPCIÓN** |
| A | 1 = 5 | SUCEDE REGULARMENTE |
| M+ | 0,75 = 4 | ES POSIBLE QUE SUCEDE |
| M | 0,5 = 3 | SUCEDE OCASIONALMENTE |
| M- | 0,25 = 2 | NO ES PROBABLE QUE SUCEDA |
| B | 0,1 = 1 | EXISTE UNA POSIBILIDAD MUY REMOTA QUE SUCEDA |

Fuente: elaboración propia a partir del libro I. de Magerit

#### 7.3.4.3. Impacto de operación.

El impacto de operación agrupa una serie de cualidades que convierten al activo en un elemento fundamental para cualquier organización, por lo tanto, si llega a ser vulnerado algunos de los aspectos que conforman el impacto de operación, la eficiencia podría verse afectada.

*Tabla 12: Impacto de Operación.*

| IMPACTO DE OPERACIÓN | | |
|---|---|---|
| **NIVEL** | | **DESCRIPCIÓN** |
| A | 100% = 5 | DAÑO MUY GRAVE |
| M+ | 75% = 4 | DAÑO GRAVE |
| M | 50% = 3 | DAÑO MEDIO |
| M- | 25% = 2 | DAÑO MENOR |
| B | 10% = 1 | DAÑO MUY INFERIOR |

Fuente: elaboración propia a partir del libro I de Magerit.

### 7.3.5. Activos y Dimensiones De La Seguridad.

En las siguientes tres tablas que se presentarán más adelante, es relevante decir que están sincronizadas conforme a los resultados obtenidos; partiendo de la tabla de activos y panorama de la seguridad, posteriormente el cálculo del riesgo y por último la tabla del impacto potencial, la cual reúne todo el proceso llevado a cabo para entender la situación de la empresa.

En la tabla Activos Y Dimensiones De La Seguridad, se tuvo a consideración la situación actual de los activos de la seguridad de la información en relación a las amenazas asociadas, con lo cual se asignó un valor teniendo en cuenta los criterios de las tablas: nivel de frecuencia e impacto de operación. Lo anterior se da, con la finalidad de medir lo reiteradas que se presentan las amenazas y el grado de afectación que tienen sobre los parámetros que sugiere Magerit.

*Tabla 13: Activos y Dimensiones o Panorama de la Seguridad.*

| CTIVO / AMENAZA | FRECUENCIA | AUTENTICIDAD | CRITICIDAD | INTEGRIDAD | DISPONIBILIDAD | TRAZABILIDAD |
|---|---|---|---|---|---|---|
| ESTACIONES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO | 0,2 | 75% | 75% | 75% | 75% | 75% |
| ESTACIONES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| ESTACIONES / DESPOJO DE INFORMACIÓN. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| ESTACIONES / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 25% | 25% | 25% | 25% | 25% |
| ESTACIONES / FALTA DE MANTENIMIENTO. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| ESTACIONES / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 0,10 | 10% | 10% | 10% | 10% | 10% |
| ESTACIONES / ELIMINACIÓN Y MODIFICACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| ESTACIONES / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ESTACIONES / INCONVENIENTES ELÉCTRICOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| ESTACIONES / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ESTACIONES / TÉCNICOS QUE NO SON IDÓNEOS. | 0,75 | 50% | 50% | 50% | 50% | 50% |
| ESTACIONES / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| ESTACIONES / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| REPETIDORAS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| REPETIDORAS / FALTA DE MANTENIMIENTO. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| REPETIDORAS / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| REPETIDORAS / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| INCONVENIENTES ELÉCTRICOS. | 0,50 | 25% | 25% | 25% | 25% | 25% |
| REPETIDORAS / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| REPETIDORAS / PÉRDIDA DE EQUIPOS. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| REPETIDORAS / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / FALTA DE MANTENIMIENTO. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |

| | | | | | | |
|---|---|---|---|---|---|---|
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / INCONVENIENTES ELÉCTRICOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / PÉRDIDA DE EQUIPOS. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / FALTA DE MANTENIMIENTO. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / INCONVENIENTES ELÉCTRICOS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| SERVIDORES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| SERVIDORES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| SERVIDORES / MALA INSTALACIÓN EN EL CABLEADO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| SERVIDORES / FALTA DE MANTENIMIENTO. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| SERVIDORES / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| SERVIDORES / INCENDIO | 0,10 | 10% | 10% | 10% | 10% | 10% |

| | | | | | | |
|---|---|---|---|---|---|---|
| SERVIDORES / INCONVENIENTES ELÉCTRICOS. | 0,25 | 25% | 25% | 25% | 25% | 25% |
| SERVIDORES / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| SERVIDORES / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| SERVIDORES / PÉRDIDA DE EQUIPOS. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| SERVIDORES / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| EQUIPOS ESCRITORIO PORTATILES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS ESCRITORIO PORTATILES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS ESCRITORIO PORTATILES / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| EQUIPOS ESCRITORIO PORTATILES / FALTA DE MANTENIMIENTO. | 0,75 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS ESCRITORIO PORTATILES / INGRESO DE PERSONAL NO AUTORIZADO. | 0,25 | 25% | 25% | 25% | 25% | 25% |
| EQUIPOS ESCRITORIO PORTATILES / SALIDA DE PERSONAL. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| EQUIPOS ESCRITORIO PORTATILES / ELIMINACIÓN Y MODIFICACIÓN. | 0,75 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS ESCRITORIO PORTATILES / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| EQUIPOS ESCRITORIO PORTATILES / INCONVENIENTES ELÉCTRICOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| EQUIPOS ESCRITORIO PORTATILES / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| EQUIPOS ESCRITORIO PORTATILES / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS ESCRITORIO PORTATILES / PÉRDIDA DE EQUIPOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| EQUIPOS ESCRITORIO PORTATILES / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| EQUIPOS ESCRITORIO PORTATILES / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| EQUIPOS DE COMUNICACIONES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS DE COMUNICACIONES / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 25% | 25% | 25% | 25% | 25% |
| EQUIPOS DE COMUNICACIONES / FALTA DE MANTENIMIENTO. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| EQUIPOS DE COMUNICACIONES / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 10% | 10% | 10% | 10% | 10% |

| | | | | | | |
|---|---|---|---|---|---|---|
| EQUIPOS DE COMUNICACIONES / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| EQUIPOS DE COMUNICACIONES / INCONVENIENTES ELÉCTRICOS. | 0,25 | 25% | 25% | 25% | 25% | 25% |
| EQUIPOS DE COMUNICACIONES / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| EQUIPOS DE COMUNICACIONES / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| EQUIPOS DE COMUNICACIONES / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS DE COMUNICACIONES / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN /PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 25% | 25% | 25% | 25% | 25% |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN /FALTA DE MANTENIMIENTO. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN /INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 10% | 10% | 10% | 10% | 10% |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / INCONVENIENTES ELÉCTRICOS. | 0,25 | 25% | 25% | 25% | 25% | 25% |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / DESPOJO DE INFORMACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / FALTA DE MANTENIMIENTO. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 75% | 75% | 75% | 75% | 75% |

| | | | | | | |
|---|---|---|---|---|---|---|
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / ELIMINACIÓN Y MODIFICACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / INCONVENIENTES ELÉCTRICOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / TÉCNICOS QUE NO SON IDÓNEOS. | 0,25 | 25% | 25% | 25% | 25% | 25% |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / PÉRDIDA DE EQUIPOS. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| EQUIPOS DE GRABACIÓN (LLAMADAS) /PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / DESPOJO DE INFORMACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / FALTA DE MANTENIMIENTO. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / ELIMINACIÓN Y MODIFICACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / INCONVENIENTES ELÉCTRICOS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / TÉCNICOS QUE NO SON IDÓNEOS. | 0,25 | 25% | 25% | 25% | 25% | 25% |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / PÉRDIDA DE EQUIPOS. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / CARENCIA DE UNA | 0,50 | 50% | 50% | 50% | 50% | 50% |

| | | | | | | |
|---|---|---|---|---|---|---|
| METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | | | | | | |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| PLANTA TELEFÓNICA / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| PLANTA TELEFÓNICA / MALA INSTALACIÓN EN EL CABLEADO. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| PLANTA TELEFÓNICA / FALTA DE MANTENIMIENTO. | 0,25 | 10% | 10% | 10% | 10% | 10% |
| PLANTA TELEFÓNICA / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 10% | 10% | 10% | 10% | 10% |
| PLANTA TELEFÓNICA / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| PLANTA TELEFÓNICA / INCONVENIENTES ELÉCTRICOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| PLANTA TELEFÓNICA / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| PLANTA TELEFÓNICA / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 25% | 25% | 25% | 25% | 25% |
| PLANTA TELEFÓNICA / PÉRDIDA DE EQUIPOS. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| PLANTA TELEFÓNICA / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| WINDOWS 7, 8 Y 10 / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,25 | 100% | 100% | 100% | 100% | 100% |
| WINDOWS 7, 8 Y 10 / DESPOJO DE INFORMACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| WINDOWS 7, 8 Y 10 / INEXISTENCIA DE PARCHES. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| WINDOWS 7, 8 Y 10 / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 0,25 | 100% | 100% | 100% | 100% | 100% |
| WINDOWS 7, 8 Y 10 / ELIMINACIÓN Y MODIFICACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| WINDOWS 7, 8 Y 10 / INCONVENIENTES ELÉCTRICOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| WINDOWS 7, 8 Y 10 / TÉCNICOS QUE NO SON IDÓNEOS. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| WINDOWS 7, 8 Y 10 / PÉRDIDA DE EQUIPOS. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| WINDOWS 7, 8 Y 10 / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| WINDOWS SERVER 2012 / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| WINDOWS SERVER 2012 / DESPOJO DE INFORMACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| WINDOWS SERVER 2012 / INEXISTENCIA DE PARCHES. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| WINDOWS SERVER 2012 / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| WINDOWS SERVER 2012 / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 25% | 25% | 25% | 25% | 25% |

| | | | | | | |
|---|---|---|---|---|---|---|
| WINDOWS SERVER 2012 / ELIMINACIÓN Y MODIFICACIÓN. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| WINDOWS SERVER 2012 / INCONVENIENTES ELÉCTRICOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| WINDOWS SERVER 2012 / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| WINDOWS SERVER 2012 / PÉRDIDA DE EQUIPOS. | 0,25 | 100% | 100% | 100% | 100% | 100% |
| WINDOWS SERVER 2012 / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| WINDOWS SERVER 2012 / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| BASES DE DATOS SQL SERVER 2014 / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS SQL SERVER 2014/ DESPOJO DE INFORMACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| BASES DE DATOS SQL SERVER 2014/ INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 10% | 10% | 10% | 10% | 10% |
| BASES DE DATOS SQL SERVER 2014/ ELIMINACIÓN Y MODIFICACIÓN. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| BASES DE DATOS SQL SERVER 2014/ INCONVENIENTES ELÉCTRICOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| BASES DE DATOS SQL SERVER 2014/ TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| BASES DE DATOS SQL SERVER 2014/ PÉRDIDA DE EQUIPOS. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS SQL SERVER 2014/ CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS SQL SERVER 2014/ TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / DESPOJO DE INFORMACIÓN. | 0,50 | 100% | 100% | 100% | 100% | 100% |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / MALA INSTALACIÓN EN EL CABLEADO. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / FALTA DE MANTENIMIENTO. | 0,75 | 75% | 75% | 75% | 75% | 75% |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / INGRESO DE PERSONAL NO AUTORIZADO. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / INCAPACIDAD. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / SALIDA DE PERSONAL. | 0,25 | 75% | 75% | 75% | 75% | 75% |

| | | | | | | |
|---|---|---|---|---|---|---|
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / ELIMINACIÓN Y MODIFICACIÓN. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / INCONVENIENTES ELÉCTRICOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / TÉCNICOS QUE NO SON IDÓNEOS. | 0,75 | 100% | 100% | 100% | 100% | 100% |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / DESPOJO DE INFORMACIÓN. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / INCAPACIDAD. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / ELIMINACIÓN Y MODIFICACIÓN. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / DELEGACIÓN DE RESPONSABILIDADES. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / PÉRDIDA DE EQUIPOS. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ANTIVIRUS: TREND MICRO / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| ANTIVIRUS: TREND MICRO / DESPOJO DE INFORMACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| ANTIVIRUS: TREND MICRO / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| ANTIVIRUS: TREND MICRO / FALTA DE MANTENIMIENTO. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| ANTIVIRUS: TREND MICRO / INEXISTENCIA DE PARCHES. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| ANTIVIRUS: TREND MICRO / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| ANTIVIRUS: TREND MICRO / ELIMINACIÓN Y MODIFICACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |

| | | | | | | |
|---|---|---|---|---|---|---|
| ANTIVIRUS: TREND MICRO / INCONVENIENTES ELÉCTRICOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| ANTIVIRUS: TREND MICRO / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| ANTIVIRUS: TREND MICRO / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| ANTIVIRUS: TREND MICRO / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| ANTIVIRUS: TREND MICRO / TERRORISMO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| OFIMÁTICA: OFFICE 365 / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| OFIMÁTICA: OFFICE 365 / DESPOJO DE INFORMACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| OFIMÁTICA: OFFICE 365 / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| OFIMÁTICA: OFFICE 365 / FALTA DE MANTENIMIENTO. | 0,10 | 10% | 10% | 10% | 10% | 10% |
| OFIMÁTICA: OFFICE 365 / INEXISTENCIA DE PARCHES. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| OFIMÁTICA: OFFICE 365 / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| OFIMÁTICA: OFFICE 365 / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| OFIMÁTICA: OFFICE 365 / ELIMINACIÓN Y MODIFICACIÓN. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| OFIMÁTICA: OFFICE 365 / TÉCNICOS QUE NO SON IDÓNEOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| OFIMÁTICA: OFFICE 365 / PÉRDIDA DE EQUIPOS. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| OFIMÁTICA: OFFICE 365 / TERRORISMO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| WEBSERVER. II / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| WEBSERVER. II / DESPOJO DE INFORMACIÓN. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| WEBSERVER. II / MALA INSTALACIÓN EN EL CABLEADO. | 0,50 | 25% | 25% | 25% | 25% | 25% |
| WEBSERVER. II / FALTA DE MANTENIMIENTO. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| WEBSERVER. II / INEXISTENCIA DE PARCHES. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| WEBSERVER. II / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| WEBSERVER. II / ELIMINACIÓN Y MODIFICACIÓN. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| WEBSERVER. II / INCONVENIENTES ELÉCTRICOS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| WEBSERVER. II / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 25% | 25% | 25% | 25% | 25% |
| WEBSERVER. II / PÉRDIDA DE EQUIPOS. | 0,10 | 10% | 10% | 10% | 10% | 10% |

| | | | | | | |
|---|---|---|---|---|---|---|
| WEBSERVER. II / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 0,75 | 50% | 50% | 50% | 50% | 50% |
| WEBSERVER. II / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| POSICIONAMIENTO: GOOGLE MAPS / FALTA DE MANTENIMIENTO. | 0,10 | 10% | 10% | 10% | 10% | 10% |
| COMUNICACIONES: MOTO TRB / FALTA DE MANTENIMIENTO. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| COMUNICACIONES: MOTO TRB / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| COMUNICACIONES: MOTO TRB / SALIDA DE PERSONAL. | 0,50 | 25% | 25% | 25% | 25% | 25% |
| COMUNICACIONES: MOTO TRB / INCENDIO | 0,10 | 75% | 75% | 75% | 75% | 75% |
| COMUNICACIONES: MOTO TRB / INCONVENIENTES ELÉCTRICOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| COMUNICACIONES: MOTO TRB / TEMBLOR | 0,10 | 75% | 75% | 75% | 75% | 75% |
| COMUNICACIONES: MOTO TRB / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| COMUNICACIONES: MOTO TRB / PÉRDIDA DE EQUIPOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| COMUNICACIONES: MOTO TRB / TERRORISMO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS CORPORATIVAS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,25 | 100% | 100% | 100% | 100% | 100% |
| BASES DE DATOS CORPORATIVAS / DESPOJO DE INFORMACIÓN. | 0,25 | 100% | 100% | 100% | 100% | 100% |
| BASES DE DATOS CORPORATIVAS / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS CORPORATIVAS / INGRESO DE PERSONAL NO AUTORIZADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS CORPORATIVAS / ELIMINACIÓN Y MODIFICACIÓN. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| BASES DE DATOS CORPORATIVAS / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| BASES DE DATOS CORPORATIVAS / INCONVENIENTES ELÉCTRICOS. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| BASES DE DATOS CORPORATIVAS / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| BASES DE DATOS CORPORATIVAS / PÉRDIDA DE EQUIPOS. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| BASES DE DATOS CORPORATIVAS / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| BASE DE DATOS CONTABLES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASE DE DATOS CONTABLES / DESPOJO DE INFORMACIÓN. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| BASE DE DATOS CONTABLES / FALTA DE MANTENIMIENTO. | 0,10 | 75% | 75% | 75% | 75% | 75% |

| | | | | | | |
|---|---|---|---|---|---|---|
| BASE DE DATOS CONTABLES / INGRESO DE PERSONAL NO AUTORIZADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| BASE DE DATOS CONTABLES / SALIDA DE PERSONAL. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASE DE DATOS CONTABLES / ELIMINACIÓN Y MODIFICACIÓN. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| BASE DE DATOS CONTABLES / INCENDIO | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASE DE DATOS CONTABLES / INCONVENIENTES ELÉCTRICOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| BASE DE DATOS CONTABLES / TEMBLOR | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASE DE DATOS CONTABLES / TÉCNICOS QUE NO SON IDÓNEOS. | 0,75 | 100% | 100% | 100% | 100% | 100% |
| BASE DE DATOS CONTABLES / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASE DE DATOS CONTABLES / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| BASE DE DATOS CONTABLES / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| BASE DE DATOS CLIENTES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASE DE DATOS CLIENTES / DESPOJO DE INFORMACIÓN. | 0,25 | 100% | 100% | 100% | 100% | 100% |
| BASE DE DATOS CLIENTES / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| BASE DE DATOS CLIENTES / INGRESO DE PERSONAL NO AUTORIZADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| BASE DE DATOS CLIENTES / SALIDA DE PERSONAL. | 0,75 | 100% | 100% | 100% | 100% | 100% |
| BASE DE DATOS CLIENTES / ELIMINACIÓN Y MODIFICACIÓN. | 0,75 | 75% | 75% | 75% | 75% | 75% |
| BASE DE DATOS CLIENTES / INCENDIO | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASE DE DATOS CLIENTES / INCONVENIENTES ELÉCTRICOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| BASE DE DATOS CLIENTES / TEMBLOR | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASE DE DATOS CLIENTES / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASE DE DATOS CLIENTES / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| BASES DE DATOS INSPECCIONES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS INSPECCIONES / DESPOJO DE INFORMACIÓN. | 0,25 | 100% | 100% | 100% | 100% | 100% |
| BASES DE DATOS INSPECCIONES / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| BASES DE DATOS INSPECCIONES / INGRESO DE PERSONAL NO AUTORIZADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |

| | | | | | | |
|---|---|---|---|---|---|---|
| BASES DE DATOS INSPECCIONES / SALIDA DE PERSONAL. | 0,75 | 100% | 100% | 100% | 100% | 100% |
| BASES DE DATOS INSPECCIONES / ELIMINACIÓN Y MODIFICACIÓN. | 0,75 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS INSPECCIONES / INCENDIO | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS INSPECCIONES / INCONVENIENTES ELÉCTRICOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| BASES DE DATOS INSPECCIONES / TEMBLOR | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS INSPECCIONES / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS INSPECCIONES / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| BASES DE DATOS INVENTARIOS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS INVENTARIOS / DESPOJO DE INFORMACIÓN. | 0,25 | 100% | 100% | 100% | 100% | 100% |
| BASES DE DATOS INVENTARIOS / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| BASES DE DATOS INVENTARIOS / INGRESO DE PERSONAL NO AUTORIZADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS INVENTARIOS / SALIDA DE PERSONAL. | 0,75 | 100% | 100% | 100% | 100% | 100% |
| BASES DE DATOS INVENTARIOS / ELIMINACIÓN Y MODIFICACIÓN. | 0,75 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS INVENTARIOS / INCENDIO | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS INVENTARIOS / INCONVENIENTES ELÉCTRICOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| BASES DE DATOS INVENTARIOS / TEMBLOR | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS INVENTARIOS / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS INVENTARIOS / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| BASES DE DATOS EMERGENCIAS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS EMERGENCIAS / DESPOJO DE INFORMACIÓN. | 0,25 | 100% | 100% | 100% | 100% | 100% |
| BASES DE DATOS EMERGENCIAS / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| BASES DE DATOS EMERGENCIAS / INGRESO DE PERSONAL NO AUTORIZADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS EMERGENCIAS / SALIDA DE PERSONAL. | 0,75 | 100% | 100% | 100% | 100% | 100% |
| BASES DE DATOS EMERGENCIAS / ELIMINACIÓN Y MODIFICACIÓN. | 0,75 | 75% | 75% | 75% | 75% | 75% |

| | | | | | | |
|---|---|---|---|---|---|---|
| BASES DE DATOS EMERGENCIAS / INCENDIO | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS EMERGENCIAS / INCONVENIENTES ELÉCTRICOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| BASES DE DATOS EMERGENCIAS / TEMBLOR | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS EMERGENCIAS / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BASES DE DATOS EMERGENCIAS / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| BACKUPS DE CONTABILIDAD / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BACKUPS DE CONTABILIDAD / DESPOJO DE INFORMACIÓN. | 0,25 | 100% | 100% | 100% | 100% | 100% |
| BACKUPS DE CONTABILIDAD / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| BACKUPS DE CONTABILIDAD / INGRESO DE PERSONAL NO AUTORIZADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| BACKUPS DE CONTABILIDAD / SALIDA DE PERSONAL. | 0,75 | 100% | 100% | 100% | 100% | 100% |
| BACKUPS DE CONTABILIDAD / ELIMINACIÓN Y MODIFICACIÓN. | 0,75 | 75% | 75% | 75% | 75% | 75% |
| BACKUPS DE CONTABILIDAD / INCENDIO | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BACKUPS DE CONTABILIDAD / INCONVENIENTES ELÉCTRICOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| BACKUPS DE CONTABILIDAD / TEMBLOR | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BACKUPS DE CONTABILIDAD / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| BACKUPS DE CONTABILIDAD / TERRORISMO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| RED DE DATOS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RED DE DATOS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| RED DE DATOS / DESPOJO DE INFORMACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| RED DE DATOS / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 100% | 100% | 100% | 100% | 100% |
| RED DE DATOS / FALTA DE MANTENIMIENTO. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| RED DE DATOS / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RED DE DATOS / INCONVENIENTES ELÉCTRICOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| RED DE DATOS / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RED DE DATOS / TÉCNICOS QUE NO SON IDÓNEOS. | 0,75 | 75% | 75% | 75% | 75% | 75% |
| RED DE DATOS / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |

| | | | | | | |
|---|---|---|---|---|---|---|
| RED RADIO COMUNICACIONES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| RED RADIO COMUNICACIONES / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| RED RADIO COMUNICACIONES / FALTA DE MANTENIMIENTO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| RED RADIO COMUNICACIONES / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| RED RADIO COMUNICACIONES / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RED RADIO COMUNICACIONES / INCONVENIENTES ELÉCTRICOS. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| RED RADIO COMUNICACIONES / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RED RADIO COMUNICACIONES / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| RED RADIO COMUNICACIONES / PÉRDIDA DE EQUIPOS. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RED RADIO COMUNICACIONES / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ACCESO A INTERNET / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| ACCESO A INTERNET / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| ACCESO A INTERNET / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 100% | 100% | 100% | 100% | 100% |
| ACCESO A INTERNET / ELIMINACIÓN Y MODIFICACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| ACCESO A INTERNET / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ACCESO A INTERNET / INCONVENIENTES ELÉCTRICOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| ACCESO A INTERNET / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ACCESO A INTERNET / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| ACCESO A INTERNET / PÉRDIDA DE EQUIPOS. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ACCESO A INTERNET / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| INTERNET / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| INTERNET / DESPOJO DE INFORMACIÓN. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| INTERNET / ELIMINACIÓN Y MODIFICACIÓN. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| INTERNET / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| INTERNET / INCONVENIENTES ELÉCTRICOS. | 0,25 | 10% | 10% | 10% | 10% | 10% |

| | | | | | | |
|---|---|---|---|---|---|---|
| INTERNET / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| INTERNET / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| INTERNET / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| INTERNET / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| INTRANET / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| INTRANET / DESPOJO DE INFORMACIÓN. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| INTRANET / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| INTRANET / INCONVENIENTES ELÉCTRICOS. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| INTRANET / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| INTRANET / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| INTRANET / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| INTRANET / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| TELEFONIA / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| TELEFONIA / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| TELEFONIA / FALTA DE MANTENIMIENTO. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| TELEFONIA / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| TELEFONIA / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| TELEFONIA / INCONVENIENTES ELÉCTRICOS. | 0,50 | 25% | 25% | 25% | 25% | 25% |
| TELEFONIA / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| TELEFONIA / TÉCNICOS QUE NO SON IDÓNEOS. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| TELEFONIA / PÉRDIDA DE EQUIPOS. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| TELEFONIA / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RADIOS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| RADIOS / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| RADIOS / FALTA DE MANTENIMIENTO. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| RADIOS / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| RADIOS / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |

| | | | | | | |
|---|---|---|---|---|---|---|
| RADIOS / INCONVENIENTES ELÉCTRICOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| RADIOS / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RADIOS / TÉCNICOS QUE NO SON IDÓNEOS. | 0,25 | 10% | 10% | 10% | 10% | 10% |
| RADIOS / PÉRDIDA DE EQUIPOS. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RADIOS / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| SISTEMA DE ALIMENTACIÓN UPS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| SISTEMA DE ALIMENTACIÓN UPS / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| SISTEMA DE ALIMENTACIÓN UPS / FALTA DE MANTENIMIENTO. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| SISTEMA DE ALIMENTACIÓN UPS / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| SISTEMA DE ALIMENTACIÓN UPS / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| SISTEMA DE ALIMENTACIÓN UPS / INCONVENIENTES ELÉCTRICOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| SISTEMA DE ALIMENTACIÓN UPS / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| SISTEMA DE ALIMENTACIÓN UPS / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 25% | 25% | 25% | 25% | 25% |
| SISTEMA DE ALIMENTACIÓN UPS / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| SISTEMA DE ALIMENTACIÓN UPS / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RADIOS PORTATILES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| RADIOS PORTATILES / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| RADIOS PORTATILES / FALTA DE MANTENIMIENTO. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| RADIOS PORTATILES / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| RADIOS PORTATILES / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RADIOS PORTATILES / INCONVENIENTES ELÉCTRICOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| RADIOS PORTATILES / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RADIOS PORTATILES / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 25% | 25% | 25% | 25% | 25% |
| RADIOS PORTATILES / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| RADIOS PORTATILES / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |

| | | | | | | |
|---|---|---|---|---|---|---|
| RADIOS MOVILES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| RADIOS MOVILES / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| RADIOS MOVILES / FALTA DE MANTENIMIENTO. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| RADIOS MOVILES / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| RADIOS MOVILES / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RADIOS MOVILES / INCONVENIENTES ELÉCTRICOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| RADIOS MOVILES / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RADIOS MOVILES / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 25% | 25% | 25% | 25% | 25% |
| RADIOS MOVILES / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| RADIOS MOVILES / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RADIO BASE / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| RADIO BASE / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| RADIO BASE / FALTA DE MANTENIMIENTO. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| RADIO BASE / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| RADIO BASE / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RADIO BASE / INCONVENIENTES ELÉCTRICOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| RADIO BASE / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| RADIO BASE / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 25% | 25% | 25% | 25% | 25% |
| RADIO BASE / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| RADIO BASE / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| REPETIDORAS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| REPETIDORAS / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| REPETIDORAS / FALTA DE MANTENIMIENTO. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| REPETIDORAS / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| REPETIDORAS / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| REPETIDORAS / INCONVENIENTES ELÉCTRICOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| REPETIDORAS / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |

| | | | | | | |
|---|---|---|---|---|---|---|
| REPETIDORAS / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 25% | 25% | 25% | 25% | 25% |
| REPETIDORAS / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| REPETIDORAS / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ANTENAS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| ANTENAS / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| ANTENAS / FALTA DE MANTENIMIENTO. | 0,50 | 50% | 50% | 50% | 50% | 50% |
| ANTENAS / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| ANTENAS / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| INCONVENIENTES ELÉCTRICOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| ANTENAS / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ANTENAS / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 25% | 25% | 25% | 25% | 25% |
| ANTENAS / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| ANTENAS / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| OPERATIVOS (BOMBEROS) / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| OPERATIVOS (BOMBEROS) / DESPOJO DE INFORMACIÓN. | 0,25 | 25% | 25% | 25% | 25% | 25% |
| OPERATIVOS (BOMBEROS) / MALA INSTALACIÓN EN EL CABLEADO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| OPERATIVOS (BOMBEROS) / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| OPERATIVOS (BOMBEROS) / INCAPACIDAD. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| OPERATIVOS (BOMBEROS) / SALIDA DE PERSONAL. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| OPERATIVOS (BOMBEROS) / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| OPERATIVOS (BOMBEROS) / INCONVENIENTES ELÉCTRICOS. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| OPERATIVOS (BOMBEROS) / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| OPERATIVOS (BOMBEROS) / FALTA DE MOTIVACIÓN. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| OPERATIVOS (BOMBEROS) / DELEGACIÓN DE RESPONSABILIDADES. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| OPERATIVOS (BOMBEROS) / PÉRDIDA DE EQUIPOS. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| OPERATIVOS (BOMBEROS) / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |

| | | | | | | |
|---|---|---|---|---|---|---|
| ADMINISTRATIVOS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| ADMINISTRATIVOS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ADMINISTRATIVOS / DESPOJO DE INFORMACIÓN. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| ADMINISTRATIVOS / MALA INSTALACIÓN EN EL CABLEADO. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| ADMINISTRATIVOS / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| ADMINISTRATIVOS / INGRESO DE PERSONAL NO AUTORIZADO. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| ADMINISTRATIVOS / INCAPACIDAD. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| ADMINISTRATIVOS / SALIDA DE PERSONAL. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| ADMINISTRATIVOS / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ADMINISTRATIVOS / INCONVENIENTES ELÉCTRICOS. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| ADMINISTRATIVOS / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ADMINISTRATIVOS / FALTA DE MOTIVACIÓN. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| ADMINISTRATIVOS / DELEGACIÓN DE RESPONSABILIDADES. | 0,75 | 50% | 50% | 50% | 50% | 50% |
| ADMINISTRATIVOS / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| ADMINISTRATIVOS / PÉRDIDA DE EQUIPOS. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| ADMINISTRATIVOS / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| SOPORTE EXTERNO / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| SOPORTE EXTERNO / DESPOJO DE INFORMACIÓN. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| SOPORTE EXTERNO / MALA INSTALACIÓN EN EL CABLEADO. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| SOPORTE EXTERNO / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 0,10 | 25% | 25% | 25% | 25% | 25% |
| SOPORTE EXTERNO / INGRESO DE PERSONAL NO AUTORIZADO. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| SOPORTE EXTERNO / INCAPACIDAD. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| SOPORTE EXTERNO / SALIDA DE PERSONAL. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| SOPORTE EXTERNO / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| SOPORTE EXTERNO / INCONVENIENTES ELÉCTRICOS. | 0,25 | 75% | 75% | 75% | 75% | 75% |

| | | | | | | |
|---|---|---|---|---|---|---|
| SOPORTE EXTERNO / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| SOPORTE EXTERNO / FALTA DE MOTIVACIÓN. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| SOPORTE EXTERNO / DELEGACIÓN DE RESPONSABILIDADES. | 0,75 | 50% | 50% | 50% | 50% | 50% |
| SOPORTE EXTERNO / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| SOPORTE EXTERNO / PÉRDIDA DE EQUIPOS. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| SOPORTE EXTERNO / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ARCHIVO FISÏCO IMPRESO / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ARCHIVO FISÏCO IMPRESO / DESPOJO DE INFORMACIÓN. | 0,25 | 100% | 100% | 100% | 100% | 100% |
| ARCHIVO FISÏCO IMPRESO / FALTA DE MANTENIMIENTO. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| ARCHIVO FISÏCO IMPRESO / INGRESO DE PERSONAL NO AUTORIZADO. | 0,25 | 10% | 10% | 10% | 10% | 10% |
| ARCHIVO FISÏCO IMPRESO / SALIDA DE PERSONAL. | 0,25 | 50% | 50% | 50% | 50% | 50% |
| ARCHIVO FISÏCO IMPRESO / ELIMINACIÓN Y MODIFICACIÓN. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ARCHIVO FISÏCO IMPRESO / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ARCHIVO FISÏCO IMPRESO / INCONVENIENTES ELÉCTRICOS. | 0,50 | 25% | 25% | 25% | 25% | 25% |
| ARCHIVO FISÏCO IMPRESO / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ARCHIVO FISÏCO IMPRESO / DELEGACIÓN DE RESPONSABILIDADES. | 0,50 | 75% | 75% | 75% | 75% | 75% |
| ARCHIVO FISÏCO IMPRESO / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / DESPOJO DE INFORMACIÓN. | 0,25 | 100% | 100% | 100% | 100% | 100% |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / SALIDA DE PERSONAL. | 0,50 | 100% | 100% | 100% | 100% | 100% |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / ELIMINACIÓN Y MODIFICACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |

| | | | | | | |
|---|---|---|---|---|---|---|
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / INCONVENIENTES ELÉCTRICOS. | 0,50 | 10% | 10% | 10% | 10% | 10% |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / TÉCNICOS QUE NO SON IDÓNEOS. | 0,75 | 50% | 50% | 50% | 50% | 50% |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / PÉRDIDA DE EQUIPOS. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / DESPOJO DE INFORMACIÓN. | 0,25 | 100% | 100% | 100% | 100% | 100% |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / SALIDA DE PERSONAL. | 0,50 | 100% | 100% | 100% | 100% | 100% |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / ELIMINACIÓN Y MODIFICACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / INCONVENIENTES ELÉCTRICOS. | 0,50 | 10% | 10% | 10% | 10% | 10% |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / TÉCNICOS QUE NO SON IDÓNEOS. | 0,75 | 50% | 50% | 50% | 50% | 50% |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 0,25 | 75% | 75% | 75% | 75% | 75% |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 0,10 | 50% | 50% | 50% | 50% | 50% |

| | | | | | | |
|---|---|---|---|---|---|---|
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / DESPOJO DE INFORMACIÓN. | 0,25 | 100% | 100% | 100% | 100% | 100% |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / SALIDA DE PERSONAL. | 0,50 | 100% | 100% | 100% | 100% | 100% |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / ELIMINACIÓN Y MODIFICACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / INCENDIO | 0,10 | 100% | 100% | 100% | 100% | 100% |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / INCONVENIENTES ELÉCTRICOS. | 0,50 | 10% | 10% | 10% | 10% | 10% |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / TEMBLOR | 0,10 | 100% | 100% | 100% | 100% | 100% |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / TÉCNICOS QUE NO SON IDÓNEOS. | 0,75 | 50% | 50% | 50% | 50% | 50% |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / PÉRDIDA DE EQUIPOS. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ALMACENAMIENTO EN INTERNET (NUBE) / DESPOJO DE INFORMACIÓN. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ALMACENAMIENTO EN INTERNET (NUBE) / INGRESO DE PERSONAL NO AUTORIZADO. | 0,10 | 100% | 100% | 100% | 100% | 100% |
| ALMACENAMIENTO EN INTERNET (NUBE) / ELIMINACIÓN Y MODIFICACIÓN. | 0,10 | 75% | 75% | 75% | 75% | 75% |
| ALMACENAMIENTO EN INTERNET (NUBE) / TÉCNICOS QUE NO SON IDÓNEOS. | 0,50 | 25% | 25% | 25% | 25% | 25% |
| ALMACENAMIENTO EN INTERNET (NUBE) / TERRORISMO. | 0,10 | 100% | 100% | 100% | 100% | 100% |

Fuente: (Arango, 2016)

**Análisis.**

Una vez realizada la relación entre las amenazas y los activos de la información, se procedió a determinar el nivel de frecuencia y el grado de incidencia que tiene la ocurrencia de cada amenaza sobre el activo de la información. En este orden de ideas, varias amenazas presentaron un nivel de frecuencia alta como sucedió con los ítems vinculados con los técnicos que no son idóneos, afectando a un gran número de activos de la información y en consecuencia el funcionamiento de la entidad. Por otra parte, elementos vinculados a las

catástrofes naturales presentaron bajos índices de frecuencia. En el caso de la incidencia que tienen las amenazas sobre las dimensiones de seguridad, varios problemas evidenciaron un impacto considerable en la autenticidad, confidencialidad, integridad, disponibilidad y la trazabilidad, lo cual se revisará más a fondo con realización de otras tablas que se presentarán más adelante. Igualmente, se ayudó a esclarecer aquellos activos que se encuentran en más alto riesgo y por lo tanto deberán ser atendidos a través del plan de tratamiento de riesgos, con el fin de identificar más detalles en los resultados analizados en la presente tabla y a continuación se elaborará una tabla con los datos ya clasificados según su nivel de gravedad, la cual permitirá analizar mejor los resultados con la tabla del cálculo del riesgo.

### 7.3.6. Tabla Calculo del Riesgo.

Para elaborar la tabla del cálculo del riesgo, se tomaron los resultados de la tabla anterior (Activos y Dimensiones De Seguridad) y se convirtieron los datos en 1,2,3,4 y 5 como lo establecen las tablas de nivel de frecuencia e impacto de operación, con la finalidad de calcular el nivel de riesgo como a continuación se va a presentar. A modo de ejemplo, es preciso señalar que, un resultado obtenido al multiplicar la probabilidad con el impacto de operación con un resultado entre 16 a 25 es considerado como alto; entre 11 a 15 como medio alto; entre 6 a 10 como medio y un resultado entre 1 a 5 como bajo.

*Tabla 14: Cálculo Del Riesgo.*

| ACTIVO / AMENAZA | PROBABILIDAD | | IMPACTO OPERACIÓN | | CÁLCULO DEL RIESGO (PROB.*IMPACTO) |
|---|---|---|---|---|---|
| ESTACIONES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO | 2 | M- | 4 | M+ | 8 |
| ESTACIONES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 4 | M+ | 4 |
| ESTACIONES / DESPOJO DE INFORMACIÓN. | 2 | M- | 4 | M+ | 8 |

| | | | | | |
|---|---|---|---|---|---|
| ESTACIONES / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 2 | M- | 4 |
| ESTACIONES / FALTA DE MANTENIMIENTO. | 2 | M- | 3 | M | 6 |
| ESTACIONES / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 1 | B | 1 |
| ESTACIONES / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4 | M+ | 4 |
| ESTACIONES / INCENDIO | 1 | B | 5 | A | 5 |
| ESTACIONES / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3 | M | 9 |
| ESTACIONES / TEMBLOR | 1 | B | 5 | A | 5 |
| ESTACIONES / TÉCNICOS QUE NO SON IDÓNEOS. | 4 | M+ | 3 | M | 12 |
| ESTACIONES / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| ESTACIONES / TERRORISMO. | 1 | B | 5 | A | 5 |
| REPETIDORAS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 4 | M+ | 4 |
| REPETIDORAS / FALTA DE MANTENIMIENTO. | 2 | M- | 3 | M | 6 |
| REPETIDORAS / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4 | M+ | 4 |
| REPETIDORAS / INCENDIO | 1 | B | 5 | A | 5 |
| INCONVENIENTES ELÉCTRICOS. | 3 | M | 2 | M- | 6 |
| REPETIDORAS / TEMBLOR | 1 | B | 5 | A | 5 |
| REPETIDORAS / PÉRDIDA DE EQUIPOS. | 1 | B | 5 | A | 5 |
| REPETIDORAS / TERRORISMO. | 1 | B | 5 | A | 5 |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 5 | A | 5 |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4 | M+ | 8 |

| | | | | | |
|---|---|---|---|---|---|
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / FALTA DE MANTENIMIENTO. | 2 | M- | 3 | M | 6 |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / INCENDIO | 1 | B | 5 | A | 5 |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3 | M | 9 |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / TEMBLOR | 1 | B | 5 | A | 5 |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4 | M+ | 12 |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / PÉRDIDA DE EQUIPOS. | 1 | B | 5 | A | 5 |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / TERRORISMO. | 1 | B | 5 | A | 5 |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 4 | M+ | 4 |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4 | M+ | 8 |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / FALTA DE MANTENIMIENTO. | 1 | B | 3 | M | 3 |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4 | M+ | 4 |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / INCENDIO | 1 | B | 5 | A | 5 |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / INCONVENIENTES ELÉCTRICOS. | 3 | M | 4 | M+ | 12 |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / TEMBLOR | 1 | B | 5 | A | 5 |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 3 | M | 9 |

| | | | | | |
|---|---|---|---|---|---|
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / TERRORISMO. | 1 | B | 5 | A | 5 |
| SERVIDORES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 4 | M+ | 8 |
| SERVIDORES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3 | M | 3 |
| SERVIDORES / MALA INSTALACIÓN EN EL CABLEADO. | 1 | B | 4 | M+ | 4 |
| SERVIDORES / FALTA DE MANTENIMIENTO. | 2 | M- | 3 | M | 6 |
| SERVIDORES / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 3 | M | 3 |
| SERVIDORES / INCENDIO | 1 | B | 1 | B | 1 |
| SERVIDORES / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 2 | M- | 4 |
| SERVIDORES / TEMBLOR | 1 | B | 5 | A | 5 |
| SERVIDORES / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 3 | M | 9 |
| SERVIDORES / PÉRDIDA DE EQUIPOS. | 1 | B | 5 | A | 5 |
| SERVIDORES / TERRORISMO. | 1 | B | 5 | A | 5 |
| EQUIPOS ESCRITORIO PORTATILES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4 | M+ | 4 |
| EQUIPOS ESCRITORIO PORTATILES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 4 | M+ | 4 |
| EQUIPOS ESCRITORIO PORTATILES / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 3 | M | 6 |

| | | | | | |
|---|---|---|---|---|---|
| EQUIPOS ESCRITORIO PORTATILES / FALTA DE MANTENIMIENTO. | 4 | M+ | 4 | M+ | 16 |
| EQUIPOS ESCRITORIO PORTATILES / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 2 | M- | 4 |
| EQUIPOS ESCRITORIO PORTATILES / SALIDA DE PERSONAL. | 1 | B | 3 | M | 3 |
| EQUIPOS ESCRITORIO PORTATILES / ELIMINACIÓN Y MODIFICACIÓN. | 4 | M+ | 4 | M+ | 16 |
| EQUIPOS ESCRITORIO PORTATILES / INCENDIO | 1 | B | 5 | A | 5 |
| EQUIPOS ESCRITORIO PORTATILES / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3 | M | 6 |
| EQUIPOS ESCRITORIO PORTATILES / TEMBLOR | 1 | B | 5 | A | 5 |
| EQUIPOS ESCRITORIO PORTATILES / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4 | M+ | 12 |
| EQUIPOS ESCRITORIO PORTATILES / PÉRDIDA DE EQUIPOS. | 2 | M- | 3 | M | 6 |
| EQUIPOS ESCRITORIO PORTATILES / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 1 | B | 2 | M- | 2 |
| EQUIPOS ESCRITORIO PORTATILES / TERRORISMO. | 1 | B | 5 | A | 5 |
| EQUIPOS DE COMUNICACIONES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 4 | M+ | 4 |
| EQUIPOS DE COMUNICACIONES / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 2 | M- | 4 |
| EQUIPOS DE COMUNICACIONES / FALTA DE MANTENIMIENTO. | 3 | M | 3 | M | 9 |
| EQUIPOS DE COMUNICACIONES / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 1 | B | 1 |

| | | | | | |
|---|---|---|---|---|---|
| EQUIPOS DE COMUNICACIONES / INCENDIO | 1 | B | 5 | A | 5 |
| EQUIPOS DE COMUNICACIONES / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 2 | M- | 4 |
| EQUIPOS DE COMUNICACIONES / TEMBLOR | 1 | B | 5 | A | 5 |
| EQUIPOS DE COMUNICACIONES / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 3 | M | 9 |
| EQUIPOS DE COMUNICACIONES / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| EQUIPOS DE COMUNICACIONES / TERRORISMO. | 1 | B | 5 | A | 5 |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN /PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3 | M | 3 |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 2 | M- | 4 |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN /FALTA DE MANTENIMIENTO. | 3 | M | 3 | M | 9 |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN /INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 1 | B | 1 |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / INCENDIO | 1 | B | 5 | A | 5 |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 2 | M- | 4 |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / TEMBLOR | 1 | B | 5 | A | 5 |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 3 | M | 9 |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / TERRORISMO. | 1 | B | 5 | A | 5 |

| | | | | | |
|---|---|---|---|---|---|
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 3 | M | 3 |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3 | M | 3 |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / DESPOJO DE INFORMACIÓN. | 1 | B | 4 | M+ | 4 |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4 | M+ | 8 |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / FALTA DE MANTENIMIENTO. | 3 | M | 4 | M+ | 12 |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4 | M+ | 4 |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4 | M+ | 4 |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / INCENDIO | 1 | B | 5 | A | 5 |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3 | M | 9 |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / TEMBLOR | 1 | B | 5 | A | 5 |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / TÉCNICOS QUE NO SON IDÓNEOS. | 2 | M- | 2 | M- | 4 |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / PÉRDIDA DE EQUIPOS. | 1 | B | 3 | M | 3 |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / CARENCIA DE UNA | 3 | M | 3 | M | 9 |

| | | | | | |
|---|---|---|---|---|---|
| METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | | | | | |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / TERRORISMO. | 1 | B | 5 | A | 5 |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 3 | M | 3 |
| EQUIPOS DE GRABACIÓN (LLAMADAS) /PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3 | M | 3 |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / DESPOJO DE INFORMACIÓN. | 1 | B | 4 | M+ | 4 |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4 | M+ | 8 |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / FALTA DE MANTENIMIENTO. | 3 | M | 4 | M+ | 12 |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4 | M+ | 4 |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4 | M+ | 4 |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / INCENDIO | 1 | B | 5 | A | 5 |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / INCONVENIENTES ELÉCTRICOS. | 3 | M | 4 | M+ | 12 |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / TEMBLOR | 1 | B | 5 | A | 5 |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / TÉCNICOS QUE NO SON IDÓNEOS. | 2 | M- | 2 | M- | 4 |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / PÉRDIDA DE EQUIPOS. | 1 | B | 3 | M | 3 |

| | | | | | |
|---|---|---|---|---|---|
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 3 | M | 3 | M | 9 |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / TERRORISMO. | 1 | B | 5 | A | 5 |
| PLANTA TELEFÓNICA / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 4 | M+ | 4 |
| PLANTA TELEFÓNICA / MALA INSTALACIÓN EN EL CABLEADO. | 3 | M | 3 | M | 9 |
| PLANTA TELEFÓNICA / FALTA DE MANTENIMIENTO. | 2 | M- | 1 | B | 2 |
| PLANTA TELEFÓNICA / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 1 | B | 1 |
| PLANTA TELEFÓNICA / INCENDIO | 1 | B | 5 | A | 5 |
| PLANTA TELEFÓNICA / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3 | M | 9 |
| PLANTA TELEFÓNICA / TEMBLOR | 1 | B | 5 | A | 5 |
| PLANTA TELEFÓNICA / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2 | M- | 6 |
| PLANTA TELEFÓNICA / PÉRDIDA DE EQUIPOS. | 1 | B | 2 | M- | 2 |
| PLANTA TELEFÓNICA / TERRORISMO. | 1 | B | 5 | A | 5 |
| WINDOWS 7, 8 Y 10 / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 5 | A | 10 |
| WINDOWS 7, 8 Y 10 / DESPOJO DE INFORMACIÓN. | 1 | B | 3 | M | 3 |
| WINDOWS 7, 8 Y 10 / INEXISTENCIA DE PARCHES. | 1 | B | 2 | M- | 2 |
| WINDOWS 7, 8 Y 10 / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 2 | M- | 5 | A | 10 |
| WINDOWS 7, 8 Y 10 / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 3 | M | 3 |
| WINDOWS 7, 8 Y 10 / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3 | M | 6 |

| | | | | | |
|---|---|---|---|---|---|
| WINDOWS 7, 8 Y 10 / TÉCNICOS QUE NO SON IDÓNEOS. | 2 | M- | 4 | M+ | 8 |
| WINDOWS 7, 8 Y 10 / PÉRDIDA DE EQUIPOS. | 1 | B | 5 | A | 5 |
| WINDOWS 7, 8 Y 10 / TERRORISMO. | 1 | B | 5 | A | 5 |
| WINDOWS SERVER 2012 / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 4 | M+ | 8 |
| WINDOWS SERVER 2012 / DESPOJO DE INFORMACIÓN. | 1 | B | 3 | M | 3 |
| WINDOWS SERVER 2012 / INEXISTENCIA DE PARCHES. | 1 | B | 2 | M- | 2 |
| WINDOWS SERVER 2012 / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 4 | M+ | 4 |
| WINDOWS SERVER 2012 / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 2 | M- | 2 |
| WINDOWS SERVER 2012 / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 2 | M- | 2 |
| WINDOWS SERVER 2012 / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3 | M | 9 |
| WINDOWS SERVER 2012 / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4 | M+ | 12 |
| WINDOWS SERVER 2012 / PÉRDIDA DE EQUIPOS. | 2 | M- | 5 | A | 10 |
| WINDOWS SERVER 2012 / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 3 | M | 4 | M+ | 12 |
| WINDOWS SERVER 2012 / TERRORISMO. | 1 | B | 5 | A | 5 |
| BASES DE DATOS SQL SERVER 2014 / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 4 | M+ | 8 |
| BASES DE DATOS SQL SERVER 2014/ DESPOJO DE INFORMACIÓN. | 1 | B | 3 | M | 3 |
| BASES DE DATOS SQL SERVER 2014/ INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 1 | B | 1 |

| | | | | | |
|---|---|---|---|---|---|
| BASES DE DATOS SQL SERVER 2014/ ELIMINACIÓN Y MODIFICACIÓN. | 2 | M- | 3 | M | 6 |
| BASES DE DATOS SQL SERVER 2014/ INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3 | M | 6 |
| BASES DE DATOS SQL SERVER 2014/ TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 3 | M | 9 |
| BASES DE DATOS SQL SERVER 2014/ PÉRDIDA DE EQUIPOS. | 2 | M- | 4 | M+ | 8 |
| BASES DE DATOS SQL SERVER 2014/ CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 3 | M | 4 | M+ | 12 |
| BASES DE DATOS SQL SERVER 2014/ TERRORISMO. | 1 | B | 5 | A | 5 |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 4 | M+ | 8 |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / DESPOJO DE INFORMACIÓN. | 3 | M | 5 | A | 15 |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / MALA INSTALACIÓN EN EL CABLEADO. | 3 | M | 4 | M+ | 12 |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / FALTA DE MANTENIMIENTO. | 4 | M+ | 4 | M+ | 16 |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 3 | M | 6 |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / INCAPACIDAD. | 2 | M- | 4 | M+ | 8 |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / SALIDA DE PERSONAL. | 2 | M- | 4 | M+ | 8 |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / ELIMINACIÓN Y MODIFICACIÓN. | 2 | M- | 4 | M+ | 8 |

| | | | | | |
|---|---|---|---|---|---|
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / INCENDIO | 1 | B | 5 | A | 5 |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3 | M | 6 |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / TEMBLOR | 1 | B | 5 | A | 5 |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / TÉCNICOS QUE NO SON IDÓNEOS. | 4 | M+ | 5 | A | 20 |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 3 | M | 4 | M+ | 12 |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / TERRORISMO. | 1 | B | 5 | A | 5 |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4 | M+ | 4 |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / DESPOJO DE INFORMACIÓN. | 2 | M- | 4 | M+ | 8 |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / INCAPACIDAD. | 2 | M- | 3 | M | 6 |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / ELIMINACIÓN Y MODIFICACIÓN. | 3 | M | 3 | M | 9 |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / DELEGACIÓN DE RESPONSABILIDADES. | 2 | M- | 3 | M | 6 |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / PÉRDIDA DE EQUIPOS. | 2 | M- | 4 | M+ | 8 |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / TERRORISMO. | 1 | B | 5 | A | 5 |

| | | | | | |
|---|---|---|---|---|---|
| ANTIVIRUS: TREND MICRO / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4 | M+ | 4 |
| ANTIVIRUS: TREND MICRO / DESPOJO DE INFORMACIÓN. | 1 | B | 4 | M+ | 4 |
| ANTIVIRUS: TREND MICRO / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 3 | M | 6 |
| ANTIVIRUS: TREND MICRO / FALTA DE MANTENIMIENTO. | 3 | M | 4 | M+ | 12 |
| ANTIVIRUS: TREND MICRO / INEXISTENCIA DE PARCHES. | 1 | B | 2 | M- | 2 |
| ANTIVIRUS: TREND MICRO / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 4 | M+ | 4 |
| ANTIVIRUS: TREND MICRO / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4 | M+ | 4 |
| ANTIVIRUS: TREND MICRO / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3 | M | 9 |
| ANTIVIRUS: TREND MICRO / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4 | M+ | 12 |
| ANTIVIRUS: TREND MICRO / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| ANTIVIRUS: TREND MICRO / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 3 | M | 3 | M | 9 |
| ANTIVIRUS: TREND MICRO / TERRORISMO. | 1 | B | 4 | M+ | 4 |
| OFIMÁTICA: OFFICE 365 / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 4 | M+ | 8 |
| OFIMÁTICA: OFFICE 365 / DESPOJO DE INFORMACIÓN. | 1 | B | 4 | M+ | 4 |
| OFIMÁTICA: OFFICE 365 / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 3 | M | 6 |
| OFIMÁTICA: OFFICE 365 / FALTA DE MANTENIMIENTO. | 1 | B | 1 | B | 1 |
| OFIMÁTICA: OFFICE 365 / INEXISTENCIA DE PARCHES. | 1 | B | 2 | M- | 2 |

| | | | | | |
|---|---|---|---|---|---|
| OFIMÁTICA: OFFICE 365 / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 4 | M+ | 4 |
| OFIMÁTICA: OFFICE 365 / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4 | M+ | 4 |
| OFIMÁTICA: OFFICE 365 / ELIMINACIÓN Y MODIFICACIÓN. | 3 | M | 4 | M+ | 12 |
| OFIMÁTICA: OFFICE 365 / TÉCNICOS QUE NO SON IDÓNEOS. | 2 | M- | 3 | M | 6 |
| OFIMÁTICA: OFFICE 365 / PÉRDIDA DE EQUIPOS. | 1 | B | 3 | M | 3 |
| OFIMÁTICA: OFFICE 365 / TERRORISMO. | 1 | B | 4 | M+ | 4 |
| WEBSERVER. II / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 3 | M | 4 | M+ | 12 |
| WEBSERVER. II / DESPOJO DE INFORMACIÓN. | 2 | M- | 4 | M+ | 8 |
| WEBSERVER. II / MALA INSTALACIÓN EN EL CABLEADO. | 3 | M | 2 | M- | 6 |
| WEBSERVER. II / FALTA DE MANTENIMIENTO. | 2 | M- | 3 | M | 6 |
| WEBSERVER. II / INEXISTENCIA DE PARCHES. | 2 | M- | 4 | M+ | 8 |
| WEBSERVER. II / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 2 | M- | 4 | M+ | 8 |
| WEBSERVER. II / ELIMINACIÓN Y MODIFICACIÓN. | 2 | M- | 4 | M+ | 8 |
| WEBSERVER. II / INCONVENIENTES ELÉCTRICOS. | 3 | M | 4 | M+ | 12 |
| WEBSERVER. II / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2 | M- | 6 |
| WEBSERVER. II / PÉRDIDA DE EQUIPOS. | 1 | B | 1 | B | 1 |
| WEBSERVER. II / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 4 | M+ | 3 | M | 12 |
| WEBSERVER. II / TERRORISMO. | 1 | B | 5 | A | 5 |
| POSICIONAMIENTO: GOOGLE MAPS / FALTA DE MANTENIMIENTO. | 1 | B | 1 | B | 1 |

| | | | | | |
|---|---|---|---|---|---|
| COMUNICACIONES: MOTO TRB / FALTA DE MANTENIMIENTO. | 2 | M- | 3 | M | 6 |
| COMUNICACIONES: MOTO TRB / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4 | M+ | 4 |
| COMUNICACIONES: MOTO TRB / SALIDA DE PERSONAL. | 3 | M | 2 | M- | 6 |
| COMUNICACIONES: MOTO TRB / INCENDIO | 1 | B | 4 | M+ | 4 |
| COMUNICACIONES: MOTO TRB / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3 | M | 9 |
| COMUNICACIONES: MOTO TRB / TEMBLOR | 1 | B | 4 | M+ | 4 |
| COMUNICACIONES: MOTO TRB / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4 | M+ | 12 |
| COMUNICACIONES: MOTO TRB / PÉRDIDA DE EQUIPOS. | 2 | M- | 3 | M | 6 |
| COMUNICACIONES: MOTO TRB / TERRORISMO. | 1 | B | 4 | M+ | 4 |
| BASES DE DATOS CORPORATIVAS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 5 | A | 10 |
| BASES DE DATOS CORPORATIVAS / DESPOJO DE INFORMACIÓN. | 2 | M- | 5 | A | 10 |
| BASES DE DATOS CORPORATIVAS / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 4 | M+ | 4 |
| BASES DE DATOS CORPORATIVAS / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 4 | M+ | 8 |
| BASES DE DATOS CORPORATIVAS / ELIMINACIÓN Y MODIFICACIÓN. | 3 | M | 3 | M | 9 |
| BASES DE DATOS CORPORATIVAS / INCENDIO | 1 | B | 5 | A | 5 |
| BASES DE DATOS CORPORATIVAS / INCONVENIENTES ELÉCTRICOS. | 1 | B | 3 | M | 3 |
| BASES DE DATOS CORPORATIVAS / TEMBLOR | 1 | B | 5 | A | 5 |
| BASES DE DATOS CORPORATIVAS / PÉRDIDA DE EQUIPOS. | 1 | B | 5 | A | 5 |

| | | | | | |
|---|---|---|---|---|---|
| BASES DE DATOS CORPORATIVAS / TERRORISMO. | 1 | B | 5 | A | 5 |
| BASE DE DATOS CONTABLES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4 | M+ | 4 |
| BASE DE DATOS CONTABLES / DESPOJO DE INFORMACIÓN. | 3 | M | 4 | M+ | 12 |
| BASE DE DATOS CONTABLES / FALTA DE MANTENIMIENTO. | 1 | B | 4 | M+ | 4 |
| BASE DE DATOS CONTABLES / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 4 | M+ | 8 |
| BASE DE DATOS CONTABLES / SALIDA DE PERSONAL. | 1 | B | 4 | M+ | 4 |
| BASE DE DATOS CONTABLES / ELIMINACIÓN Y MODIFICACIÓN. | 3 | M | 4 | M+ | 12 |
| BASE DE DATOS CONTABLES / INCENDIO | 1 | B | 4 | M+ | 4 |
| BASE DE DATOS CONTABLES / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3 | M | 6 |
| BASE DE DATOS CONTABLES / TEMBLOR | 1 | B | 4 | M+ | 4 |
| BASE DE DATOS CONTABLES / TÉCNICOS QUE NO SON IDÓNEOS. | 4 | M+ | 5 | A | 20 |
| BASE DE DATOS CONTABLES / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| BASE DE DATOS CONTABLES / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 3 | M | 4 | M+ | 12 |
| BASE DE DATOS CONTABLES / TERRORISMO. | 1 | B | 5 | A | 5 |
| BASE DE DATOS CLIENTES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4 | M+ | 4 |
| BASE DE DATOS CLIENTES / DESPOJO DE INFORMACIÓN. | 2 | M- | 5 | A | 10 |
| BASE DE DATOS CLIENTES / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 2 | M- | 2 |

| | | | | | |
|---|---|---|---|---|---|
| BASE DE DATOS CLIENTES / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 4 | M+ | 8 |
| BASE DE DATOS CLIENTES / SALIDA DE PERSONAL. | 4 | M+ | 5 | A | 20 |
| BASE DE DATOS CLIENTES / ELIMINACIÓN Y MODIFICACIÓN. | 4 | M+ | 4 | M+ | 16 |
| BASE DE DATOS CLIENTES / INCENDIO | 1 | B | 4 | M+ | 4 |
| BASE DE DATOS CLIENTES / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3 | M | 9 |
| BASE DE DATOS CLIENTES / TEMBLOR | 1 | B | 4 | M+ | 4 |
| BASE DE DATOS CLIENTES / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| BASE DE DATOS CLIENTES / TERRORISMO. | 1 | B | 5 | A | 5 |
| BASES DE DATOS INSPECCIONES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4 | M+ | 4 |
| BASES DE DATOS INSPECCIONES / DESPOJO DE INFORMACIÓN. | 2 | M- | 5 | A | 10 |
| BASES DE DATOS INSPECCIONES / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 2 | M- | 2 |
| BASES DE DATOS INSPECCIONES / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 4 | M+ | 8 |
| BASES DE DATOS INSPECCIONES / SALIDA DE PERSONAL. | 4 | M+ | 5 | A | 20 |
| BASES DE DATOS INSPECCIONES / ELIMINACIÓN Y MODIFICACIÓN. | 4 | M+ | 4 | M+ | 16 |
| BASES DE DATOS INSPECCIONES / INCENDIO | 1 | B | 4 | M+ | 4 |
| BASES DE DATOS INSPECCIONES / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3 | M | 9 |
| BASES DE DATOS INSPECCIONES / TEMBLOR | 1 | B | 4 | M+ | 4 |
| BASES DE DATOS INSPECCIONES / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |

| | | | | | |
|---|---|---|---|---|---|
| BASES DE DATOS INSPECCIONES / TERRORISMO. | 1 | B | 5 | A | 5 |
| BASES DE DATOS INVENTARIOS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4 | M+ | 4 |
| BASES DE DATOS INVENTARIOS / DESPOJO DE INFORMACIÓN. | 2 | M- | 5 | A | 10 |
| BASES DE DATOS INVENTARIOS / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 2 | M- | 2 |
| BASES DE DATOS INVENTARIOS / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 4 | M+ | 8 |
| BASES DE DATOS INVENTARIOS / SALIDA DE PERSONAL. | 4 | M+ | 5 | A | 20 |
| BASES DE DATOS INVENTARIOS / ELIMINACIÓN Y MODIFICACIÓN. | 4 | M+ | 4 | M+ | 16 |
| BASES DE DATOS INVENTARIOS / INCENDIO | 1 | B | 4 | M+ | 4 |
| BASES DE DATOS INVENTARIOS / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3 | M | 9 |
| BASES DE DATOS INVENTARIOS / TEMBLOR | 1 | B | 4 | M+ | 4 |
| BASES DE DATOS INVENTARIOS / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| BASES DE DATOS INVENTARIOS / TERRORISMO. | 1 | B | 5 | A | 5 |
| BASES DE DATOS EMERGENCIAS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4 | M+ | 4 |
| BASES DE DATOS EMERGENCIAS / DESPOJO DE INFORMACIÓN. | 2 | M- | 5 | A | 10 |
| BASES DE DATOS EMERGENCIAS / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 2 | M- | 2 |
| BASES DE DATOS EMERGENCIAS / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 4 | M+ | 8 |
| BASES DE DATOS EMERGENCIAS / SALIDA DE PERSONAL. | 4 | M+ | 5 | A | 20 |

| | | | | | |
|---|---|---|---|---|---|
| BASES DE DATOS EMERGENCIAS / ELIMINACIÓN Y MODIFICACIÓN. | 4 | M+ | 4 | M+ | 16 |
| BASES DE DATOS EMERGENCIAS / INCENDIO | 1 | B | 4 | M+ | 4 |
| BASES DE DATOS EMERGENCIAS / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3 | M | 9 |
| BASES DE DATOS EMERGENCIAS / TEMBLOR | 1 | B | 4 | M+ | 4 |
| BASES DE DATOS EMERGENCIAS / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| BASES DE DATOS EMERGENCIAS / TERRORISMO. | 1 | B | 5 | A | 5 |
| BACKUPS DE CONTABILIDAD / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4 | M+ | 4 |
| BACKUPS DE CONTABILIDAD / DESPOJO DE INFORMACIÓN. | 2 | M- | 5 | A | 10 |
| BACKUPS DE CONTABILIDAD / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 2 | M- | 2 |
| BACKUPS DE CONTABILIDAD / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 4 | M+ | 8 |
| BACKUPS DE CONTABILIDAD / SALIDA DE PERSONAL. | 4 | M+ | 5 | A | 20 |
| BACKUPS DE CONTABILIDAD / ELIMINACIÓN Y MODIFICACIÓN. | 4 | M+ | 4 | M+ | 16 |
| BACKUPS DE CONTABILIDAD / INCENDIO | 1 | B | 4 | M+ | 4 |
| BACKUPS DE CONTABILIDAD / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3 | M | 9 |
| BACKUPS DE CONTABILIDAD / TEMBLOR | 1 | B | 4 | M+ | 4 |
| BACKUPS DE CONTABILIDAD / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| BACKUPS DE CONTABILIDAD / TERRORISMO. | 1 | B | 4 | M+ | 4 |
| RED DE DATOS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 5 | A | 5 |

| | | | | | |
|---|---|---|---|---|---|
| RED DE DATOS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 2 | M- | 3 | M | 6 |
| RED DE DATOS / DESPOJO DE INFORMACIÓN. | 1 | B | 4 | M+ | 4 |
| RED DE DATOS / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 5 | A | 10 |
| RED DE DATOS / FALTA DE MANTENIMIENTO. | 3 | M | 4 | M+ | 12 |
| RED DE DATOS / INCENDIO | 1 | B | 5 | A | 5 |
| RED DE DATOS / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3 | M | 6 |
| RED DE DATOS / TEMBLOR | 1 | B | 5 | A | 5 |
| RED DE DATOS / TÉCNICOS QUE NO SON IDÓNEOS. | 4 | M+ | 4 | M+ | 16 |
| RED DE DATOS / TERRORISMO. | 1 | B | 5 | A | 5 |
| RED RADIO COMUNICACIONES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3 | M | 3 |
| RED RADIO COMUNICACIONES / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4 | M+ | 8 |
| RED RADIO COMUNICACIONES / FALTA DE MANTENIMIENTO. | 2 | M- | 4 | M+ | 8 |
| RED RADIO COMUNICACIONES / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 3 | M | 3 |
| RED RADIO COMUNICACIONES / INCENDIO | 1 | B | 5 | A | 5 |
| RED RADIO COMUNICACIONES / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 4 | M+ | 8 |
| RED RADIO COMUNICACIONES / TEMBLOR | 1 | B | 5 | A | 5 |
| RED RADIO COMUNICACIONES / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 3 | M | 9 |
| RED RADIO COMUNICACIONES / PÉRDIDA DE EQUIPOS. | 1 | B | 5 | A | 5 |
| RED RADIO COMUNICACIONES / TERRORISMO. | 1 | B | 5 | A | 5 |

| | | | | | |
|---|---|---|---|---|---|
| ACCESO A INTERNET / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4 | M+ | 4 |
| ACCESO A INTERNET / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 4 | M+ | 4 |
| ACCESO A INTERNET / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 5 | A | 10 |
| ACCESO A INTERNET / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4 | M+ | 4 |
| ACCESO A INTERNET / INCENDIO | 1 | B | 5 | A | 5 |
| ACCESO A INTERNET / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3 | M | 6 |
| ACCESO A INTERNET / TEMBLOR | 1 | B | 5 | A | 5 |
| ACCESO A INTERNET / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4 | M+ | 12 |
| ACCESO A INTERNET / PÉRDIDA DE EQUIPOS. | 1 | B | 5 | A | 5 |
| ACCESO A INTERNET / TERRORISMO. | 1 | B | 5 | A | 5 |
| INTERNET / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 2 | M- | 2 |
| INTERNET / DESPOJO DE INFORMACIÓN. | 1 | B | 5 | A | 5 |
| INTERNET / ELIMINACIÓN Y MODIFICACIÓN. | 2 | M- | 4 | M+ | 8 |
| INTERNET / INCENDIO | 1 | B | 5 | A | 5 |
| INTERNET / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 1 | B | 2 |
| INTERNET / TEMBLOR | 1 | B | 5 | A | 5 |
| INTERNET / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4 | M+ | 12 |
| INTERNET / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| INTERNET / TERRORISMO. | 1 | B | 5 | A | 5 |

| | | | | | |
|---|---|---|---|---|---|
| INTRANET / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 2 | M- | 2 |
| INTRANET / DESPOJO DE INFORMACIÓN. | 1 | B | 5 | A | 5 |
| INTRANET / INCENDIO | 1 | B | 5 | A | 5 |
| INTRANET / INCONVENIENTES ELÉCTRICOS. | 1 | B | 3 | M | 3 |
| INTRANET / TEMBLOR | 1 | B | 5 | A | 5 |
| INTRANET / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4 | M+ | 12 |
| INTRANET / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| INTRANET / TERRORISMO. | 1 | B | 5 | A | 5 |
| TELEFONIA / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 4 | M+ | 4 |
| TELEFONIA / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 3 | M | 6 |
| TELEFONIA / FALTA DE MANTENIMIENTO. | 2 | M- | 3 | M | 6 |
| TELEFONIA / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 2 | M- | 2 |
| TELEFONIA / INCENDIO | 1 | B | 5 | A | 5 |
| TELEFONIA / INCONVENIENTES ELÉCTRICOS. | 3 | M | 2 | M- | 6 |
| TELEFONIA / TEMBLOR | 1 | B | 5 | A | 5 |
| TELEFONIA / TÉCNICOS QUE NO SON IDÓNEOS. | 2 | M- | 4 | M+ | 8 |
| TELEFONIA / PÉRDIDA DE EQUIPOS. | 1 | B | 3 | M | 3 |
| TELEFONIA / TERRORISMO. | 1 | B | 5 | A | 5 |
| RADIOS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3 | M | 3 |
| RADIOS / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4 | M+ | 8 |

| | | | | | |
|---|---|---|---|---|---|
| RADIOS / FALTA DE MANTENIMIENTO. | 2 | M- | 3 | M | 6 |
| RADIOS / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 3 | M | 3 |
| RADIOS / INCENDIO | 1 | B | 5 | A | 5 |
| RADIOS / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3 | M | 6 |
| RADIOS / TEMBLOR | 1 | B | 5 | A | 5 |
| RADIOS / TÉCNICOS QUE NO SON IDÓNEOS. | 2 | M- | 1 | B | 2 |
| RADIOS / PÉRDIDA DE EQUIPOS. | 1 | B | 5 | A | 5 |
| RADIOS / TERRORISMO. | 1 | B | 5 | A | 5 |
| SISTEMA DE ALIMENTACIÓN UPS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3 | M | 3 |
| SISTEMA DE ALIMENTACIÓN UPS / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4 | M+ | 8 |
| SISTEMA DE ALIMENTACIÓN UPS / FALTA DE MANTENIMIENTO. | 3 | M | 3 | M | 9 |
| SISTEMA DE ALIMENTACIÓN UPS / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4 | M+ | 4 |
| SISTEMA DE ALIMENTACIÓN UPS / INCENDIO | 1 | B | 5 | A | 5 |
| SISTEMA DE ALIMENTACIÓN UPS / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3 | M | 6 |
| SISTEMA DE ALIMENTACIÓN UPS / TEMBLOR | 1 | B | 5 | A | 5 |
| SISTEMA DE ALIMENTACIÓN UPS / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2 | M- | 6 |
| SISTEMA DE ALIMENTACIÓN UPS / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| SISTEMA DE ALIMENTACIÓN UPS / TERRORISMO. | 1 | B | 5 | A | 5 |

| | | | | | |
|---|---|---|---|---|---|
| RADIOS PORTATILES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3 | M | 3 |
| RADIOS PORTATILES / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4 | M+ | 8 |
| RADIOS PORTATILES / FALTA DE MANTENIMIENTO. | 3 | M | 3 | M | 9 |
| RADIOS PORTATILES / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4 | M+ | 4 |
| RADIOS PORTATILES / INCENDIO | 1 | B | 5 | A | 5 |
| RADIOS PORTATILES / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3 | M | 6 |
| RADIOS PORTATILES / TEMBLOR | 1 | B | 5 | A | 5 |
| RADIOS PORTATILES / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2 | M- | 6 |
| RADIOS PORTATILES / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| RADIOS PORTATILES / TERRORISMO. | 1 | B | 5 | A | 5 |
| RADIOS MOVILES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3 | M | 3 |
| RADIOS MOVILES / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4 | M+ | 8 |
| RADIOS MOVILES / FALTA DE MANTENIMIENTO. | 3 | M | 3 | M | 9 |
| RADIOS MOVILES / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4 | M+ | 4 |
| RADIOS MOVILES / INCENDIO | 1 | B | 5 | A | 5 |
| RADIOS MOVILES / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3 | M | 6 |
| RADIOS MOVILES / TEMBLOR | 1 | B | 5 | A | 5 |
| RADIOS MOVILES / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2 | M- | 6 |
| RADIOS MOVILES / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| RADIOS MOVILES / TERRORISMO. | 1 | B | 5 | A | 5 |

| | | | | | |
|---|---|---|---|---|---|
| RADIO BASE / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3 | M | 3 |
| RADIO BASE / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4 | M+ | 8 |
| RADIO BASE / FALTA DE MANTENIMIENTO. | 3 | M | 3 | M | 9 |
| RADIO BASE / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4 | M+ | 4 |
| RADIO BASE / INCENDIO | 1 | B | 5 | A | 5 |
| RADIO BASE / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3 | M | 6 |
| RADIO BASE / TEMBLOR | 1 | B | 5 | A | 5 |
| RADIO BASE / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2 | M- | 6 |
| RADIO BASE / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| RADIO BASE / TERRORISMO. | 1 | B | 5 | A | 5 |
| REPETIDORAS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3 | M | 3 |
| REPETIDORAS / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4 | M+ | 8 |
| REPETIDORAS / FALTA DE MANTENIMIENTO. | 3 | M | 3 | M | 9 |
| REPETIDORAS / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4 | M+ | 4 |
| REPETIDORAS / INCENDIO | 1 | B | 5 | A | 5 |
| REPETIDORAS / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3 | M | 6 |
| REPETIDORAS / TEMBLOR | 1 | B | 5 | A | 5 |
| REPETIDORAS / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2 | M- | 6 |
| REPETIDORAS / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| REPETIDORAS / TERRORISMO. | 1 | B | 5 | A | 5 |

| | | | | | |
|---|---|---|---|---|---|
| ANTENAS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3 | M | 3 |
| ANTENAS / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4 | M+ | 8 |
| ANTENAS / FALTA DE MANTENIMIENTO. | 3 | M | 3 | M | 9 |
| ANTENAS / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4 | M+ | 4 |
| ANTENAS / INCENDIO | 1 | B | 5 | A | 5 |
| INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3 | M | 6 |
| ANTENAS / TEMBLOR | 1 | B | 5 | A | 5 |
| ANTENAS / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2 | M- | 6 |
| ANTENAS / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| ANTENAS / TERRORISMO. | 1 | B | 5 | A | 5 |
| OPERATIVOS (BOMBEROS) / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 5 | A | 5 |
| OPERATIVOS (BOMBEROS) / DESPOJO DE INFORMACIÓN. | 2 | M- | 2 | M- | 4 |
| OPERATIVOS (BOMBEROS) / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4 | M+ | 8 |
| OPERATIVOS (BOMBEROS) / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 5 | A | 5 |
| OPERATIVOS (BOMBEROS) / INCAPACIDAD. | 2 | M- | 4 | M+ | 8 |
| OPERATIVOS (BOMBEROS) / SALIDA DE PERSONAL. | 2 | M- | 4 | M+ | 8 |
| OPERATIVOS (BOMBEROS) / INCENDIO | 1 | B | 5 | A | 5 |
| OPERATIVOS (BOMBEROS) / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 4 | M+ | 8 |
| OPERATIVOS (BOMBEROS) / TEMBLOR | 1 | B | 5 | A | 5 |

| | | | | | |
|---|---|---|---|---|---|
| OPERATIVOS (BOMBEROS) / FALTA DE MOTIVACIÓN. | 2 | M- | 4 | M+ | 8 |
| OPERATIVOS (BOMBEROS) / DELEGACIÓN DE RESPONSABILIDADES. | 3 | M | 4 | M+ | 12 |
| OPERATIVOS (BOMBEROS) / PÉRDIDA DE EQUIPOS. | 2 | M- | 3 | M | 6 |
| OPERATIVOS (BOMBEROS) / TERRORISMO. | 1 | B | 5 | A | 5 |
| ADMINISTRATIVOS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4 | M+ | 4 |
| ADMINISTRATIVOS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 5 | A | 5 |
| ADMINISTRATIVOS / DESPOJO DE INFORMACIÓN. | 2 | M- | 4 | M+ | 8 |
| ADMINISTRATIVOS / MALA INSTALACIÓN EN EL CABLEADO. | 3 | M | 4 | M+ | 12 |
| ADMINISTRATIVOS / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 2 | M- | 2 |
| ADMINISTRATIVOS / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 3 | M | 6 |
| ADMINISTRATIVOS / INCAPACIDAD. | 2 | M- | 4 | M+ | 8 |
| ADMINISTRATIVOS / SALIDA DE PERSONAL. | 2 | M- | 4 | M+ | 8 |
| ADMINISTRATIVOS / INCENDIO | 1 | B | 5 | A | 5 |
| ADMINISTRATIVOS / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 4 | M+ | 8 |
| ADMINISTRATIVOS / TEMBLOR | 1 | B | 5 | A | 5 |
| ADMINISTRATIVOS / FALTA DE MOTIVACIÓN. | 3 | M | 4 | M+ | 12 |
| ADMINISTRATIVOS / DELEGACIÓN DE RESPONSABILIDADES. | 4 | M+ | 3 | M | 12 |
| ADMINISTRATIVOS / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4 | M+ | 12 |

| | | | | | |
|---|---|---|---|---|---|
| ADMINISTRATIVOS / PÉRDIDA DE EQUIPOS. | 2 | M- | 4 | M+ | 8 |
| ADMINISTRATIVOS / TERRORISMO. | 1 | B | 5 | A | 5 |
| SOPORTE EXTERNO / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 5 | A | 5 |
| SOPORTE EXTERNO / DESPOJO DE INFORMACIÓN. | 2 | M- | 4 | M+ | 8 |
| SOPORTE EXTERNO / MALA INSTALACIÓN EN EL CABLEADO. | 3 | M | 4 | M+ | 12 |
| SOPORTE EXTERNO / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 2 | M- | 2 |
| SOPORTE EXTERNO / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 3 | M | 6 |
| SOPORTE EXTERNO / INCAPACIDAD. | 2 | M- | 4 | M+ | 8 |
| SOPORTE EXTERNO / SALIDA DE PERSONAL. | 2 | M- | 4 | M+ | 8 |
| SOPORTE EXTERNO / INCENDIO | 1 | B | 5 | A | 5 |
| SOPORTE EXTERNO / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 4 | M+ | 8 |
| SOPORTE EXTERNO / TEMBLOR | 1 | B | 5 | A | 5 |
| SOPORTE EXTERNO / FALTA DE MOTIVACIÓN. | 3 | M | 4 | M+ | 12 |
| SOPORTE EXTERNO / DELEGACIÓN DE RESPONSABILIDADES. | 4 | M+ | 3 | M | 12 |
| SOPORTE EXTERNO / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4 | M+ | 12 |
| SOPORTE EXTERNO / PÉRDIDA DE EQUIPOS. | 2 | M- | 4 | M+ | 8 |
| SOPORTE EXTERNO / TERRORISMO. | 1 | B | 5 | A | 5 |
| ARCHIVO FISÏCO IMPRESO / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 5 | A | 5 |
| ARCHIVO FISÏCO IMPRESO / DESPOJO DE INFORMACIÓN. | 2 | M- | 5 | A | 10 |

| | | | | | |
|---|---|---|---|---|---|
| ARCHIVO FISÏCO IMPRESO / FALTA DE MANTENIMIENTO. | 3 | M | 4 | M+ | 12 |
| ARCHIVO FISÏCO IMPRESO / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 1 | B | 2 |
| ARCHIVO FISÏCO IMPRESO / SALIDA DE PERSONAL. | 2 | M- | 3 | M | 6 |
| ARCHIVO FISÏCO IMPRESO / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 5 | A | 5 |
| ARCHIVO FISÏCO IMPRESO / INCENDIO | 1 | B | 5 | A | 5 |
| ARCHIVO FISÏCO IMPRESO / INCONVENIENTES ELÉCTRICOS. | 3 | M | 2 | M- | 6 |
| ARCHIVO FISÏCO IMPRESO / TEMBLOR | 1 | B | 5 | A | 5 |
| ARCHIVO FISÏCO IMPRESO / DELEGACIÓN DE RESPONSABILIDADES. | 3 | M | 4 | M+ | 12 |
| ARCHIVO FISÏCO IMPRESO / TERRORISMO. | 1 | B | 5 | A | 5 |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 4 | M+ | 8 |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3 | M | 3 |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / DESPOJO DE INFORMACIÓN. | 2 | M- | 5 | A | 10 |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 5 | A | 5 |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / SALIDA DE PERSONAL. | 3 | M | 5 | A | 15 |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4 | M+ | 4 |

| | | | | | |
|---|---|---|---|---|---|
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / INCENDIO | 1 | B | 5 | A | 5 |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / INCONVENIENTES ELÉCTRICOS. | 3 | M | 1 | B | 3 |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / TEMBLOR | 1 | B | 5 | A | 5 |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / TÉCNICOS QUE NO SON IDÓNEOS. | 4 | M+ | 3 | M | 12 |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / PÉRDIDA DE EQUIPOS. | 1 | B | 5 | A | 5 |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / TERRORISMO. | 1 | B | 5 | A | 5 |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 4 | M+ | 8 |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3 | M | 3 |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / DESPOJO DE INFORMACIÓN. | 2 | M- | 5 | A | 10 |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 5 | A | 5 |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / SALIDA DE PERSONAL. | 3 | M | 5 | A | 15 |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4 | M+ | 4 |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / INCENDIO | 1 | B | 5 | A | 5 |

| | | | | | |
|---|---|---|---|---|---|
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / INCONVENIENTES ELÉCTRICOS. | 3 | M | 1 | B | 3 |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / TEMBLOR | 1 | B | 5 | A | 5 |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / TÉCNICOS QUE NO SON IDÓNEOS. | 4 | M+ | 3 | M | 12 |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / TERRORISMO. | 1 | B | 5 | A | 5 |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 4 | M+ | 8 |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3 | M | 3 |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / DESPOJO DE INFORMACIÓN. | 2 | M- | 5 | A | 10 |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 5 | A | 5 |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / SALIDA DE PERSONAL. | 3 | M | 5 | A | 15 |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4 | M+ | 4 |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / INCENDIO | 1 | B | 5 | A | 5 |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / INCONVENIENTES ELÉCTRICOS. | 3 | M | 1 | B | 3 |

| | | | | | |
|---|---|---|---|---|---|
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / TEMBLOR | 1 | B | 5 | A | 5 |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / TÉCNICOS QUE NO SON IDÓNEOS. | 4 | M+ | 3 | M | 12 |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / PÉRDIDA DE EQUIPOS. | 1 | B | 4 | M+ | 4 |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / TERRORISMO. | 1 | B | 5 | A | 5 |
| ALMACENAMIENTO EN INTERNET (NUBE) / DESPOJO DE INFORMACIÓN. | 1 | B | 5 | A | 5 |
| ALMACENAMIENTO EN INTERNET (NUBE) / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 5 | A | 5 |
| ALMACENAMIENTO EN INTERNET (NUBE) / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4 | M+ | 4 |
| ALMACENAMIENTO EN INTERNET (NUBE) / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2 | M- | 6 |
| ALMACENAMIENTO EN INTERNET (NUBE) / TERRORISMO. | 1 | B | 5 | A | 5 |

Fuente: (Arango, 2016)

**Análisis.**

Gracias a la elaboración de la tabla del cálculo del riesgo, se logró reconocer de forma más clara el nivel de afectación que tiene la frecuencia y el impacto de operación, arrojando como resultado aquellos activos que se encuentran en una alta vulnerabilidad para la organización según los valores adquiridos de multiplicar la probabilidad por el impacto de operación. Producto de esta tabla, se realizó otra que agrupa la información según el estado que se encuentra y más adelante se observarán los activos contemplados como de más alto riesgo y de riesgo medio alto, los cuales serán los que requieren de manera más perentoria de un tratamiento debido al nivel de afectación que podría generar a la organización si alguno se llegara a presentar.

### 7.3.7. Impacto Potencial.

Una vez se han realizado los cálculos de la tabla anterior, se procede a determinar el impacto potencial, teniendo en cuenta los datos utilizados previamente desde la tabla del cálculo del riesgo. Es importante realizar este procedimiento puesto que contribuye a determinar los activos con sus respectivas amenazas que se encuentran más susceptibles a ser ejecutados y por lo tanto puedan poner en peligro los activos de la información en la entidad.

Para poder establecer el impacto potencial, en primer término se tiene en cuenta el grado de probabilidad de frecuencia o de ocurrencia que tiene la amenaza con el activo y en segundo término se debe tener en cuenta el impacto operativo el cual se relaciona con lo inherente al grado de afectación que tiene la amenaza con el activo en cuanto suceda, el resultado de estos dos ítems se multiplica y de esta forma se obtiene la puntuación de los activos que están expuestos a un alto nivel de afectación por las amenazas.

Por ejemplo: Si en primer término tenemos un riesgo que es frecuente se considera como alto y se representa con un porcentaje que está en el rango del 75% al 100% =5, en lugar de tomar el valor del porcentaje para determinar el riesgo más alto daremos una valoración que para este caso será una puntuación de cinco (ver tabla Nivel de frecuencia). En segundo término, si tenemos un riesgo alto en relación al impacto de operación se representa igualmente cuando su porcentaje está entre el 75% a 100%=5 y su valoración será de cinco puntos (ver tabla Impacto de operación). Teniendo en cuenta que si tenemos un riesgo alto en la probabilidad de frecuencia con la valoración de cinco y un impacto alto de operación con una valoración de cinco. Para continuar con la operación y poder determinar el riesgo más alto lo que debemos hacer es multiplicar las valoraciones equivalentes a los porcentajes lo que es igual a 5x5= 25 y así determinar en términos numéricos el riesgo más alto.

Es preciso volver a mencionar que: los activos y las amenazas que obtuvieron un resultado entre 16 y 25 serán considerados como “alto”, aquellos que alcanzaron un resultado entre 11 a 15 serán considerados como “medio alto”, por otra parte, los activos y amenazas que consiguieron un resultado entre 5 a 10 serán categorizados como “medio” y

los activos y amenazas que obtuvieron un valor entre 0 a 5, serán aquellos que pertenecen al nivel más bajo.

*Tabla 15: Clasificación Del Riesgo Según El Grado de Importancia.*

| ACTIVO / AMENAZA | PROBABILIDAD | | IMPACTO OPERACIÓN | | RIESGO (PROB.*IMPACTO) | TIPO DE RIESGO |
|---|---|---|---|---|---|---|
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / TÉCNICOS QUE NO SON IDÓNEOS. | 4 | M+ | 5,00 | A | 20 | ALTO |
| BASE DE DATOS CONTABLES / TÉCNICOS QUE NO SON IDÓNEOS. | 4 | M+ | 5,00 | A | 20 | ALTO |
| BASE DE DATOS CLIENTES / SALIDA DE PERSONAL. | 4 | M+ | 5,00 | A | 20 | ALTO |
| BASES DE DATOS INSPECCIONES / SALIDA DE PERSONAL. | 4 | M+ | 5,00 | A | 20 | ALTO |
| BASES DE DATOS INVENTARIOS / SALIDA DE PERSONAL. | 4 | M+ | 5,00 | A | 20 | ALTO |
| BASES DE DATOS EMERGENCIAS / SALIDA DE PERSONAL. | 4 | M+ | 5,00 | A | 20 | ALTO |
| BACKUPS DE CONTABILIDAD / SALIDA DE PERSONAL. | 4 | M+ | 5,00 | A | 20 | ALTO |
| EQUIPOS ESCRITORIO PORTATILES / FALTA DE MANTENIMIENTO. | 4 | M+ | 4,00 | M+ | 16 | ALTO |
| EQUIPOS ESCRITORIO PORTATILES / ELIMINACIÓN Y MODIFICACIÓN. | 4 | M+ | 4,00 | M+ | 16 | ALTO |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / FALTA DE MANTENIMIENTO. | 4 | M+ | 4,00 | M+ | 16 | ALTO |
| BASE DE DATOS CLIENTES / ELIMINACIÓN Y MODIFICACIÓN. | 4 | M+ | 4,00 | M+ | 16 | ALTO |
| BASES DE DATOS INSPECCIONES / ELIMINACIÓN Y MODIFICACIÓN. | 4 | M+ | 4,00 | M+ | 16 | ALTO |
| BASES DE DATOS INVENTARIOS / ELIMINACIÓN Y MODIFICACIÓN. | 4 | M+ | 4,00 | M+ | 16 | ALTO |
| BASES DE DATOS EMERGENCIAS / ELIMINACIÓN Y MODIFICACIÓN. | 4 | M+ | 4,00 | M+ | 16 | ALTO |
| BACKUPS DE CONTABILIDAD / ELIMINACIÓN Y MODIFICACIÓN. | 4 | M+ | 4,00 | M+ | 16 | ALTO |
| RED DE DATOS / TÉCNICOS QUE NO SON IDÓNEOS. | 4 | M+ | 4,00 | M+ | 16 | ALTO |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / DESPOJO DE INFORMACIÓN. | 3 | M | 5,00 | A | 15 | MEDIO ALTO |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / SALIDA DE PERSONAL. | 3 | M | 5,00 | A | 15 | MEDIO ALTO |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / SALIDA DE PERSONAL. | 3 | M | 5,00 | A | 15 | MEDIO ALTO |

| | | | | | | |
|---|---|---|---|---|---|---|
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / SALIDA DE PERSONAL. | 3 | M | 5,00 | A | 15 | MEDIO ALTO |
| ESTACIONES / TÉCNICOS QUE NO SON IDÓNEOS. | 4 | M+ | 3,00 | M | 12 | MEDIO ALTO |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / INCONVENIENTES ELÉCTRICOS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| EQUIPOS ESCRITORIO PORTATILES / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / FALTA DE MANTENIMIENTO. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / FALTA DE MANTENIMIENTO. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / INCONVENIENTES ELÉCTRICOS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| WINDOWS SERVER 2012 / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| WINDOWS SERVER 2012 / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| BASES DE DATOS SQL SERVER 2014/ CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / MALA INSTALACIÓN EN EL CABLEADO. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| ANTIVIRUS: TREND MICRO / FALTA DE MANTENIMIENTO. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| ANTIVIRUS: TREND MICRO / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| OFIMÁTICA: OFFICE 365 / ELIMINACIÓN Y MODIFICACIÓN. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| WEBSERVER. II / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| WEBSERVER. II / INCONVENIENTES ELÉCTRICOS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| WEBSERVER. II / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 4 | M+ | 3,00 | M | 12 | MEDIO ALTO |
| COMUNICACIONES: MOTO TRB / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| BASE DE DATOS CONTABLES / DESPOJO DE INFORMACIÓN. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| BASE DE DATOS CONTABLES / ELIMINACIÓN Y MODIFICACIÓN. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |

| | | | | | | |
|---|---|---|---|---|---|---|
| BASE DE DATOS CONTABLES / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| RED DE DATOS / FALTA DE MANTENIMIENTO. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| ACCESO A INTERNET / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| INTERNET / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| INTRANET / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| OPERATIVOS (BOMBEROS) / DELEGACIÓN DE RESPONSABILIDADES. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| ADMINISTRATIVOS / MALA INSTALACIÓN EN EL CABLEADO. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| ADMINISTRATIVOS / FALTA DE MOTIVACIÓN. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| ADMINISTRATIVOS / DELEGACIÓN DE RESPONSABILIDADES. | 4 | M+ | 3,00 | M | 12 | MEDIO ALTO |
| ADMINISTRATIVOS / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| SOPORTE EXTERNO / MALA INSTALACIÓN EN EL CABLEADO. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| SOPORTE EXTERNO / FALTA DE MOTIVACIÓN. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| SOPORTE EXTERNO / DELEGACIÓN DE RESPONSABILIDADES. | 4 | M+ | 3,00 | M | 12 | MEDIO ALTO |
| SOPORTE EXTERNO / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| ARCHIVO FISÏCO IMPRESO / FALTA DE MANTENIMIENTO. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| ARCHIVO FISÏCO IMPRESO / DELEGACIÓN DE RESPONSABILIDADES. | 3 | M | 4,00 | M+ | 12 | MEDIO ALTO |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / TÉCNICOS QUE NO SON IDÓNEOS. | 4 | M+ | 3,00 | M | 12 | MEDIO ALTO |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / TÉCNICOS QUE NO SON IDÓNEOS. | 4 | M+ | 3,00 | M | 12 | MEDIO ALTO |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / TÉCNICOS QUE NO SON IDÓNEOS. | 4 | M+ | 3,00 | M | 12 | MEDIO ALTO |
| WINDOWS 7, 8 Y 10 / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 5,00 | A | 10 | MEDIO |
| WINDOWS 7, 8 Y 10 / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 2 | M- | 5,00 | A | 10 | MEDIO |
| WINDOWS SERVER 2012 / PÉRDIDA DE EQUIPOS. | 2 | M- | 5,00 | A | 10 | MEDIO |
| BASES DE DATOS CORPORATIVAS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 5,00 | A | 10 | MEDIO |

| | | | | | | |
|---|---|---|---|---|---|---|
| BASES DE DATOS CORPORATIVAS / DESPOJO DE INFORMACIÓN. | 2 | M- | 5,00 | A | 10 | MEDIO |
| BASE DE DATOS CLIENTES / DESPOJO DE INFORMACIÓN. | 2 | M- | 5,00 | A | 10 | MEDIO |
| BASES DE DATOS INSPECCIONES / DESPOJO DE INFORMACIÓN. | 2 | M- | 5,00 | A | 10 | MEDIO |
| BASES DE DATOS INVENTARIOS / DESPOJO DE INFORMACIÓN. | 2 | M- | 5,00 | A | 10 | MEDIO |
| BASES DE DATOS EMERGENCIAS / DESPOJO DE INFORMACIÓN. | 2 | M- | 5,00 | A | 10 | MEDIO |
| BACKUPS DE CONTABILIDAD / DESPOJO DE INFORMACIÓN. | 2 | M- | 5,00 | A | 10 | MEDIO |
| RED DE DATOS / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 5,00 | A | 10 | MEDIO |
| ACCESO A INTERNET / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 5,00 | A | 10 | MEDIO |
| ARCHIVO FISÏCO IMPRESO / DESPOJO DE INFORMACIÓN. | 2 | M- | 5,00 | A | 10 | MEDIO |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / DESPOJO DE INFORMACIÓN. | 2 | M- | 5,00 | A | 10 | MEDIO |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / DESPOJO DE INFORMACIÓN. | 2 | M- | 5,00 | A | 10 | MEDIO |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / DESPOJO DE INFORMACIÓN. | 2 | M- | 5,00 | A | 10 | MEDIO |
| ESTACIONES / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| SERVIDORES / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| EQUIPOS DE COMUNICACIONES / FALTA DE MANTENIMIENTO. | 3 | M | 3,00 | M | 9 | MEDIO |
| EQUIPOS DE COMUNICACIONES / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN /FALTA DE MANTENIMIENTO. | 3 | M | 3,00 | M | 9 | MEDIO |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 3 | M | 3,00 | M | 9 | MEDIO |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / CARENCIA DE UNA | 3 | M | 3,00 | M | 9 | MEDIO |

| | | | | | | |
|---|---|---|---|---|---|---|
| METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | | | | | | |
| PLANTA TELEFÓNICA / MALA INSTALACIÓN EN EL CABLEADO. | 3 | M | 3,00 | M | 9 | MEDIO |
| PLANTA TELEFÓNICA / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| WINDOWS SERVER 2012 / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| BASES DE DATOS SQL SERVER 2014/ TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / ELIMINACIÓN Y MODIFICACIÓN. | 3 | M | 3,00 | M | 9 | MEDIO |
| ANTIVIRUS: TREND MICRO / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| ANTIVIRUS: TREND MICRO / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 3 | M | 3,00 | M | 9 | MEDIO |
| COMUNICACIONES: MOTO TRB / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| BASES DE DATOS CORPORATIVAS / ELIMINACIÓN Y MODIFICACIÓN. | 3 | M | 3,00 | M | 9 | MEDIO |
| BASE DE DATOS CLIENTES / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| BASES DE DATOS INSPECCIONES / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| BASES DE DATOS INVENTARIOS / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| BASES DE DATOS EMERGENCIAS / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| BACKUPS DE CONTABILIDAD / INCONVENIENTES ELÉCTRICOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| RED RADIO COMUNICACIONES / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 3,00 | M | 9 | MEDIO |
| SISTEMA DE ALIMENTACIÓN UPS / FALTA DE MANTENIMIENTO. | 3 | M | 3,00 | M | 9 | MEDIO |
| RADIOS PORTATILES / FALTA DE MANTENIMIENTO. | 3 | M | 3,00 | M | 9 | MEDIO |
| RADIOS MOVILES / FALTA DE MANTENIMIENTO. | 3 | M | 3,00 | M | 9 | MEDIO |
| RADIO BASE / FALTA DE MANTENIMIENTO. | 3 | M | 3,00 | M | 9 | MEDIO |
| REPETIDORAS / FALTA DE MANTENIMIENTO. | 3 | M | 3,00 | M | 9 | MEDIO |
| ANTENAS / FALTA DE MANTENIMIENTO. | 3 | M | 3,00 | M | 9 | MEDIO |
| ESTACIONES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| ESTACIONES / DESPOJO DE INFORMACIÓN. | 2 | M- | 4,00 | M+ | 8 | MEDIO |

| | | | | | | |
|---|---|---|---|---|---|---|
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| SERVIDORES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| WINDOWS 7, 8 Y 10 / TÉCNICOS QUE NO SON IDÓNEOS. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| WINDOWS SERVER 2012 / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| BASES DE DATOS SQL SERVER 2014 / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| BASES DE DATOS SQL SERVER 2014/ PÉRDIDA DE EQUIPOS. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / INCAPACIDAD. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / SALIDA DE PERSONAL. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / ELIMINACIÓN Y MODIFICACIÓN. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / DESPOJO DE INFORMACIÓN. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / PÉRDIDA DE EQUIPOS. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| OFIMÁTICA: OFFICE 365 / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| WEBSERVER. II / DESPOJO DE INFORMACIÓN. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| WEBSERVER. II / INEXISTENCIA DE PARCHES. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| WEBSERVER. II / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| WEBSERVER. II / ELIMINACIÓN Y MODIFICACIÓN. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| BASES DE DATOS CORPORATIVAS / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| BASE DE DATOS CONTABLES / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |

| | | | | | | |
|---|---|---|---|---|---|---|
| BASE DE DATOS CLIENTES / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| BASES DE DATOS INSPECCIONES / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| BASES DE DATOS INVENTARIOS / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| BASES DE DATOS EMERGENCIAS / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| BACKUPS DE CONTABILIDAD / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| RED RADIO COMUNICACIONES / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| RED RADIO COMUNICACIONES / FALTA DE MANTENIMIENTO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| RED RADIO COMUNICACIONES / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| INTERNET / ELIMINACIÓN Y MODIFICACIÓN. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| TELEFONIA / TÉCNICOS QUE NO SON IDÓNEOS. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| RADIOS / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| SISTEMA DE ALIMENTACIÓN UPS / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| RADIOS PORTATILES / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| RADIOS MOVILES / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| RADIO BASE / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| REPETIDORAS / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| ANTENAS / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| OPERATIVOS (BOMBEROS) / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| OPERATIVOS (BOMBEROS) / INCAPACIDAD. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| OPERATIVOS (BOMBEROS) / SALIDA DE PERSONAL. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| OPERATIVOS (BOMBEROS) / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| OPERATIVOS (BOMBEROS) / FALTA DE MOTIVACIÓN. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| ADMINISTRATIVOS / DESPOJO DE INFORMACIÓN. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| ADMINISTRATIVOS / INCAPACIDAD. | 2 | M- | 4,00 | M+ | 8 | MEDIO |

| | | | | | | |
|---|---|---|---|---|---|---|
| ADMINISTRATIVOS / SALIDA DE PERSONAL. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| ADMINISTRATIVOS / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| ADMINISTRATIVOS / PÉRDIDA DE EQUIPOS. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| SOPORTE EXTERNO / DESPOJO DE INFORMACIÓN. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| SOPORTE EXTERNO / INCAPACIDAD. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| SOPORTE EXTERNO / SALIDA DE PERSONAL. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| SOPORTE EXTERNO / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| SOPORTE EXTERNO / PÉRDIDA DE EQUIPOS. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 2 | M- | 4,00 | M+ | 8 | MEDIO |
| ESTACIONES / FALTA DE MANTENIMIENTO. | 2 | M- | 3,00 | M | 6 | MEDIO |
| REPETIDORAS / FALTA DE MANTENIMIENTO. | 2 | M- | 3,00 | M | 6 | MEDIO |
| INCONVENIENTES ELÉCTRICOS. | 3 | M | 2,00 | M- | 6 | MEDIO |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / FALTA DE MANTENIMIENTO. | 2 | M- | 3,00 | M | 6 | MEDIO |
| SERVIDORES / FALTA DE MANTENIMIENTO. | 2 | M- | 3,00 | M | 6 | MEDIO |
| EQUIPOS ESCRITORIO PORTATILES / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 3,00 | M | 6 | MEDIO |
| EQUIPOS ESCRITORIO PORTATILES / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3,00 | M | 6 | MEDIO |
| EQUIPOS ESCRITORIO PORTATILES / PÉRDIDA DE EQUIPOS. | 2 | M- | 3,00 | M | 6 | MEDIO |
| PLANTA TELEFÓNICA / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2,00 | M- | 6 | MEDIO |
| WINDOWS 7, 8 Y 10 / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3,00 | M | 6 | MEDIO |
| BASES DE DATOS SQL SERVER 2014/ ELIMINACIÓN Y MODIFICACIÓN. | 2 | M- | 3,00 | M | 6 | MEDIO |
| BASES DE DATOS SQL SERVER 2014/ INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3,00 | M | 6 | MEDIO |

| | | | | | | |
|---|---|---|---|---|---|---|
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 3,00 | M | 6 | MEDIO |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3,00 | M | 6 | MEDIO |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / INCAPACIDAD. | 2 | M- | 3,00 | M | 6 | MEDIO |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / DELEGACIÓN DE RESPONSABILIDADES. | 2 | M- | 3,00 | M | 6 | MEDIO |
| ANTIVIRUS: TREND MICRO / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 3,00 | M | 6 | MEDIO |
| OFIMÁTICA: OFFICE 365 / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 3,00 | M | 6 | MEDIO |
| OFIMÁTICA: OFFICE 365 / TÉCNICOS QUE NO SON IDÓNEOS. | 2 | M- | 3,00 | M | 6 | MEDIO |
| WEBSERVER. II / MALA INSTALACIÓN EN EL CABLEADO. | 3 | M | 2,00 | M- | 6 | MEDIO |
| WEBSERVER. II / FALTA DE MANTENIMIENTO. | 2 | M- | 3,00 | M | 6 | MEDIO |
| WEBSERVER. II / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2,00 | M- | 6 | MEDIO |
| COMUNICACIONES: MOTO TRB / FALTA DE MANTENIMIENTO. | 2 | M- | 3,00 | M | 6 | MEDIO |
| COMUNICACIONES: MOTO TRB / SALIDA DE PERSONAL. | 3 | M | 2,00 | M- | 6 | MEDIO |
| COMUNICACIONES: MOTO TRB / PÉRDIDA DE EQUIPOS. | 2 | M- | 3,00 | M | 6 | MEDIO |
| BASE DE DATOS CONTABLES / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3,00 | M | 6 | MEDIO |
| RED DE DATOS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 2 | M- | 3,00 | M | 6 | MEDIO |
| RED DE DATOS / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3,00 | M | 6 | MEDIO |
| ACCESO A INTERNET / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3,00 | M | 6 | MEDIO |
| TELEFONIA / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 3,00 | M | 6 | MEDIO |
| TELEFONIA / FALTA DE MANTENIMIENTO. | 2 | M- | 3,00 | M | 6 | MEDIO |
| TELEFONIA / INCONVENIENTES ELÉCTRICOS. | 3 | M | 2,00 | M- | 6 | MEDIO |
| RADIOS / FALTA DE MANTENIMIENTO. | 2 | M- | 3,00 | M | 6 | MEDIO |
| RADIOS / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3,00 | M | 6 | MEDIO |
| SISTEMA DE ALIMENTACIÓN UPS / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3,00 | M | 6 | MEDIO |

| | | | | | | |
|---|---|---|---|---|---|---|
| SISTEMA DE ALIMENTACIÓN UPS / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2,00 | M- | 6 | MEDIO |
| RADIOS PORTATILES / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3,00 | M | 6 | MEDIO |
| RADIOS PORTATILES / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2,00 | M- | 6 | MEDIO |
| RADIOS MOVILES / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3,00 | M | 6 | MEDIO |
| RADIOS MOVILES / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2,00 | M- | 6 | MEDIO |
| RADIO BASE / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3,00 | M | 6 | MEDIO |
| RADIO BASE / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2,00 | M- | 6 | MEDIO |
| REPETIDORAS / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3,00 | M | 6 | MEDIO |
| REPETIDORAS / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2,00 | M- | 6 | MEDIO |
| INCONVENIENTES ELÉCTRICOS. | 2 | M- | 3,00 | M | 6 | MEDIO |
| ANTENAS / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2,00 | M- | 6 | MEDIO |
| OPERATIVOS (BOMBEROS) / PÉRDIDA DE EQUIPOS. | 2 | M- | 3,00 | M | 6 | MEDIO |
| ADMINISTRATIVOS / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 3,00 | M | 6 | MEDIO |
| SOPORTE EXTERNO / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 3,00 | M | 6 | MEDIO |
| ARCHIVO FISÏCO IMPRESO / SALIDA DE PERSONAL. | 2 | M- | 3,00 | M | 6 | MEDIO |
| ARCHIVO FISÏCO IMPRESO / INCONVENIENTES ELÉCTRICOS. | 3 | M | 2,00 | M- | 6 | MEDIO |
| ALMACENAMIENTO EN INTERNET (NUBE) / TÉCNICOS QUE NO SON IDÓNEOS. | 3 | M | 2,00 | M- | 6 | MEDIO |
| ESTACIONES / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| ESTACIONES / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| ESTACIONES / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| REPETIDORAS / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| REPETIDORAS / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| REPETIDORAS / PÉRDIDA DE EQUIPOS. | 1 | B | 5,00 | A | 5 | BAJO |
| REPETIDORAS / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |

| | | | | | | |
|---|---|---|---|---|---|---|
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 5,00 | A | 5 | BAJO |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / PÉRDIDA DE EQUIPOS. | 1 | B | 5,00 | A | 5 | BAJO |
| CENTRO PROCESAMIENTO DE DATOS PRINCIPAL / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| SERVIDORES / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| SERVIDORES / PÉRDIDA DE EQUIPOS. | 1 | B | 5,00 | A | 5 | BAJO |
| SERVIDORES / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| EQUIPOS ESCRITORIO PORTATILES / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| EQUIPOS ESCRITORIO PORTATILES / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| EQUIPOS ESCRITORIO PORTATILES / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| EQUIPOS DE COMUNICACIONES / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| EQUIPOS DE COMUNICACIONES / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| EQUIPOS DE COMUNICACIONES / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |

| | | | | | | |
|---|---|---|---|---|---|---|
| EQUIPOS DE GRABACIÓN (LLAMADAS) / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| PLANTA TELEFÓNICA / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| PLANTA TELEFÓNICA / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| PLANTA TELEFÓNICA / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| WINDOWS 7, 8 Y 10 / PÉRDIDA DE EQUIPOS. | 1 | B | 5,00 | A | 5 | BAJO |
| WINDOWS 7, 8 Y 10 / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| WINDOWS SERVER 2012 / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| BASES DE DATOS SQL SERVER 2014/ TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| WEBSERVER. II / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| BASES DE DATOS CORPORATIVAS / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| BASES DE DATOS CORPORATIVAS / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| BASES DE DATOS CORPORATIVAS / PÉRDIDA DE EQUIPOS. | 1 | B | 5,00 | A | 5 | BAJO |
| BASES DE DATOS CORPORATIVAS / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| BASE DE DATOS CONTABLES / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| BASE DE DATOS CLIENTES / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| BASES DE DATOS INSPECCIONES / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| BASES DE DATOS INVENTARIOS / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| BASES DE DATOS EMERGENCIAS / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |

| | | | | | | |
|---|---|---|---|---|---|---|
| RED DE DATOS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 5,00 | A | 5 | BAJO |
| RED DE DATOS / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| RED DE DATOS / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| RED DE DATOS / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| RED RADIO COMUNICACIONES / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| RED RADIO COMUNICACIONES / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| RED RADIO COMUNICACIONES / PÉRDIDA DE EQUIPOS. | 1 | B | 5,00 | A | 5 | BAJO |
| RED RADIO COMUNICACIONES / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| ACCESO A INTERNET / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| ACCESO A INTERNET / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| ACCESO A INTERNET / PÉRDIDA DE EQUIPOS. | 1 | B | 5,00 | A | 5 | BAJO |
| ACCESO A INTERNET / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| INTERNET / DESPOJO DE INFORMACIÓN. | 1 | B | 5,00 | A | 5 | BAJO |
| INTERNET / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| INTERNET / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| INTERNET / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| INTRANET / DESPOJO DE INFORMACIÓN. | 1 | B | 5,00 | A | 5 | BAJO |
| INTRANET / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| INTRANET / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| INTRANET / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| TELEFONIA / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| TELEFONIA / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| TELEFONIA / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| RADIOS / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |

| | | | | | | |
|---|---|---|---|---|---|---|
| RADIOS / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| RADIOS / PÉRDIDA DE EQUIPOS. | 1 | B | 5,00 | A | 5 | BAJO |
| RADIOS / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| SISTEMA DE ALIMENTACIÓN UPS / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| SISTEMA DE ALIMENTACIÓN UPS / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| SISTEMA DE ALIMENTACIÓN UPS / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| RADIOS PORTATILES / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| RADIOS PORTATILES / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| RADIOS PORTATILES / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| RADIOS MOVILES / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| RADIOS MOVILES / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| RADIOS MOVILES / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| RADIO BASE / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| RADIO BASE / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| RADIO BASE / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| REPETIDORAS / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| REPETIDORAS / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| REPETIDORAS / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| ANTENAS / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| ANTENAS / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| ANTENAS / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| OPERATIVOS (BOMBEROS) / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 5,00 | A | 5 | BAJO |
| OPERATIVOS (BOMBEROS) / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 5,00 | A | 5 | BAJO |
| OPERATIVOS (BOMBEROS) / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| OPERATIVOS (BOMBEROS) / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |

| | | | | | | |
|---|---|---|---|---|---|---|
| OPERATIVOS (BOMBEROS) / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| ADMINISTRATIVOS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 5,00 | A | 5 | BAJO |
| ADMINISTRATIVOS / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| ADMINISTRATIVOS / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| ADMINISTRATIVOS / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| SOPORTE EXTERNO / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 5,00 | A | 5 | BAJO |
| SOPORTE EXTERNO / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| SOPORTE EXTERNO / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| SOPORTE EXTERNO / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| ARCHIVO FISÏCO IMPRESO / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 5,00 | A | 5 | BAJO |
| ARCHIVO FISÏCO IMPRESO / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 5,00 | A | 5 | BAJO |
| ARCHIVO FISÏCO IMPRESO / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| ARCHIVO FISÏCO IMPRESO / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| ARCHIVO FISÏCO IMPRESO / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 5,00 | A | 5 | BAJO |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / PÉRDIDA DE EQUIPOS. | 1 | B | 5,00 | A | 5 | BAJO |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 5,00 | A | 5 | BAJO |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / | 1 | B | 5,00 | A | 5 | BAJO |

| | | | | | | |
|---|---|---|---|---|---|---|
| INGRESO DE PERSONAL NO AUTORIZADO. | | | | | | |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / INCENDIO | 1 | B | 5,00 | A | 5 | BAJO |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / TEMBLOR | 1 | B | 5,00 | A | 5 | BAJO |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| ALMACENAMIENTO EN INTERNET (NUBE) / DESPOJO DE INFORMACIÓN. | 1 | B | 5,00 | A | 5 | BAJO |
| ALMACENAMIENTO EN INTERNET (NUBE) / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 5,00 | A | 5 | BAJO |
| ALMACENAMIENTO EN INTERNET (NUBE) / TERRORISMO. | 1 | B | 5,00 | A | 5 | BAJO |
| ESTACIONES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| ESTACIONES / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 2,00 | M- | 4 | BAJO |
| ESTACIONES / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| ESTACIONES / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| REPETIDORAS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| REPETIDORAS / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| SERVIDORES / MALA INSTALACIÓN EN EL CABLEADO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| SERVIDORES / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 2,00 | M- | 4 | BAJO |
| EQUIPOS ESCRITORIO PORTATILES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| EQUIPOS ESCRITORIO PORTATILES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| EQUIPOS ESCRITORIO PORTATILES / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 2,00 | M- | 4 | BAJO |

| | | | | | | |
|---|---|---|---|---|---|---|
| EQUIPOS DE COMUNICACIONES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| EQUIPOS DE COMUNICACIONES / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 2,00 | M- | 4 | BAJO |
| EQUIPOS DE COMUNICACIONES / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 2,00 | M- | 4 | BAJO |
| EQUIPOS DE COMUNICACIONES / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / MALA INSTALACIÓN EN EL CABLEADO. | 2 | M- | 2,00 | M- | 4 | BAJO |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 2,00 | M- | 4 | BAJO |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / DESPOJO DE INFORMACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / TÉCNICOS QUE NO SON IDÓNEOS. | 2 | M- | 2,00 | M- | 4 | BAJO |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / DESPOJO DE INFORMACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / TÉCNICOS QUE NO SON IDÓNEOS. | 2 | M- | 2,00 | M- | 4 | BAJO |
| PLANTA TELEFÓNICA / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| WINDOWS SERVER 2012 / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 4,00 | M+ | 4 | BAJO |
| APLICATIVO CONTABLE: LGX VERSIONES 10 Y 11 / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| CORREO ELECTRÓNICO: HOTMAIL, YAHOO Y GMAIL / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| ANTIVIRUS: TREND MICRO / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| ANTIVIRUS: TREND MICRO / DESPOJO DE INFORMACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| ANTIVIRUS: TREND MICRO / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 4,00 | M+ | 4 | BAJO |
| ANTIVIRUS: TREND MICRO / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |

| | | | | | | |
|---|---|---|---|---|---|---|
| ANTIVIRUS: TREND MICRO / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| ANTIVIRUS: TREND MICRO / TERRORISMO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| OFIMÁTICA: OFFICE 365 / DESPOJO DE INFORMACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| OFIMÁTICA: OFFICE 365 / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 4,00 | M+ | 4 | BAJO |
| OFIMÁTICA: OFFICE 365 / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| OFIMÁTICA: OFFICE 365 / TERRORISMO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| COMUNICACIONES: MOTO TRB / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| COMUNICACIONES: MOTO TRB / INCENDIO | 1 | B | 4,00 | M+ | 4 | BAJO |
| COMUNICACIONES: MOTO TRB / TEMBLOR | 1 | B | 4,00 | M+ | 4 | BAJO |
| COMUNICACIONES: MOTO TRB / TERRORISMO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASES DE DATOS CORPORATIVAS / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASE DE DATOS CONTABLES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASE DE DATOS CONTABLES / FALTA DE MANTENIMIENTO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASE DE DATOS CONTABLES / SALIDA DE PERSONAL. | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASE DE DATOS CONTABLES / INCENDIO | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASE DE DATOS CONTABLES / TEMBLOR | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASE DE DATOS CONTABLES / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASE DE DATOS CLIENTES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASE DE DATOS CLIENTES / INCENDIO | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASE DE DATOS CLIENTES / TEMBLOR | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASE DE DATOS CLIENTES / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASES DE DATOS INSPECCIONES / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASES DE DATOS INSPECCIONES / INCENDIO | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASES DE DATOS INSPECCIONES / TEMBLOR | 1 | B | 4,00 | M+ | 4 | BAJO |

| | | | | | | |
|---|---|---|---|---|---|---|
| BASES DE DATOS INSPECCIONES / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASES DE DATOS INVENTARIOS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASES DE DATOS INVENTARIOS / INCENDIO | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASES DE DATOS INVENTARIOS / TEMBLOR | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASES DE DATOS INVENTARIOS / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASES DE DATOS EMERGENCIAS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASES DE DATOS EMERGENCIAS / INCENDIO | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASES DE DATOS EMERGENCIAS / TEMBLOR | 1 | B | 4,00 | M+ | 4 | BAJO |
| BASES DE DATOS EMERGENCIAS / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| BACKUPS DE CONTABILIDAD / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| BACKUPS DE CONTABILIDAD / INCENDIO | 1 | B | 4,00 | M+ | 4 | BAJO |
| BACKUPS DE CONTABILIDAD / TEMBLOR | 1 | B | 4,00 | M+ | 4 | BAJO |
| BACKUPS DE CONTABILIDAD / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| BACKUPS DE CONTABILIDAD / TERRORISMO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| RED DE DATOS / DESPOJO DE INFORMACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| ACCESO A INTERNET / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| ACCESO A INTERNET / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| ACCESO A INTERNET / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| INTERNET / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| INTRANET / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| TELEFONIA / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| SISTEMA DE ALIMENTACIÓN UPS / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| SISTEMA DE ALIMENTACIÓN UPS / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| RADIOS PORTATILES / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4,00 | M+ | 4 | BAJO |

| | | | | | | |
|---|---|---|---|---|---|---|
| RADIOS PORTATILES / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| RADIOS MOVILES / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| RADIOS MOVILES / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| RADIO BASE / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| RADIO BASE / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| REPETIDORAS / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| REPETIDORAS / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| ANTENAS / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| ANTENAS / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| OPERATIVOS (BOMBEROS) / DESPOJO DE INFORMACIÓN. | 2 | M- | 2,00 | M- | 4 | BAJO |
| ADMINISTRATIVOS / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 4,00 | M+ | 4 | BAJO |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / PÉRDIDA DE EQUIPOS. | 1 | B | 4,00 | M+ | 4 | BAJO |
| ALMACENAMIENTO EN INTERNET (NUBE) / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 4,00 | M+ | 4 | BAJO |
| UPS, SALA DE COMUNICACIONES, SALA ELECTRICA / FALTA DE MANTENIMIENTO. | 1 | B | 3,00 | M | 3 | BAJO |
| SERVIDORES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| SERVIDORES / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 3,00 | M | 3 | BAJO |
| EQUIPOS ESCRITORIO PORTATILES / SALIDA DE PERSONAL. | 1 | B | 3,00 | M | 3 | BAJO |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN /PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 3,00 | M | 3 | BAJO |

| | | | | | | |
|---|---|---|---|---|---|---|
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| EQUIPOS DE SEGURIDAD PERIMETRAL (CAMARAS) / PÉRDIDA DE EQUIPOS. | 1 | B | 3,00 | M | 3 | BAJO |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 3,00 | M | 3 | BAJO |
| EQUIPOS DE GRABACIÓN (LLAMADAS) /PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| EQUIPOS DE GRABACIÓN (LLAMADAS) / PÉRDIDA DE EQUIPOS. | 1 | B | 3,00 | M | 3 | BAJO |
| WINDOWS 7, 8 Y 10 / DESPOJO DE INFORMACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| WINDOWS 7, 8 Y 10 / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| WINDOWS SERVER 2012 / DESPOJO DE INFORMACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| BASES DE DATOS SQL SERVER 2014/ DESPOJO DE INFORMACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| OFIMÁTICA: OFFICE 365 / PÉRDIDA DE EQUIPOS. | 1 | B | 3,00 | M | 3 | BAJO |
| BASES DE DATOS CORPORATIVAS / INCONVENIENTES ELÉCTRICOS. | 1 | B | 3,00 | M | 3 | BAJO |
| RED RADIO COMUNICACIONES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| RED RADIO COMUNICACIONES / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 3,00 | M | 3 | BAJO |
| INTRANET / INCONVENIENTES ELÉCTRICOS. | 1 | B | 3,00 | M | 3 | BAJO |
| TELEFONIA / PÉRDIDA DE EQUIPOS. | 1 | B | 3,00 | M | 3 | BAJO |
| RADIOS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| RADIOS / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 3,00 | M | 3 | BAJO |
| SISTEMA DE ALIMENTACIÓN UPS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| RADIOS PORTATILES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| RADIOS MOVILES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| RADIO BASE / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| REPETIDORAS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |

| | | | | | | |
|---|---|---|---|---|---|---|
| ANTENAS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| DÍSCOS DUROS DE SERVIDORES Y ESTACIONES DE TRABAJO / INCONVENIENTES ELÉCTRICOS. | 3 | M | 1,00 | B | 3 | BAJO |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| DISCOS EXTERNOS INFORMACIÓN DE BACKUPS / INCONVENIENTES ELÉCTRICOS. | 3 | M | 1,00 | B | 3 | BAJO |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / PROBLEMAS EN LA ESTRUCTURA DE LA ORGANIZACIÓN. | 1 | B | 3,00 | M | 3 | BAJO |
| UNIDADES DE CD , DVD Y MEMORIAS EXTRAÏBLES / INCONVENIENTES ELÉCTRICOS. | 3 | M | 1,00 | B | 3 | BAJO |
| EQUIPOS ESCRITORIO PORTATILES / CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | 1 | B | 2,00 | M- | 2 | BAJO |
| PLANTA TELEFÓNICA / FALTA DE MANTENIMIENTO. | 2 | M- | 1,00 | B | 2 | BAJO |
| PLANTA TELEFÓNICA / PÉRDIDA DE EQUIPOS. | 1 | B | 2,00 | M- | 2 | BAJO |
| WINDOWS 7, 8 Y 10 / INEXISTENCIA DE PARCHES. | 1 | B | 2,00 | M- | 2 | BAJO |
| WINDOWS SERVER 2012 / INEXISTENCIA DE PARCHES. | 1 | B | 2,00 | M- | 2 | BAJO |
| WINDOWS SERVER 2012 / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 2,00 | M- | 2 | BAJO |
| WINDOWS SERVER 2012 / ELIMINACIÓN Y MODIFICACIÓN. | 1 | B | 2,00 | M- | 2 | BAJO |
| ANTIVIRUS: TREND MICRO / INEXISTENCIA DE PARCHES. | 1 | B | 2,00 | M- | 2 | BAJO |
| OFIMÁTICA: OFFICE 365 / INEXISTENCIA DE PARCHES. | 1 | B | 2,00 | M- | 2 | BAJO |
| BASE DE DATOS CLIENTES / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 2,00 | M- | 2 | BAJO |
| BASES DE DATOS INSPECCIONES / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 2,00 | M- | 2 | BAJO |
| BASES DE DATOS INVENTARIOS / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 2,00 | M- | 2 | BAJO |
| BASES DE DATOS EMERGENCIAS / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 2,00 | M- | 2 | BAJO |
| BACKUPS DE CONTABILIDAD / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 2,00 | M- | 2 | BAJO |
| INTERNET / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 2,00 | M- | 2 | BAJO |

| | | | | | | |
|---|---|---|---|---|---|---|
| INTERNET / INCONVENIENTES ELÉCTRICOS. | 2 | M- | 1,00 | B | 2 | BAJO |
| INTRANET / PERMITIR LA EJECUCIÓN DE UN SOFTWARE MALICIOSO. | 1 | B | 2,00 | M- | 2 | BAJO |
| TELEFONIA / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 2,00 | M- | 2 | BAJO |
| RADIOS / TÉCNICOS QUE NO SON IDÓNEOS. | 2 | M- | 1,00 | B | 2 | BAJO |
| ADMINISTRATIVOS / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 2,00 | M- | 2 | BAJO |
| SOPORTE EXTERNO / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 2,00 | M- | 2 | BAJO |
| ARCHIVO FISÏCO IMPRESO / INGRESO DE PERSONAL NO AUTORIZADO. | 2 | M- | 1,00 | B | 2 | BAJO |
| ESTACIONES / UTILIZACIÓN DE SOFTWARE NO OFICIAL. | 1 | B | 1,00 | B | 1 | BAJO |
| SERVIDORES / INCENDIO | 1 | B | 1,00 | B | 1 | BAJO |
| EQUIPOS DE COMUNICACIONES / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 1,00 | B | 1 | BAJO |
| EQUIPO DE RADIO, GPS Y COMUNICACIÓN /INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 1,00 | B | 1 | BAJO |
| PLANTA TELEFÓNICA / INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 1,00 | B | 1 | BAJO |
| BASES DE DATOS SQL SERVER 2014/ INGRESO DE PERSONAL NO AUTORIZADO. | 1 | B | 1,00 | B | 1 | BAJO |
| OFIMÁTICA: OFFICE 365 / FALTA DE MANTENIMIENTO. | 1 | B | 1,00 | B | 1 | BAJO |
| WEBSERVER. II / PÉRDIDA DE EQUIPOS. | 1 | B | 1,00 | B | 1 | BAJO |
| POSICIONAMIENTO: GOOGLE MAPS / FALTA DE MANTENIMIENTO. | 1 | B | 1,00 | B | 1 | BAJO |

Fuente: Elaboración propia.

**Análisis.**

Al analizar los datos obtenidos, se logró observar que afortunadamente para la organización no todos los activos tuvieron un resultado que los ubicara en una situación de riesgo medio o alto, sin embargo, lo anterior no quiere decir que no hay que hacer nada al respecto, debido a que la realización de tan solo una de las amenazas que se sitúan en un riesgo medio o alto, ocasionarían problemas graves al normal funcionamiento de la organización.

Conforme a los datos obtenidos en la tabla anterior (clasificación del riesgo según el grado de importancia), se evidencia que el 25% está ubicado en una situación de alta

vulnerabilidad, por lo cual, es prioritario para la organización tomar acciones al respecto por medio de un plan de tratamiento que permita remover los activos catalogados como "Alto" y Medio Alto" en un nivel más bajo o lograr disiparlo.

### 7.3.8. Margen Porcentual de Amenazas.

Con el fin de conocer más a fondo los resultados de la tabla anterior (Clasificación Del Riesgo Según El Grado de Importancia), en seguida se mostrará el margen porcentual de los activos y amenazas que se hallan en un nivel bajo, medio, medio alto y alto.

*Tabla 16: Margen Porcentual De Amenazas*

| **Margen Porcentual de Amenazas** | | | |
|---|---|---|---|
| Rojo | Ato | 284,00 | 9% |
| Naranja | Medio Alto | 540,00 | 16% |
| Amarillo | Medio | 1.232,00 | 38% |
| Verde | Bajo | 1.231,00 | 37% |
| **Total** | | 3.287,00 | 100% |

Fuente: Elaboración propia.

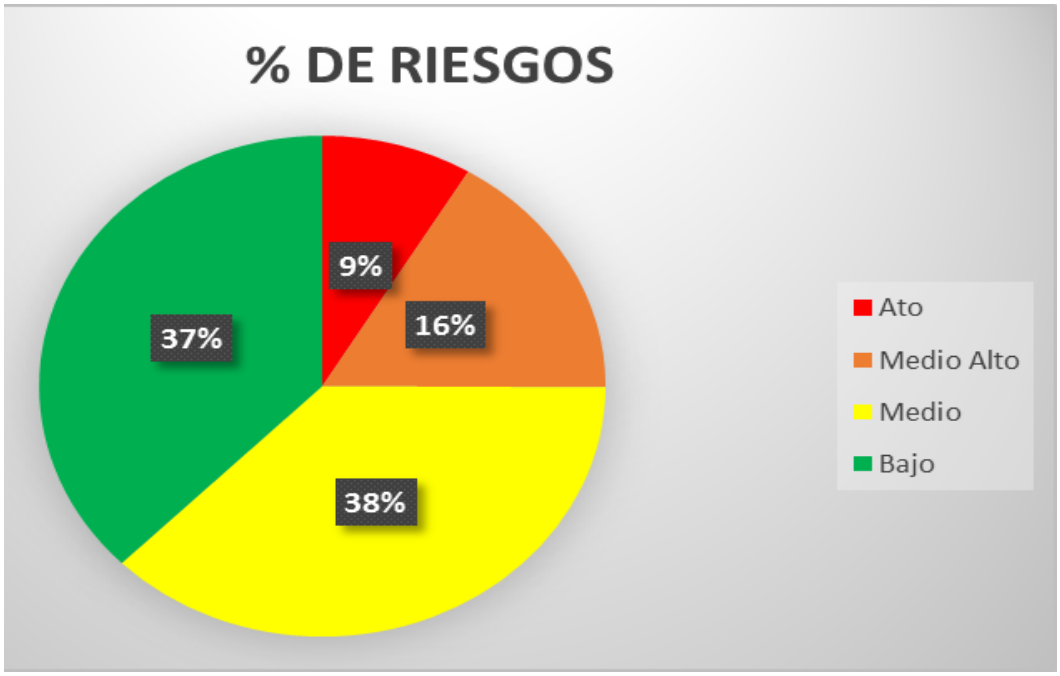


*Figura 31: Clasificación del Riesgo Según el Grado de Importancia.*

Fuente: Elaboración propia.

De acuerdo a los datos encontrados, los riesgos que exigen un tratamiento de manera urgente son los siguientes:

- Técnicos Que No Son Idóneos. (20)
- Salida de personal. (8)
- Eliminación y modificación. (8)
- Falta de mantenimiento. (7)
- Delegación De Responsabilidades. (5)
- Carencia de una metodología para la utilización de programas. (5)
- Mala instalación en el cableado. (3)
- Inconvenientes eléctricos. (3)
- Falta de motivación. (2)
- Despojo de información. (2)
- Ejecución de un software malicioso. (1)

Es preciso señalar que, en el listado de los riesgos anteriormente expuestos la lista está ordenada de forma ascendente, sin embargo, el riesgo que tiene que ver con "técnicos que no son idóneos representa un amplio número con respecto a lo demás riesgos que se encuentran en el listado.

### 7.3.9. PLAN DE TRATAMIENTO DEL RIESGO.

Una vez realizado el listado de los riesgos más propensos a los que está expuesta la organización, es necesario realizar un plan de tratamiento que facilite la eliminación o disminuya el nivel que actualmente tienen. Para lograr elaborar un plan de tratamiento que cumpla con las expectativas, es imperioso sugerir acciones acordes con las necesidades que tiene la organización, las cuales serán presentadas en la siguiente tabla:

*Tabla 17: Plan De Tratamiento De Riesgos.*

| AMENAZAS | TRATAMIENTO | | | | PLAN DE CONTROL | ENCARGADO | EFECTO ESPERADO |
|---|---|---|---|---|---|---|---|
| | ACEPTARLO | EVITARLO | MITIGARLO | TRANSFERIRLO | | | |
| TÉCNICOS QUE NO SON IDÓNEOS | | | X | | Antes de contratar el servicio técnico de un ingeniero, es necesario realizar una prueba de conocimiento que se ajuste a las exigencias de la entidad. - Que todos los ingenieros estén capacitados para brindar apoyo técnico al software LGX. - Implementar procedimientos de seguridad para proteger las bases de datos. -Establecer reglas específicas para que los empleados conozcan la responsabilidad de sus labores, en cuanto a la seguridad de la información. - Antes de tener acceso a los activos de la información, es importante instaurar un acuerdo de confidencialidad y responsabilidad en sus labores, independientemente del tipo de vínculo con la entidad - Crear una plaza encargada de dirigir el departamento de sistemas. | Asesor De Tecnología Y Comunicaciones O Jefe Del Departamento De Sistemas. | Disminuir los inconvenientes presentados a nivel medio o inferior. - Reducir la falta de ineficiencia en la entidad, como consecuencia de los errores cometidos por el soporte externo.- Mantener protegida la integridad de la información. |
| DELEGACIÓN DE RESPONSABILIDADES | | | X | | Establecer un lineamiento detallado de las responsabilidades que tienen los empleados que manejan los activos de la información. - Designar el miembro responsable de cada activo o procedimiento de seguridad, mediante un documento. - Definir perfiles de acceso a la información tangible e intangible que posee la entidad. - Implementar un departamento de sistemas responsable de la preservación, operación y administración de los recursos tecnológicos. - Los empleados no podrán emplear equipos tecnológicos para fines personales. - Socializar el material realizado para que los empleados conozcan acerca del uso y protección que deben tener los activos de la información. | Asesor De Tecnología Y Comunicaciones O Jefe Del Departamento De Sistemas | Disminuir los problemas presentados a nivel medio o inferior. - Disminuir los problemas asociados a los recursos tecnológicos. - Mejorar la eficiencia |
| FALTA DE MANTENIMIENTO | | | X | | Seguir las recomendaciones del proveedor de acuerdo a las especificaciones de uso. - Establecer responsabilidades inherentes al personal que está autorizado de brindar soporte técnico. - Mantener un registro de todas las fallas y procedimientos realizados. - Dar cumplimiento a todas las exigencias impuestas por las pólizas de seguros. | Asesor De Tecnología Y Comunicaciones O Jefe Del Departamento De Sistemas. | Disminuir el nivel del riesgo a medio o inferior. - Mejorar la eficacia en las labores por parte del personal. - Gestionar desde el departamento de sistemas para que los errores presentados no vuelvan a ocurrir. - |
| FALTA DE MOTIVACIÓN. | | | X | | Poner en práctica actividades de integración dirigidas al personal de la entidad. - Mejorar la remuneración salarial. - Implementar becas de estudio. - Crear escenarios enfocados a resolver conflictos. | Asesor De Tecnología Y Comunicaciones O Jefe Del Departamento De Sistemas. | Reducir el nivel del riesgo a nivel medio o inferior. - Corregir la falta de motivación del personal. - Disminuir los errores. - Optimizar el ambiente laboral. |
| MALA INSTACIÓN EN EL CABLEADO. | | | X | | Implementar medidas de protección en el cableado como por ejemplo que sea subterráneo o canalizado. - El cableado deberá estar custodiado ante interceptaciones a través de canales de carácter público. – Diferenciar los cables de energía con los cables de comunicaciones para evitar interferencias. | Asesor De Tecnología Y Comunicaciones O Jefe Del Departamento De Sistemas. | Disminuir el nivel del riesgo a medio o inferior. - Evitar errores inherentes al cableado. - Mejorar la productividad. - Aumentar la eficiencia. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| CARENCIA DE UNA METODOLOGÍA PARA LA UTILIZACIÓN DE PROGRAMAS. | | | X | | Hacer capacitaciones y mantener al personal actualizado en los programas que utilizan a diario. – Hacer una lista de los programas más utilizados. | Asesor De Tecnología Y Comunicaciones O Jefe Del Departamento De Sistemas. | Disminuir el nivel de riesgo a medio o inferior. - Asegurar la empleabilidad correcta y segura de los medios de procesamiento de información. |
| ELIMINACIÓN Y MODIFICACIÓN. | | | X | | Tener identificados los responsables de los activos de la información en la entidad. - Almacenar en diferentes medios (discos duros, memorias USB, nube, etc.) la información confidencial que posee la entidad. - Restringir al máximo el acceso de la información a personal no autorizado. | Asesor De Tecnología Y Comunicaciones O Jefe Del Departamento De Sistemas. | Disminuir el nivel del riesgo a medio o inferior. - Evitar la pérdida de información. - No cometer errores. - Proteger la integridad de la información. |
| INCONVENIENTES ELÉCTRICOS. | | | X | | Tener un generador para emergencias con suficiente combustible. - Contemplar la idea de implementar diferentes fuentes de energía. | Asesor De Tecnología Y Comunicaciones O Jefe Del Departamento De Sistemas. | Disminuir el nivel del riesgo a medio o inferior. - Impedir los errores asociados con inconvenientes eléctricos. - Promover la eficiencia.- Reducir los apagones. |
| EJECUCIÓN DE SOFTWARE MALICIOSO | | | X | | Mantener el antivirus actualizado con todos los servicios disponibles. - Evitar que los empleados conecten sus dispositivos personales a los equipos de la entidad.- Definir responsabilidades y deberes al personal que maneja diariamente activos de la información. | Asesor De Tecnología Y Comunicaciones O Jefe Del Departamento De Sistemas. | Disminuir el nivel de riesgo a medio o inferior. - Impedir problemas de funcionalidad en los equipos. - Procurar que no exista el robo de información. |
| SALIDA DE PERSONAL | | | X | | Previo al contrato, es necesario que la persona que desea ingresar a la entidad conozca las responsabilidades inherentes a la seguridad de la información. - Antes de iniciar sus tareas, se deberá hacer un registro de los activos de la información que tiene a cargo. - En el contrato de cada trabajador (independientemente si es nuevo o antiguo) incluir una cláusula de confidencialidad. | Asesor De Tecnología Y Comunicaciones O Jefe Del Departamento De Sistemas. | Disminuir el nivel de riesgo a medio o inferior. - Evitar el robo de información. - Conocer los activos que deja a disposición de la entidad la persona que termina o deja su trabajo. |
| DESPOJO DE INFORMACIÓN | | | X | | Manifestar al área de sistemas cualquier indicio de inseguridad que presenten los activos de la información. - Investigar los antecedentes de las personas postuladas al puesto de trabajo, en especial aquellos que manejan información confidencial. | Asesor De Tecnología Y Comunicaciones O Jefe Del Departamento De Sistemas. | Disminuir el nivel de riesgo a medio o inferior. - Evitar el robo de información. - Impedir la pérdida de integridad de la información. |

Fuente: Arango (2016)

**Análisis.**

Teniendo en cuenta el objetivo del plan de tratamiento de riesgos, se espera que, mediante diferentes acciones se logre mitigar todos los problemas de gravedad inherentes a la seguridad de la información que en la actualidad tiene la organización, por medio de labores encaminadas a cambiar el comportamiento de los empleados, dado el gran desconocimiento por muchos miembros de la entidad, como se evidenció en todos los resultados obtenidos desde la tabla de dimensiones de seguridad de los activos de la información.

En la tabla del Plan De Tratamiento De Riesgos (tabla 15), se hizo bastante énfasis en la amenaza que implica contratar técnicos que no son idóneos, se sugirió tener en cuenta la importancia de contratar gente idónea para las necesidades que tiene la organización, ya que en muchas ocasiones ni siquiera conocían por ejemplo del software contable u otras herramientas en las actividades diarias de la empresa.

En cuanto a la delegación de responsabilidades, existe un gran desconocimiento de las personas que tienen bajo su responsabilidad activos de la información y de igual manera el manejo que deberían darles. Para dar una solución urgente, se estableció con el listado de activos de la información, asociarlo con los miembros que tienen la responsabilidad de protegerlos y brindar una charla acerca del cuidado y uso que se le debe dar a la información de la organización.

## 8. Conclusiones y recomendaciones.

El trabajo realizado por medio de la Norma ISO 27001 versión 2013, la Norma ISO 31000 versión 2011 y la metodología para la valoración del riesgo (Magerit), permitió un estudio riguroso para examinar el estado actual que se encuentra la entidad, a través de un análisis interno, el tipo de riesgos bajo los cuales está sometido cada activo, el nivel de frecuencia que tiene cada riesgo y en general, los errores asociados con el sistema de gestión de seguridad de la información de la entidad. En tal sentido, se logró consolidar una primera fase para contemplar más adelante implantar cada aspecto de la Norma, lo cual implicaría la revisión del desempeño y aplicar la mejora continua.

Al revisar el estado actual del Cuerpo de Bomberos Voluntarios de Tunja en cuanto a la aplicación de la Norma ISO 27001 versión 2013, se evidencia que no se adelantó el proceso conforme a un cronograma que indicara tiempos y metas a cumplir a pesar de contar con un elemento tan significativo como la política de seguridad de la información. Así mismo, al ejecutar el análisis diferencial fue posible detectar que existen muchos vacíos en la seguridad de los activos de la información de la entidad. Como consecuencia de lo anterior, se puede afirmar que el estado actual no es muy favorable para la implementación, en la medida que muy pocos ítems obtuvieron un resultado positivo (trabajo en áreas seguras y áreas de despacho y carga), mientras que al analizar de forma general los demás resultados, la gran mayoría obtuvo un valor de cero porque no se han llevado a cabo

acciones en beneficio de la seguridad de la información y por lo tanto se sugiere nuevamente revisar el proceso, conforme al análisis realizado y actualizar la política.

Dado que se conoció la situación del Cuerpo De Bomberos Voluntarios De Tunja con respecto a la Norma ISO 27001, los errores que fueron detectados se analizaron de manera muy detallada para entender el grado de afectación que tienen sobre las dimensiones en la seguridad, la incidencia que tiene sobre cada activo, el nivel de frecuencia que ocurren, entre otros aspectos y se espera que, por medio de la implementación del plan de tratamiento de riesgos se logre prevenir, mitigar o evitar cometer los mismos errores del pasado en la gestión de los datos y mejorar la eficiencia de los procesos relacionados con el sistema de información.

Por medio de la revisión efectuada al estado actual de los activos de la información, es evidente la situación de vulnerabilidad que se presenta la organización como resultado de la ausencia de controles que contribuyan a prevenir dificultades asociadas con la protección de datos, pérdida de eficiencia, errores al tomar decisiones y especialmente pérdidas económicas. Por lo anterior, se recomienda implementar controles que faciliten la retroalimentación e incorporación de medidas de control que detecten a tiempo riesgos asociados a los activos de la información y orienten gerencialmente a los directivos.

Se recomienda a los directivos revisar el plan de tratamiento de riesgos que orienta la forma en que debe darse seguimiento a los riesgos a los que está expuesta la entidad, el tiempo y urgencia de atender algunas situaciones que impactarían negativamente, generando pérdidas importantes tanto de información como económicas. Responsabilizar a los equipos de trabajo de cada dependencia en la actualización y gestión de los activos de la información a su cargo, así como empoderarlos en el proceso de detención e identificación de amenazas de acuerdo con la política de seguridad de la información de manera íntegra.

## 9. Referencias


Abantos. (2014). Clasificación de Redes. En Abantos, *Cuerpo De Gestión De Sistemas E Informática De La Administración Del Estado* (págs. 7-8). Villanueva De La Cañada: Grupo Abantos Formación Y Consultoría.

Aguado, J. M. (2004). Aproximación al concepto de comunicación: Fundamentos para la delimitación y estudio del fenómeno comunicacional. En J. M. Aguado, *Introducción A Las Teorías De La Comunicación Y La Información* (págs. 9 -23). Universidad De Murcia.

Anzil, F. (1 de Septiembre de 2010). *Zona Económica*. Obtenido de Zona Económica: https://www.zonaeconomica.com/control

Arango, P. A. (6 de junio de 2016). *Repositorio Universidad Oberta de Catalunya.* Obtenido de UOC: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/53466/8/pmayaaTFM0616memoria.pdf

Avella, L., & Parra, P. (2013). *Repositorio Universidad Nacional de Colombia.* Obtenido de http://bdigital.unal.edu.co/: http://bdigital.unal.edu.co/11172/1/laurayanethavellamartinez.2013.pdf

Ballester, E. G., Barco, P. M., Pozo, P. M., Cueto, A. S., Guijarro, A. M., & Boro, E. S. (2007). *Repositorio Institucional de la Universidad de Alicante.* Obtenido de RUA: https://rua.ua.es/dspace/bitstream/10045/2990/1/ApuntesBD1.pdf

Barceló, M., Iñigo, J., Martí, R., Peig, E., & Perramon, X. (2004). Breve Historia De Las Comunicaciones. En M. Barceló, J. Iñigo, R. Martí, E. Peig, & X. Perramon, *redes de computadores* (págs. 26-28). Barcelona: Eureca Media, SL.

Bolaños, D. E., & Mora, Á. D. (2013). Riesgos, Amenazas Y Vulnerabilidades De Los Sistemas De Información Geográfica. *Universidad Católica de Colombia Trabajo de Investigación.*, 14.

Cáceres, E. (2014). *Universidad Nacional de San Juan.* Obtenido de Repositorio Universidad Nacional de San Juan: http://www.facso.unsj.edu.ar/catedras/ciencias-economicas/sistemas-de-informacion-II/documentos/aydise14.pdf

Caldas, U. D. (2011). *udistrital.edu.co.* Obtenido de udistrital.edu.co: https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf

Carlos. (27 de enero de 2014). *hostname*. Obtenido de https://www.hostname.cl/blog/servidores-de-videojuegos

Carvajal, R. J. (2014). *Mantenimiento del software* . Málaga: IC Editorial.

Cedano, M., Cedano, A., Rubio, J., & Vega, A. (2014). Redes. En M. Cedano, A. Cedano, J. Rubio, & A. Vega, *Fundamentos De Computación Para Ingenieros* (págs. 128-130). Ciudad de México: Grupo Editorial Patria.

Celsia. (12 de mayo de 2014). *Cerlsia Empresa de Energía.* Obtenido de https://www.celsia.com/Portals/0/contenidos-celsia/nuestra-empresa/politicas-y-adhesiones/politicas/politica-seguridad-de-la-informacion.pdf

COLOMBIA. (2014). *Mintic.gov.co.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Congreso de la República de Colombia. (1991). *Constitución Politica de la República de Colombia* . Obtenido de http://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia.pdf

Cots, S. (2012). La estandarización de la gestión de TI a través de ISO/IEC 20.000. *VII Congreso Acdémico Internacional En Gobierno y Gestión del Servicio de TI*. Obtenido de https://www.researchgate.net/profile/Santi_Cots/publication/258820429_La_estandarizacion_de_la_gestion_de_TI_a_traves_de_ISO_IEC_20000/links/00b49528fba5de500b000000.pdf

Cruzatti, I. P. (2008). Investigación Descriptiva. En I. P. Cruzatti, *Tiempo de investigar, investigación científica 1* (págs. 27-29). Quito: Editeka Ediciones.

Cusi, M. L., & Bernal, L. D. (30 de marzo de 2015). *Universidad Icesi.* Obtenido de https://pdf.sciencedirectassets.com/287546/1-s2.0-S0123592314X00094/1-s2.0-S0123592314001570/main.pdf?X-Amz-Security-Token=AgoJb3JpZ2luX2VjENr%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLWVhc3QtMSJGMEQCIEGuQzWKWpUAgX1f6bGMXD8Irp2TngMVhbNEim3Slq%2FAAiADkMQJJ05v74

Deloitte. (2017). *Seguridad de la Información en Ecuador.* Quito: Deloitte Global Services Limited.

Díaz, G., Armendáriz, I., Ruiz, E., & Castro, M. (2014). Descripción del problema de seguridad en redes. Tipos de ataques. En G. Díaz, I. Armendáriz, E. Ruiz, & M. Castro, *Procesos y herramientas para la seguridad de redes* (págs. 15-18). Madrid: UNED - Universidad Nacional de Educación a Distancia.

Díaz, G., Mur, F., & Sancristóbal, E. (2004). Intrudicción. En G. Díaz, F. Mur, & E. Sancristóbal, *Seguridad en las comunicaciones y en la información* (págs. 87-89). Madrid: UNED - Universidad Nacional de Educación a Distancia.

Díaz, L., & Navarro, M. (2014). Los Sistemas En La Empresa Y La Estrategia. En L. Díaz, & M. Navarro, *Sistemas de Información en la Empresa* (págs. 13-15). Alcalá: Universidad de Alcalá Servicio de Publicaciones.

Digital, C. (22 de Agosto de 2016). *El Tiempo*. Obtenido de El Tiempo: http://blogs.eltiempo.com/colombia-digital/2016/08/22/la-confidencialidad-de-la-informacion-y-los-negocios/

Dinero. (6 de Agosto de 2001). *Dinero*. Obtenido de Dinero: http://www.dinero.com/edicion-impresa/especial-comercial/recuadro/empresas-certificadas-icontec/8088

Espinosa, A. P., & Campos, B. P. (2005). *Conceptos de informática.* Madrid: McGraw-Hill España.

Espinosa, A. P., Ruiz, A. L., & Cantero, J. C. (2006). *Introducción a la informática (4a. ed.).* Madrid: McGraw-Hill España.

Fajardo, C. E. (2017). *Politécnico Grancolombiano.* Obtenido de Repositorio Politécnico Grancolombiano: http://repository.poligran.edu.co/bitstream/handle/10823/995/3.%20Documento%20Final%20Opci%C3%B3n%20de%20grado%20II.pdf?sequence=1&isAllowed=y

Fernández, L. G., & Alvaréz, A. A. (2012). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre Seguridad en Sistemas de información para pymes.* . Madrid: AENOR.

Funes, D. J. (25 de Abril de 2013). *innsz.mx*. Obtenido de innsz.mx: http://www.innsz.mx/opencms/contenido/investigacion/comiteEtica/confidencialidadInformacion.html

Gallego, F. E. (junio de 2007). *Scielo.* Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-47722007000100007

García, D., Gomez, S., Molina, E., & Rubio, M. (2017). Redes de Ordenadores. En D. García, S. Gomez, E. Molina, & M. Rubio, *Introducción A La Informática Básica* (pág. 231). Madrid: UNED.

Garrido, C. (octubre de 2008). *Repositorio Universidad de San Carlos de Guatemala.* Obtenido de http://biblioteca.usac.edu.gt/tesis/07/07_2010.pdf

Gómez, L., & Álvarez, A. (2012). *Introducción a los Sistemas de Gestión de Seguridad de la Información (SGSI).* Madrid: AENOR - Asociación Española de Normalización y Certificación.

Gómez, L., & Rivero, P. (2015). Elaboración del inventario de activos. En L. Rivero, & G. Pablo, *Cómo implantar un SGSI según UNE-ISO/IEC 27001* (págs. 59-60). Madrid: AENOR.

González, J. E. (17 de enero de 2014). *DocIRS.* Obtenido de https://www.docirs.cl/implantacion_sistema.htm

Graells, P. M. (2012 de diciembre de 2012). *3ciencias.* Obtenido de https://www.3ciencias.com/wp-content/uploads/2013/01/impacto-de-las-tic.pdf

Hillar, G. (2004). Arquitectura de Redes Lan. En G. Hillar, *Redes: Diseño, Actualización Y Reparación* (págs. 60-62). Buenos Aires: Hispano Americana S.A.

Huapaya, J. (2 de mayo de 2017). *Scribd Inc.* Obtenido de https://es.scribd.com/document/346995972/SERVIDOR-CORREO-pdf

Ibrahi, G. d. (15 de enero de 2017). *Equipo Editorial El Mostrador*. Obtenido de https://www.elmostrador.cl/cultura/2017/01/15/editor-de-the-economist-anticipa-en-chile-la-extincion-de-las-actuales-formas-de-trabajo-ante-la-cuarta-revolucion-industrial/

Icontec. (2006). *Tecnología De La Información. Técnicas De Seguridad. Sistemas De Gestión De La Seguridad De La Información (Sgsi). Requisitos.* Bogotá: Instituto Colombiano de Normas Técnicas y Certificación.

Instituto Colombiano De Normas Técnicas Y Certificación. (2011). *Gestión Del Riesgo. Principios Y Directrices.* Bogotá: ICONTEC.

Instituto Colombiano de Normas Técnicas y Certificación. (2005). *Tecnología De La Información. Técnicas De Seguridad. Sistemas De Gestión De La Seguridad De La Información (Sgsi).* Bogotá: ICONTEC.

Instituto Colombiano de Normas Técnicas y Certificación. (2007). *Sistemas De Gestión En Seguridad Y Salud Ocupacional. Requisitos.* Bogotá: ICONTEC.

Instituto Colombiano de Normas Técnicas y Certificación. (2013). *TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. CÓDIGO DE PRÁCTICAS PARA CONTROLES DE SEGURIDAD DE LA INFORMACIÓN.* Bogotá: Instituto Colombiano de Normas Técnicas y Certificación.

Instituto Colombiano de Normas Técnicas y Certificación. (2013). *Tecnologías De La Información. Técnicas De Seguridad. Sistemas De Gestión De Seguridad De La Informacón.* Bogotá: ICONTEC.

Instituto Nacional De Ciberseguridad. (20 de Marzo de 2017). *Instituto Nacional De Seguridad*. Obtenido de Instituto Nacional De Seguridad: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Instituto Nacional De Salud. (2018). *Instituto Nacional De Salud (CO).* Obtenido de https://www.ins.gov.co/Transparencia/Planes%20estratgicos%20sectoriales%20e%20institucionales/PLAN%20DE%20TRATAMIENTO%20DE%20SEGURIDAD%20Y%20PRIVACIDAD%20DE%20LA%20INFORMACI%C3%93N%20INS%20%281%29.pdf

Instituto Nacional de Tecnologías de la Comunicación. (2010). *Implantación de un SGSI en la empresa.* Obtenido de https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

Islas, O., & Gutierrez, F. (2004). Sociedad De La Información ¿utopía o panóptico? *Revista Latinoamericana De Comunicación Chasqui*, 28-29.

ISO Tools Excellence. (28 de Septiembre de 2013). *SGSI Blog especializado en Sistemas de Gestión.* Obtenido de SGSI Blog especializado en Sistemas de Gestión.: https://www.pmg-ssi.com/2017/09/situacion-norma-iso-27001-sudamerica/

López, J. S. (2013). *Proyecto Piloto Círculos De Innovación Social.* Obtenido de https://proyectocirculos.files.wordpress.com/2013/11/software.pdf

Lopez, R. (1998). Crítica de la teoría de la información. *Cinta de Moebio*. Obtenido de https://www.redalyc.org/pdf/101/10100304.pdf

Manga, G. (1995). planificación. En G. Manga, *Pedogógico Universal* (pág. 934). Bogotá: PROLIBROS LTDA.

Marcial, A. (diciembre de 2018). *DOCPLAYER.* Obtenido de https://docplayer.es/56292897-Angulo-marcial-noel-informacion-una-propuesta-conceptual-en-ciencias-de-la-informacion-vol-27-no-1-dic-p.html

Martínez, E. A. (30 de junio de 2016). *Repositorio Universidad horizonte.* Obtenido de http://www.unihorizonte.edu.co/revistas/index.php/TECKNE/article/download/165/155

Ministerio De Haciendas Y Administraciones Públicas De España. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

Ministerio del Interior de Colombia. (2014). *Políticas De Seguridad De La Información.* Bogotá.: MinInterior.

Molina, P. (10 de julio de 2013). *BBC MUNDO*. Obtenido de https://www.bbc.com/mundo/noticias/2013/07/130702_chomsky_internet_digital_criticas_pmt

Montilla, Y., Atencio, R., & Ruíz, A. (2009). *El Computador.* El Cid Editor.

Mora, C., Castro, M., Arroba, J., Perez, F., Pérez, C., García, Á., . . . Fernández, R. (2013). *Estructura y tecnología de los computadores I : gestión y sistemas.* Madrid: Uned.

Morales, J. (2011). El potencial de la información en nuestras empresas. En J. Morales, *Sistemas de información en la empresa* (págs. 7 -8). Barcelona: Editorial UOC.

Navarro, E. (2005). *Documenta.* Obtenido de http://documenta.ftp.catedu.es/apuntes/h_comunicacion.pdf

Neira, A. L. (2007). SGPI: Privacidad y beneficio económico en un SGSI . *27000.ES*, 3. Obtenido de ISO 27000.es.

Neira, B., & Gudiño, E. (2017). *Repositorio Politecnica Salesiana De Ecuador.* Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/14162/1/GT001840.pdf

Norton, P. (2006). *INTRODUCCION A LA COMPUTACION.* Ciudad de México: MCGRAW-HILL / INTERAMERICANA DE MEXICO.

Novoa, H. (20 de febrero de 2015). *Metodología para la implementación de un SGSI en la Fundación Universitaria Juan de Castellanos, bajo la Norma ISO 27001:2005.* Obtenido de https://reunir.unir.net/bitstream/handle/123456789/3129/HelenaClaraIsabel_Aleman_Novoa.pdf?sequence=1&isAllowed=y

Ñaupas, H., Mejía, E., Novoa, E., & Villagómez, A. (2014). Tipos, Niveles Y Enfoques De Investigación. En E. M. Humberto Ñaupas, *Metodología De La Investigación Cualitativa-Cuantivativa Y Redacción De La Tesis* (pág. 93.94). Bogotá: Ediciones de la U.

Ochoa, J. M., Armenta, J. A., Pizá, R. I., & Gonzalez, E. V. (octubre de 2009). *Instituto Tecnológico de Sonora.* Obtenido de https://patteitson.files.wordpress.com/2010/07/elementos-basicos-manual-1-final.pdf

Organización Para La Cooperación Y El Desarrollo Económico. (16 de junio de 2010). *oecd.org*. Obtenido de OECD: https://www.oecd.org/centrodemexico/ticsenlareactivacioneconomicademexico.htm

Pascual, S. (13 de Marzo de 2014). *Grupo Formazion*. Obtenido de Formación.com: https://www.formazion.com/noticias_formacion/importancia-del-certificado-de-calidad-iso-en-la-empresa-org-2804.html

Patterson, D. A., & Hennessy, J. L. (2011). Tipos de aplicaciones de computador y sus características. En D. A. Patterson, & J. L. Hennessy, *Estructura y diseño de computadores: la interfaz hardware/software (4a. ed.)* (págs. 5-6). Barcelona: Reverté, S. A.

Peralta, E. (2016). *revistas.curnvirtual.edu.co.* Obtenido de http://revistas.curnvirtual.edu.co/index.php/aglala/article/view/901/729

Pérez, J., & Gardey, A. (2012). *definicion.de*. Obtenido de https://definicion.de/planificacion/

Pérez, R. (2015). *Creatividad computacional.* Azcapotzalco: Grupo Editorial Patria.

Pérez, R., Lozano, P. M., Martínez, M., & Hernández, E. M. (Enero de 2018). *Scielo.org.mx.* Obtenido de http://www.scielo.org.mx/pdf/ride/v8n16/2007-7467-ride-8-16-00847.pdf

Portafolio. (23 de Agosto de 2016). *Portafolio.* Obtenido de Portafolio: http://www.portafolio.co/negocios/empresas/una-empresa-certificada-es-competitiva-499815

Porto, J. P., & Gardey, A. (8 de Agosto de 2013). *Definición. De*. Obtenido de Definición. De: https://definicion.de/confidencialidad/

Prolibros. (1995). Implantar. En Prolibros, *Pedagógico Universal* (pág. 620). Bogotá: Printer colombiana S.A.

Ranchal, J. (31 de diciembre de 2014). *muySeguridad.net*. Obtenido de Total Publishing Network S.A.: https://www.muyseguridad.net/2014/12/31/violaciones-de-seguridad-en-2014/

Real Academia Española. (2018). *DLE RAE*. Obtenido de https://dle.rae.es/?id=WT8tAMI

Real Academia Española. (2018). *dle.rae.es*. Obtenido de https://dle.rae.es/?id=L4RvR9q

Revista Dinero. (16 de octubre de 2014). *DINERO*. Obtenido de DINERO.COM: https://www.dinero.com/edicion-impresa/caratula/articulo/las-empresas-mas-admiradas-colombia/202113

Revista especializada ISOTOOLS. (15 de mayo de 2015). *ISOTools Excellence*. Obtenido de SGSI Blog especializado en Sistemas de Gestión: https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

Revista Portafolio. (23 de agosto de 2016). *Portafolio*. Obtenido de Portafolio.co: https://www.portafolio.co/negocios/empresas/una-empresa-certificada-es-competitiva-499815

Rosero, P. V. (2006). *Introducción A La Programación De Computadores.* Tangua.

Ruiz, R., & Buira, J. (2007). ¿Porqué nos ha de importar? En R. Ruiz, & J. Buira, *La sociedad de la información* (págs. 65-68). Barcelona: UOC, d'aquesta edició.

Santillán, J. V. (2016). *Informática I.* Ciudad de México: Grupo Editorial Patria, S.A.

Santos, J. (2014). Amenazas. En J. Santos, *Seguridad informática* (págs. 30-40). Madrid: RA-MA Editorial.

Santos, J. (2014). ELEMENTOS VULNERABLES EN EL SISTEMA INFORMÁTICO: HARDWARE, SOFTWARE Y DATOS. En J. Santos, *Seguridad Informática* (pág. 30). Madrid: RA-MA Editorial.

Servicio Nacional De Aprendizaje. (2018). *Sofia PLus.* Obtenido de http://oferta.senasofiaplus.edu.co/sofia-oferta/detalle-oferta.html?fm=0&fc=9CMnBjMmR6g

Solanes, J. M. (27 de agosto de 2015). *jmsolanes.net*. Obtenido de https://www.jmsolanes.net/es/servidor-de-archivos/

Tarazona, C. (2007). *Universidad Externdo de Colombia*. Obtenido de Universidad Externdo de Colombia: https://revistas.uexternado.edu.co/index.php/derpen/article/download/965/915/

Tarazona, C. H. (2013). Amenazas Informáticas Y Seguridad De La Información. *Etek Internacional.*, 137-138.

Tasaico, L. (06 de mayo de 2015). *preventionworld*. Obtenido de https://prevention-world.com/actualidad/articulos/principales-causas-los-errores-humanos-producen-accidentes/

Tecnología. (28 de Marzo de 2018). *LA FM*. Obtenido de LA FM: https://www.lafm.com.co/tecnologia/facebook-anuncia-cambios-tras-el-escandalo-de-cambridge-analytica/

Tejada, E. C. (2014). *Auditoría de seguridad informática.* Andalucía: IC Editorial.

Torres, S. A. (2014). IMPORTANCIA DE IMPLEMENTAR EL SGSI EN UNA EMPRESA CERTIFICADA. *Universidad Militar Nueva Granda*, 3.

Vásquez, S. B. (10 de agosto de 2010). *Wordpress*. Obtenido de http://redestipostopologias.blogspot.com/2009/03/topologia-de-redes.html

Vazquez, J. B. (2012). *Arquitectura De Computadoras I.* Tlalnepantla: RED TERCER MILENIO.

Vera, Á. A. (2014). *Instalacioón y Parametrización del Software.* Andalucía: IC Editorial.

Voutssas, J. (12 de abril de 2012). *Instituto de Investigaciones Bibliotecológicas y de la Información, UNAM.* Obtenido de http://www.interpares.org/display_file.cfm?doc=ip3_mexico_dissemination_jar_voutssas_legajos_12_2012.pdf

Zapata, C. E. (27 de julio de 2015). *Universidad Tecnológica Nacional Facultad Regional de Tucumán.* Obtenido de http://www.frt.utn.edu.ar/tecnoweb/imagenes/file/Material%20didactico%20de%20Tec_%20Educ_/EDUCACION%20Y%20TICS.pdf

# Anexos

Anexo 1: Tabla Análisis diferencial del Cuerpo de Bomberos Voluntarios de Tunja.xlsx

Anexo 2 tablas para el análisis y tratamiento de los riesgos en el cuerpo de bomberos voluntarios de tunja.xlsx